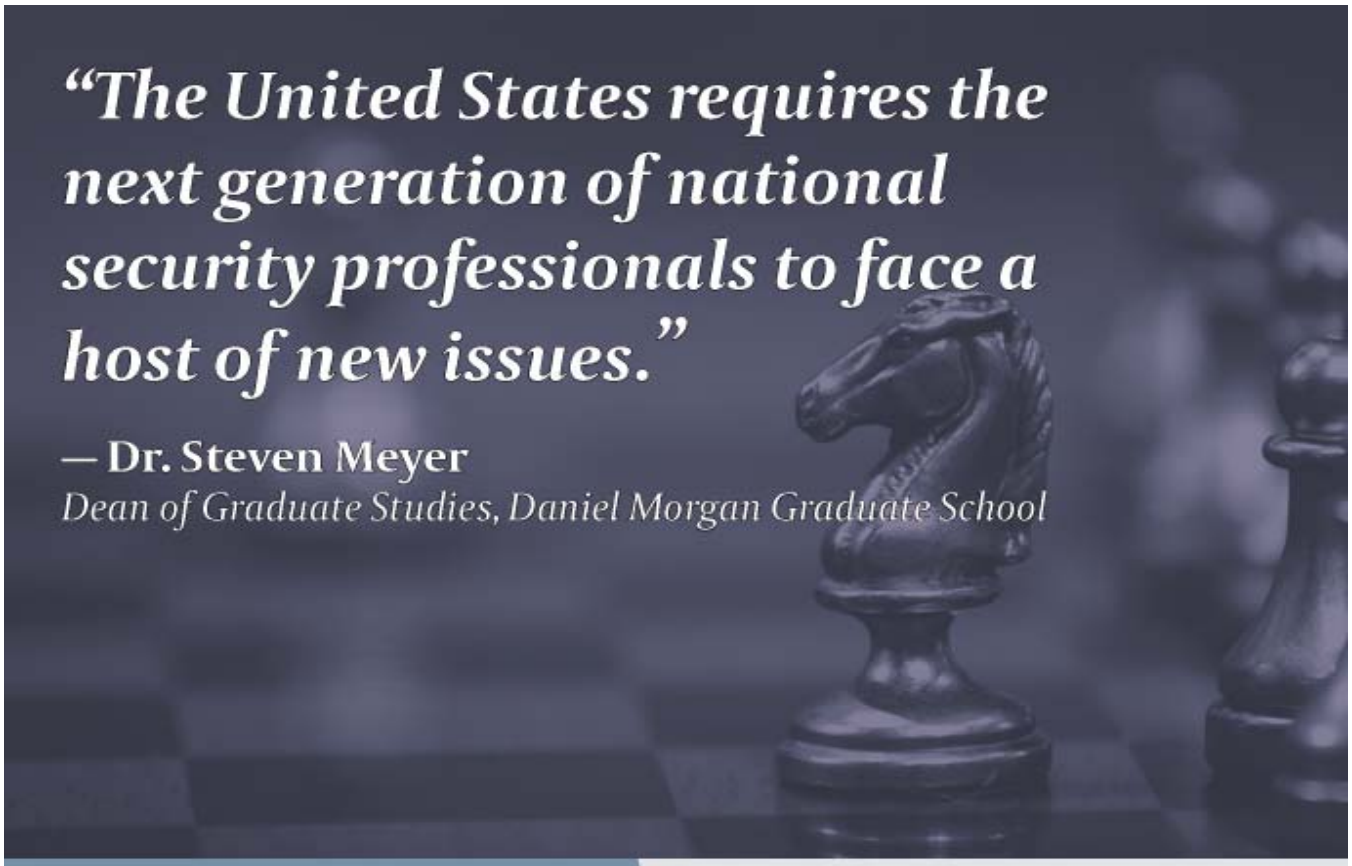
AMERICAN INTELLIGENCE JOURNAL

THE MAGAZINE FOR INTELLIGENCE PROFESSIONALS

The Cyber Threat: The Future of Intelligence in a Wired World

NMIF

Vol. 34, No. 1, 2017



"The United States requires the next generation of national security professionals to face a host of new issues."

— Dr. Steven Meyer
Dean of Graduate Studies, Daniel Morgan Graduate School

MISSION

The Daniel Morgan Graduate School educates and prepares future leaders to develop actionable solutions to global and domestic security challenges.

MASTER'S PROGRAMS

National Security

Intelligence

Managing Disruption & Violence

Visit **dmgs.org/nmia** to learn more.

DANIEL MORGAN
GRADUATE SCHOOL OF NATIONAL SECURITY

— WASHINGTON, D.C. —

American Intelligence Journal

THE MAGAZINE FOR INTELLIGENCE PROFESSIONALS

Vol. 34, No. 1 *2017* ISSN 0883-072X

The *American Intelligence Journal* (*AIJ*) is published by the National Military Intelligence Foundation (NMIF), a non-profit, non-political foundation supporting American intelligence professionals and the U.S. Intelligence Community, primarily through educational means. NMIF believes in the power of the intelligence mission to inspire young people to join the intelligence profession as a career of service to the nation. NMIF continuously engages current and future intelligence professionals, organizations, industry, and academic institutions to contribute to the overall sustainment of the U.S. military intelligence workforce.

Authors interested in submitting an article to the *Journal* are encouraged to send an inquiry—with a short summary of the text—to the Editor by e-mail at <aijeditor@nmif.org>. Articles and inquiries may also be submitted in hard copy to Editor, c/o NMIF, 256 Morris Creek Road, Cullen, Virginia 23934. Comments, suggestions, and observations on the editorial content of the *Journal* are also welcomed. Questions concerning subscriptions, advertising, and distribution should be directed to the Production Manager at <admin@nmif.org>.

The *American Intelligence Journal* is published semi-annually. Each issue runs 100-200 pages and is distributed to key government officials, members of Congress and their staffs, and university professors and libraries, as well as to NMIF donors, *Journal* subscribers, and contributors. Contributors include Intelligence Community leaders and professionals as well as academicians, research fellows, students, and others with interesting and informative perspectives.

AMERICAN INTELLIGENCE JOURNAL

Table of Contents

Table of Contents *(Continued)*

The opinions expressed in these articles are those of the authors alone. They do not reflect the official position of the U.S. government, nor that of the National Military Intelligence Foundation, nor that of the organizations where the authors are employed.

President's Message

The supposed Chinese curse "May you live in interesting times" seems to be upon us. Nothing seems to be going quite as it should. It does not matter if it is economics, politics, defense budgets, foreign threats, or the constantly changing face of terrorism. All these changes and "interesting" developments have impacted us. For the National Military Intelligence Foundation and the National Military Intelligence Association, it became apparent that a single organization would better serve the intelligence and national security communities. Instead of two organizations providing similar intelligence and national security support, NMIF has been reorganized to include most of the previous NMIA support areas, and the two organizations are now one under the NMIF logo. As a result, the *American Intelligence Journal*, other documents, the Awards Banquet, and other support areas are being moved over to NMIF, and a new website is being established, complete with more information and greater access.

The next step is planning NMIF activities for 2018. The Awards Banquet will be held at the McLean Hilton on 3 June 2018. The Awards Banquet provides the Intelligence Community the formal opportunity to recognize its best and most accomplished intelligence and national security professionals. The awards are normally presented by the appropriate service intel chief, agency director, or deputy director. The awards are named for intelligence luminaries and bestow the dignity of the award legacies on modern-day practitioners. In addition, NMIF Scholarship award winners are recognized. It is an inspiring ceremony, with musical entertainment provided by the West Point Alumni Glee Club singing patriotic and period songs. Last year, the Glee Club presented a memorable medley of Vietnam-era songs that brought deep emotions to many who lived through that time frame, and all of its turmoil.

In a year that has gone through many unforeseen changes, we learned with sad hearts of the passing of Lieutenant General James A. Williams. Not only did he have a long and distinguished military career, but he was a lifelong advocate for intelligence careers writ large. Starting out as a volunteer in the Observer Corps in 1942, he graduated from West Point in 1954. Early in his career he was offered a position in what would become INSCOM (U.S. Army Intelligence and Security Command). He shrewdly accepted, and consequently became an intelligence pioneer working through national intelligence issues for over four decades. Not only was he a key leader in many of the intelligence evolutions and revolutions, he continued to work intel and national security issues for the Intelligence Community as NMIA Chair. He was tireless in his efforts to organize symposia, special meetings, senior-level discussions, academic outreach, and multi-disciplinary events to help the IC and intel professionals address evolving threats, disconnects, and hard target problems. In fact, at the time he passed he was pursuing the possibility of a threat symposium given recent developments in the Arctic, and the more aggressive approach of potential competitors.

General Williams will be greatly missed, but NMIF will continue his tradition of support to the IC and to intel and national security professionals. The 2018 Awards Banquet will be dedicated to General Williams, and his daughter will present the award to the NMIF LTG Williams Fellow selectee. In addition, during the disestablishment of NMIA and the incorporation of most of its activities under NMIF, the combined Board of Directors took a broader view of the changing landscape in the larger Intelligence Community. A new Strategic Plan has been developed and the NMIF website is being developed for easier access. It will provide more information on careers, opportunities, mentoring, academic outreach, and an expanded speakers' bureau. Additional study areas are being reviewed, and the NMIF Scholarship effort is being enhanced.

LTG (USA, Ret) Mary Legere is the new NMIF Chair. She is a distinguished intelligence professional having served as Army G2 and INSCOM Commander. She spent considerable time overseas working the most difficult intelligence challenges. She is leading the planning for a spring presentation by a former senior intel leader focusing on "an intelligence career conversation . . . state of the IC . . . and the future of the IC"—all from the perspective of a senior official with many decades of service in intelligence leadership positions. National Intelligence University and other

national security students and professors will be invited, and it will be scheduled not to conflict with student courses and other activities. In addition, a separate effort is under way to assemble former intelligence directors for a half-day presentation and discussion with students and NMIF associates.

One area of NMIF that cannot be replicated is the large cadre of intelligence and national security professionals who are part of the Foundation, plus the Board of Directors. This is a pool of expertise that will be offered to organizations and universities to serve as consultants and multi-disciplinary spokespersons on critical issues and problem sets. These volunteers have served as senior intel leaders including COCOM J-2s, or their equivalent, and are eager to assist in the advocacy and support of career personnel, universities, and federal organizations.

One of the flagships for NMIF is the *American Intelligence Journal*, and it will continue its focus on key areas of concern within the intelligence arena. All past *AIJ*s have now been digitized, making distribution and research easier. This edition provides a comprehensive update of "Cyber Threats: The Future of Intelligence in a Wired World." It is an especially timely subject, and this issue provides an update to *AIJ*, Vol. 28, No. 2 (2010), "Cyber Security and Operations." The next *AIJ* will be dedicated to "Honoring Our Intelligence Heroes." Students pursuing intel or national security studies will also be invited to submit articles for publication in the *Journal*. The *AIJ* staff will provide assistance and staff mentoring, as well as guidance. We are also reviewing the possibility of adding interns to the *AIJ* staff. Out of these "interesting times," NMIF is planning to add appropriate historical context.

The Editor's Desk

Welcome to the first issue of *AIJ* published under the leadership of NMIF! As I remarked in this column in the final issue that came out as an NMIA product, the change should be negligible for authors and readers of the *Journal*, though we hope to be able to reach an even wider audience with the new lash-up.

The board of directors asked me to produce another issue dealing with cyber, as this subject has taken on ever greater significance since we put out a previous one (Vol. 28, No. 2, 2010) with the theme "Cyber Security and Operations." That volume primarily discussed cyber management and process, as U.S. Cyber Command was in its infancy and roles, missions, authorities, and procedures were still being worked out; this one focuses more on the threat itself. One common thread between the two issues is a leadoff article by the same brilliant muse, Paul Milton Hobart (a fictional pen name), to whet the readers' appetite. I'll leave it to our curious and enterprising readers to figure out the true identity of the author. That's what deciphering puzzles in the cyber world is all about! Paul's contribution seven years ago was "Cyber Death in Cyber Time and Cyber Space." This time he speculates on what might happen during a "Black Hats Attack."

Few people nowadays discard the seriousness of warfare in the cyber domain. In a lead-up to the annual meeting of the Association of the United States Army, held in October 2017, the weekly newsletter *AUSA's 5 Things* included a blurb "Threat Beyond the Borders," from which I quote: "Cyber warfare, a key part of the Multi-Domain Battle concept, is an example of a borderless threat the Army is addressing. 'Cyber threats have changed the way the Army looks at the network, data and networked systems,' said Lt. Gen. Paul Nakasone, Army Cyber Command commander. There is a lot of room for error. Attackers 'only have to be right once' to knock down a network, he said. What to watch: At AUSA's annual meeting…a Warrior's Corner presentation…focused on how to improve networks…and a forum…about talent management for cyber warriors." In February 2015, then-President Obama directed the DNI to establish a Cyber Threat Intelligence Integration Center. The CTIIC was designed as a national intelligence center focused on "connecting the dots" regarding malicious foreign cyber threats to the nation and cyber incidents affecting U.S. national interests. It would also provide to U.S. policymakers all-source analysis of those threats.

Since 2010, in addition to USCYBERCOM, not only the Army but virtually all the other services have established component commands to deal with this new, and frankly frightening, domain. As just one example of the kind of high-level talent needed here, LtGen (USMC) Vince Stewart, recently departed Director of DIA, came to that job in January 2015 from the cyber world as commander of Marine Forces Cyber (previously as a 1-star he was Director of Intelligence, USMC) and left it in October 2017 to become deputy commander of CYBERCOM. Right after he turned over DIA to LTG (USA) Bob Ashley, that Agency announced in its weekly Chief of Staff Update that October would be National Cyber Security Awareness Month. The National Counterintelligence and Security Center (NCSC), under ODNI, launched its "Know the Risk, Raise Your Shield" campaign to "engage and educate the IC on cybersecurity issues and provide tools and resources for being vigilant while using the internet and to protect national security."

Of course, the biggest news coming out of the upper levels of cyber management in 2017 was the decision by President Trump to elevate CYBERCOM from its status as a sub-unified command under U.S. Strategic Command to a full-fledged combatant command in its own right. For now, the CYBERCOM commander, ADM (USN) Mike Rogers, is still dual-hatted as Director of NSA, but many knowledgeable observers see the next logical step in the command's evolution being the separation of the two hats between two individuals. There has been quite a bit of crosstalk within Congress and the IC on this subject, and I would predict that it will likely be resolved sometime in 2018, when ADM Rogers is expected to retire. Whether that might mean NSA will be headed by a senior civilian for the first time in its 65-year history instead of a 3-star uniformed officer (4-star since the dual-hatting arrangement was devised during the long tenure of GEN (USA) Keith Alexander) remains to be seen. ADM Rogers has spoken to students at NIU

two successive years; though I cannot provide details, suffice it to say the Admiral has been very candid about this issue and some of the challenges for NSA and CYBERCOM during both the Obama and Trump administrations.

In a September 5, 2017, column in *The Washington Times*, titled "U.S. Cybersecurity Stuck in Its Own 'Groundhog Day'," David Inserra commented that a few months earlier Trump had tweeted that he was thinking about working with the Russians to create "an impenetrable Cyber Security unit so that election hacking, & many other negative things, will be guarded." When I heard that, I couldn't help but picture in my mind the proverbial "fox guarding the henhouse." Although the episode blew over after the tweet was quickly walked back, as many of Trump's tweets have been, Inserra suggested that "it exposed Washington's continuing confusion about how to approach bad actors in cyberspace." He added, going back to the Obama era, "The U.S. indicted five Chinese military hackers for cyberespionage. Then in 2015, the U.S. went back to buddy-buddy mode, inking an agreement with China on cybersecurity." Regarding Beijing, Inserra warns that "despite its promise to stop state-sponsored cyberattacks and espionage, the regime continues these activities, albeit in a less in-your-face fashion. Iran and North Korea are just as bad, or worse," he insists. "Washington's seesaw approach to cybersecurity—playing nice with our antagonists and then playing hardball—only shows them that we do not understand them or how to handle them. And that simply emboldens them further."

Another indicator that cyber has come into its own is the fact the Army provisionally designated its Cyber Corps as a new branch in 2014. As a retired Army officer, I was frankly amazed, but not surprised, when that decision was made. A Cyber Operations Officer (17A) now wears distinctive branch insignia with two crossed lightning bolts surmounted by a vertical dagger. According to an official Army website, "Cyber branch is a maneuver branch with the mission to conduct defensive and offensive cyberspace operations (DCO and OCO). Cyber is the only branch designed to directly engage threats within the cyberspace domain." The last time that service created a new branch was Aviation, back in the era when I was still serving. The Army's cyber component command is located at Fort Belvoir, VA, but plans are to move it to Fort Gordon, GA, which will be not only the home of Signal Corps but also the Cyber Center of Excellence, just as Fort Huachuca, AZ, is the Intelligence Center of Excellence.

Included in this rather lengthy issue of *AIJ* are several cyber-related articles. Navy CDR Cassie Deppa, a CYBERCOM public affairs officer, provides a command overview which I personally had the pleasure of hearing during a meeting of the NCR Chapter of then-NMIA held in a most fitting location at Fort Meade, MD, the National Cryptologic Museum. Repeat *AIJ* author Dr. Bill Kelly of Auburn University writes about alleged Chinese "cyberspies," with that global competitor representing one of the greatest threats to U.S. national security. AFOSI agent and former NIU student Sarah Heidenreich teamed with one of her former instructors and repeat *AIJ* author, Dr. "Wes" Westbrooks, to highlight the challenge of exposing criminals who utilize "darknet" markets. Jim Carlini, representing the private sector, which is probably the most vulnerable to cyber mischief, has coined his own concept, "NANOKRIEG," and explains how global net superiority can be achieved. Another repeat author (several times over), Troy Smith of Trinidad and Tobago, explores how the Islamic State has exploited the use of cyber in its dastardly and vicious campaign to establish a permanent caliphate. Although not precisely focused on the cyber threat per se, but instead the exploding role of social media, COL Steve Henricks talks about social media and open-source information as they relate to the IC, while Columbia graduate student Nicki Softness also holds forth on social media and intelligence. COL Reid Webber proposes an intelligence strategy for Joint Force 2020, and one of my former students now with ODNI, MAJ Mike Hein, explains how the Army's Strategic Intelligence Officers (FA 34) are making a big impact in the integrated DIA regional intelligence centers set up as the result of a major reorganization pushed by then-Director Mike Flynn (who has been all over the news in 2017 for other activities since his military retirement in 2014).

In this issue we are proud to offer three superb articles by women about women. A group of students in NIU's School of S&T Intelligence join with their then-Associate Dean (now Dean) in showcasing "Renaissance women." Contrary to the conventional wisdom that men tend to excel in the hard sciences while women are better in social sciences and humanities, this group insists women are a perfect match for S&T intelligence education, and they provide the statistics to back it up. Repeat *AIJ* author Kailah Murry of the Army Command and General Staff College follows up a previous article she wrote for the *Journal* and explores women in combat operations. Finally, Dr. Bina Patel of NGIC, an expert on terrorism and the radicalization process, explores what motivates female suicide bombers, a growing and disturbing trend.

THE EDITOR'S DESK

As is customary each year, we publish award-winning papers from the various military service schools. The last winner of the NMIA writing award at the Air Command and Staff College, Lt Col Jesse Winkels, explains how humanitarian assistance and disaster relief operations can be enhanced by expanding integrated coalition and NGO ISR. Keeping with our effort to include at least one article on China in every issue, our second article on that highly ambitious, emerging global power is by a sterling student who recently graduated from Yale and is now at Oxford. Alex Herkert examines U.S. intelligence failures related to the China-Taiwan relationship and our difficult "One China" policy. My former teaching colleague, Dr. John Gentry, now at Georgetown, insists that the career cycle of intelligence analysts needs to be rebalanced. John will be the discussant for a panel I am chairing during the 2018 convention of the Intelligence Studies Association in San Francisco. Many of my close academic contacts have been forged through ISA's vibrant Intelligence Studies Section, and some of the papers presented have been turned into *AIJ* articles. Also in the realm of analysis, two perceptive British military officers explore ways to "assess assessments" and ask just how useful predictive intelligence is. Some observers would insist the role of intelligence is not to predict, but merely to forecast. Not wishing to get into that fight, I will steer clear of such semantic arguments for the time being.

I relish receiving manuscripts from young enlisted personnel, though I don't receive as many as desired. I always tell them their opinions are just as important as, if not more so, those of the officer corps. Consequently, Airman First Class Candace Stevens offers an interesting treatise on technology in foreign intelligence gathering. Speaking of foreign, we continue to receive a large number of inputs from international partners, and not just from the "Five Eyes." I advise them not to be intimidated by the moniker "American" in the publication's title and "National" in the organization's name. It's clear no nation fights alone nowadays. Alliances, coalitions, and partnerships are the only way to deal with the complex global threats we are facing, and of course the cyber threat penetrates national boundaries with ease. Dr. Rad Malkawi of Jordan talks about cultural awareness and interactions by U.S. military personnel during overseas deployments, harking back to one of my favorite issues of *AIJ* several years ago which explored regional issues and cultural intelligence. Finally, repeat author Dan Opstal, who graduated from sending me several book reviews to full-length feature articles, provides a vivid pictorial essay on how the U.S. government's Civil Applications Committee utilizes interagency remote sensing to support a host of emergency-type situations that demand civil-military collaboration.

Our selection for the "In My View" corner of *AIJ* offers an intriguing piece by one of NIU's Cyber concentration faculty members. Anthony Smith writes about "signal pollution" as an unseen threat that must be tackled. Our "Profiles in Intelligence" offering digs back into history and reveals deception used in the ill-fated case of Mary, Queen of Scots. This is an excellent sequel to the issue we published a couple of years ago on "Denial and Deception." Finally, as usual we have a terrific collection of book reviews in the current issue, at least one of which touches on our cyber theme.

Our next issue will be a special one dedicated to the remarkable figures for whom the annual NMIF awards are named. The theme is "Honoring Our Intelligence Heroes: The Historical Heritage of NMIA/NMIF Awards." It will contain biographic sketches and remembrances of each of those individuals, the intent being to present a hard copy to all future award winners, starting with next June's Awards Banquet, as a token of our appreciation for their service and contributions to the intelligence enterprise. That issue is now closed out, as I have enough volunteers to write all those relatively short articles. However, there is still plenty of space in the next two editions, the first focusing on the theme "Counterintelligence and the Insider Threat" and the second on "HUMINT in the 21st Century: Espionage, Attaché Operations, and Other Challenges." I solicit your inputs to the *Journal*, whether or not what you would like to write about fits one of these themes closely. If your manuscript deals with intelligence, or national security with an intelligence bent, your wisdom is highly valued and we want to offer you a venue to share it with our broad and growing audience. The CI issue will be published in the fall of 2018, the HUMINT issue in early 2019. I am also looking for book reviews for those two issues. If interested, please contact me at William.Spracher@dodiis.mil.

Many thanks to all for your support and feedback in making *AIJ* successful and highly respected, and also your dedication to the goals and objectives of NMIF!

Bill Spracher
Editor

Black Hats Attack

by Paul Milton Hobart

Two young women sat next to each other in chairs facing three screens each. The air was filled with electricity, figuratively and maybe actually. The room they were in—the building they were in—seemed to hum with unseen kinetic energy. The screens were filled with overlapping tabs and moving symbols, plus an occasional graphic that showed progress and specifics in understandable but detailed form.

The women were intently engaged, and had not noticed the man behind them enter the room, let alone note that he was standing behind them so that he could see both sets of screens and the work of the two operators. There were no reflections in the soft flat screens. There had been no noise. The small fans blew the electric air away from the women toward their backs. Nothing gave him away. Even though there were at least two instructors in the room, no one spoke.

The women were enjoying their interaction. They were, in effect, playing computer games, although both realized that if they did what they were doing now to distant real servers and computers, and the people who depended on those mechanisms, they would be doing harm to others and would be breaking the law.

…they were cyber murderers and mathematical maimers and information thieves and system vandals and computational teenagers on a crime-ridden joy ride through the digital back alleys of the cyber universe.

They were changing digits in a fire control link. They modified data for a ship's navigational computations. They caused the failure of hoses that delivered volatile fuel. They sucked information out of the pulsing lights of computers seen from above or through windows from afar. They activated cameras where people least expected them. They slowed operations and hid necessary command prompts. They seeded parasitic digi-creatures into digital mechanisms to take everything away. They destroyed key methods and processes. They defeated air gaps. They placed false and misleading information in realistic locations, concealed within dependable data. They exploited information systems. They were learning how to enter and affect cryptocurrency channels. Finally, they killed the vital systems that made the target machines work. In their most blunt form, they were cyber murderers and mathematical maimers and information thieves and system vandals and computational teenagers on a crime-ridden joy ride through the digital back alleys of the cyber universe.

Their work was also delicate, nuanced, and special—filled with wafting movements and fleeting moments of pure technical beauty—like digital multi-colored feathers falling softly through the algorithmic atmosphere, having been shed by gliding bird-like entities inhabiting and passing—always passing—through the nether-regions of cyberspace. Sometimes they felt they were God-like.

They had engaged in conversations between themselves and with their trainers about the ethical issues that each of them had noted during their training. They wrestled with the idea that they were training and practicing to enter the intimate information spheres and high-priced advanced technologies belonging to other human beings, and to organizational entities of some import, to damage them, to steal from them, to take advantage of them, to subvert them and, in some few cases, to utterly destroy them. They came to grips with the idea that they were soldiers of a kind whom few would recognize—without uniforms, without traditional presence, and acting outside what might be thought of as the rule of law. They were spies too, engaging in technical espionage. They would be feared, and that too was part of their reward.

They had been given information that allowed them to hack into training systems and to penetrate programs and accounts which had been assigned to them ahead of time. Each one had a notebook which contained everything they needed, and a memory stick that could only be used on the third screen, which was not connected to the Internet. It was on this third screen, from the memory sticks, that they developed program sets and increments of code, stripped of Internet protocols and identifying addressable data, which

they needed for various tasks and missions. They would update base data for the task at hand and then load this finished work onto completely clean disks and use only those disks to move programs and bits of data onto the organizational intranet and eventually into the wild of the Internet to send them against the targets they were attacking.

Once used, even in this training, those disks were never used again but instead were inserted into a container of chemicals which turned them and the data they held to instant mush. They were told this was for the protection of the intellectual property with which they worked and of which they now were part, something the people they were working for had explained many times. The women were not fooled by that claim. They knew it was more about how "illegal" things worked.

They had been given a scenario in which they would assemble a set of processes and procedures to enter targeted systems, in this case primarily known as hard-wired servers, but also some "cloud" repositories too.

One of the most interesting things they were given to do was to lay the groundwork for future cyber operations. The concept had been part of their overall training throughout, but only on three occasions had they participated directly in specific exercises. One reason for that was that it took so long—on the last iteration they had stayed at their systems nearly 24 hours and were relieved from the exercise only when they began to make mistakes which "monitor central" had been only too happy to point out. During these "operational training modules," which is how the Instructors referred to them, the room they worked in was full of observers and note-takers. Often one of their screens would be projected up on the huge central display which everyone in the room could see and discuss. A senior instructor was always present and directly engaged in all their decisions and actions.

They had been given a scenario in which they would assemble a set of processes and procedures to enter targeted systems, in this case primarily known as hard-wired servers, but also some "cloud" repositories too. The goal was to set—inside the system's ancillary apps, deep into functional programs, and even in the security software the systems were relying on to protect them—sleeping capabilities. These "sleepers" as they liked to call them, would then be capable of being activated at any time, over a very long period. Some came with transferable code which ensured that if, say, a security program which was being used throughout a system was upgraded or totally replaced, their hidden "sleeper" would self-transfer or hide and wait to embed itself in any new program.

One of their favorite methods was called the "Orange." The reason for the name was that, once the outer layer of a system had been penetrated, the remainder of the system was accessible and vulnerable. Often the technical other-source intelligence provided to them had included enough information so that they could enter a system's firewall or security scanning program and worm their way in from there. The trick was to do so without disturbing the cyber "Wa," ŒT, and to continue into the layer elements of the system until they found the right site to nest and lay fallow. These intrusions were detectable, and often were the subject of intense security scrutiny and technical solution interest. What few people knew was that the "sleepers" had the ability to reproduce and to "slide" away from the counter-cyber hunters. They were the tools of the future—and both women appreciated the fact that they were being entrusted with them in any way.

No one ever explained several questions they had, but they imagined they knew some answers. These "sleepers" were the enablers for a variety of actions, when the time was right. As an example, they could spurt erroneous data into a data stream, masking it as real data since the time-phase was the same as the original or current operating data. They could open cyber "chutes" to and from data and functions, providing "backdoors" and "open Windows" through which any kind of functional attack or debilitating strike might be made, or from which enormous amounts of data could be surreptitiously exported out to eager receivers. Retrieval was impossible, they were told. Once embedded, the "sleepers" could only be recovered in partial form and would commit "cell and code suicide" at some point, appearing to be, in the end, simple word processing programs.

No one discussed activation of the "sleepers" in any detail, but it seemed obvious to the women that in some cases activation was human-enabled or accomplished from non-cyber sources. They knew all about the recent cases of human activity that would facilitate this—for example, the export of files from the U.S. military undertaken by Bradley (now Chelsea) Manning, and the similar huge compromise of material from the U.S. National Security Agency by Edward Snowden. However, those were not the only ones. They wondered how many people would recognize these names: Gary McKinnon, Jeremy Hammond, Vladimir Levin, and Michael Calce, or groups like LulzSec, the Syrian Electronic Army, Lizard Squad, or the Aurora Hackers, not to mention the very famous Anonymous? They wondered what it was that led investigators to believe simply everything these people and groups had done was over with when they were arrested or had run away, or in at least one case had become "good hackers."

Once a week, usually on Thursday, the day was given over to non-computer-focused training. The women were taught about current events relating to reported espionage and cyber-attack events, and on historical information that would help them understand the context of their training. They spent considerable time on what some called APT—advanced persistent threats—against nation-states, against political entities, and against large business entities. As an example, they were taught about the Sony Corporation's problems with pirated intellectual property which had been held for ransom by the perpetrators, and vulnerabilities in computer company hardware and software which had been exploited by common hackers, whom the women thought of as "brothers or sisters in arms," but not on the same level as they were on.

They studied counter-cybercrime reports and reports by applicable companies working in the anti-cybercrime and counter-cybercrime and cyberespionage fields. They were up to date on the recent cases of nation-states hacking into privileged communications systems and then putting collected information into the public domain to compromise the integrity of inter- and intra-nation relationships and leadership. They were well-informed about cyberattacks at the nation-state level, such as those carried out apparently by Russia against Georgia, Estonia, and Ukraine. They knew about some events that had never been widely reported and they understood that such knowledge was potentially dangerous for them, but was also, they thought, a sign of the trust and confidence in which they were held by their employers.

All of this was exciting and stimulating. The women were sometimes visibly affected by their training and what they were practicing to do. They found their work worth any cost in family disengagement and monk-like living in the compound. They were a little lonely sometimes. Even the observers and instructors were not able to engage them on a personal level, nor were the women able to interact with them except in the most official of ways. Security had made that very plain from the beginning. This was all business and obviously important for their employers—whoever they were—to invest in them like this.

The women were basically anonymous, having no real identity and no obvious appearance or traits that would set them apart. They were, in the end, the most secret of weapons, the unsuspected and the unrecognized, but deadly and dangerous just the same. It was exhilarating and at the same time challenging. They were told repeatedly that their success depended on leaving no trace behind, showing no calling card, and having no excessive need for recognition. They were unique—and that had to be enough.

They had talked quietly during monitored walks they took, to get a break from their machines, about the implications of this new life they were leading, and how it might end. They were not naïve, but the benefits so far were seemingly worth the risk. Their bank accounts were impressive.

They had been given "break-out" instructions from their anxious security officers. If anything happened to put them or the facility in which they worked, or the quarters in which they were housed, at risk—and if they believed their work was compromised and they were threatened in some way—they were to stop whatever they were doing, pick up their pre-packed bag with two sets of untraceable clothing, new identity cards, money, and other tools and materials, and go to a specified bus station, use the specified ID they had been given, pay cash, take any bus, and stay on buses for two days, then switch to a rental car using ID set #2, drive a specified route from one city to another, and then "meld" into the social order. No airplanes were allowed. If the team wanted them again, it would contact them through the one-way phones in their bags. Otherwise they would be free to begin new lives. The women were impressed. This seemed to indicate their lives were "worth saving."

Date night was also part of their reality now. Once a week they were treated to a night with a new man—which was their preference—never the same, but always impressive. There was only one rule: no discussion at all of anything they did in their work. They assumed they were under close video and audio surveillance but had yet to detect it.

They had several "routine" missions to perform, including penetrating firewalls and protective barriers of all kinds, installing malware, installing hidden entry codes, and copying precise files, once again assigned to them surreptitiously. What made it so much fun was that somewhere there was a monitoring person, whom they had never met but who sent them messages, pointing out mistakes and risks that they may not otherwise have seen. At some point, it became a game to see if they could do everything right, thus avoiding the snarky comments from "monitor central," who often had mentioned their lack of knowledge and even their inadequate personal intellect. If they ever met the "monitor," they would certainly give him a piece of their minds. They were sure he was a man, without good scientific reasons for that belief. It just seemed right. What a pìyan!

This was their twentieth "operational" session. During the past two, they had not heard from the "monitor" until the very end. He had grudgingly complimented them on their learned achievements, but more important than gratuitous compliments he did not or could not point out any deficiencies.

This time, they had gotten into their targets and had done everything they were asked to do, with one exception. They were now preparing to enter malicious codes that would, according to their instructors, be very difficult to find, impossible to fix, and would basically render the distant servers and computers ineffective—forever. It would break them to the point that they would have to be replaced.

They had done this routine three times before. It required that they follow a strict protocol and carefully complete sequential tasks without alerting the distant computers and their human operators that something terrible was happening. They had failed—so said the tiresome monitor—during all three of the earlier attempts, but they were very close to success on the third try. Today it seemed like they knew what to do and how to do it well enough to complete the task without any warning to the distant ends.

They brought the code up on each screen. It was a program written in modified LISP, not a new or exactly modern approach, but one that had proven effective and was what the instructors wanted. They could read it using language comments provided by instructors but could not understand fully how it worked and, despite their questions, the instructors had told them nothing. It seemed that some of the effective elements and cues would be borrowed from distant operating systems and then would autonomously morph into computer-killers and virus-injectors while residing inside the targeted machines.

All three of the "black" servers were operating on the Darknet, through virtual private networks, and could be rental-accessed for short periods of time simply to send information anonymously.

This made them think that what they saw on their screens was not the entirety of the coded language with which they were working. They each had a passing knowledge of C++ and Python because of the work they had to do at their schools, strains of which they thought they had detected in some of the "monitor's" comments. It seemed like some of the code they applied could be made much more efficient and effective if they had simply used Java script. They also believed they had detected Ruby on Rails apps. They had brought both insights up to their instructors, but their views and ideas were met with stony silence. This made them think there was more to this than they had been told. Of course, there was! They admitted this quietly to each other.

They staged their working code in packets—forming it to be sent in parts, in irregular forms, and in asynchronous channels—so that detecting the full structure and make-up along the way would be very hard to do. They lined up twelve or more servers through which to send the packets, geographically dispersed and in at least three cases not fully identified with real Internet protocol addresses. All three of the "black" servers were operating on the Darknet, through virtual private networks, and could be rental-accessed for short periods of time simply to send information anonymously. In their work, the two women had never rented anything. They had hacked the Darknet machines with no problem. They wondered who really thought they were immune from discovery and identification on the so-called "black side?"

What really gave them confidence in what they were doing was their instructors insisting that whatever could be encrypted should be. They used public key encryption and military-grade PGP code often, but occasionally the instructors had given them access to a separate encryption program in which they simply entered their work—always on the third screen—and then set the finished encrypted product loose on the network they were targeting. They assumed someone, maybe a partially witting insider, had a way to capture their work and put it in a form, decrypted they thought so that the tasks embodied in their coded tools would then be understood and applied in microseconds, but neither of them was sure of that. No discussion had ever occurred about such procedures.

Each of the women took the disks out of their third-screen machines and set them into the disk drives of one of their active machines. Once they closed the drive, they had only so long as it took for the machines to read the disks and send the information on its way. As soon as the process was complete, they were to remove the disks immediately and hand them over to the instructors.

On this day, just before they were completing their preparation, something unusual had happened, which they assumed to be part of their training and testing. The process of assigning the attack/killing code to a specific distant end address had been changed. They were given a new ISP, other address externals, and some internal information and told to put this new information on the attack disk. This was easy to do, and after a short period of change they were ready to act. There was a short delay which they assumed to be a timing issue.

They looked to the instructor who was sitting in front of them; they saw him smile and look just over their heads. The tension they felt was amplified by something in the instructor's glance and then his almost imperceptible nod. Each of them closed the disk drawer and then pressed the mouse to stimulate the cursor that was hovering over the activating instruction. It was, to them, like pulling a trigger on a gun and seeing the bullet leave the barrel, at least in

their mind's eye. They felt the impact, distant though it was, and knew with the certainty of a sniper that they had each killed. It was their first blood.

It was, to them, like pulling a trigger on a gun and seeing the bullet leave the barrel, at least in their mind's eye. They felt the impact, distant though it was, and knew with the certainty of a sniper that they had each killed. It was their first blood.

The women did not know each other before they had been brought together in this training, but the similarities in their backgrounds were noteworthy. Each had been interested in computers from an early age, owing to their parents who had provided them with simple and then more complicated computational devices when they were barely three years old.

Each had done well in school in math, general science and, of course, computer operations, but had faltered in common subjects such as history and the arts. They were both like electronic mechanics, understanding computers and how they worked without socializing themselves in other ways. Once they rose to gymnasium level they were hopelessly engaged in all things computers. They inhabited arcades for fun and spent hours of their time online using several made-up identities. They went to malls to visit the Apple© and Microsoft© stores and to see what was on the shelves at BestBuy© and other similar stores.

They were not without their vices. Each had relationships with other persons, but nothing had ever really clicked. They were okay in everyday appearance but very nice looking if they put on make-up and the right clothes. One of them had a small tattoo which the administrative people had removed in a painful laser-based session. There was little that tied them to any sort of counter-culture or revolutionary group. They simply had no interest in that approach to life. They used alcohol occasionally and smoked cannabis but not often. They were consumed by computers and, as they matured into adulthood, they each developed code-writing skills in contemporary computer languages. For each of them, that had been the turning point. They could do something that had value, and not everyone could do.

Each woman had been approached by universities and commercial companies which offered good salaries and educational opportunities. Each of them had attended seminars and interviews and "meet & greet" parties, and each of them was considering which school or which job opportunity to go for. They met at one of the "meet & greet" gatherings sponsored by a coastal university. They had been asked to provide their resumes ahead of time, and they were paired with each other during the presentations before the social hour. They had been formally introduced by a good-looking young man who said he was an intern for one of the professors. He was impressively polite and after introductions he left them to interact on their own.

They talked for a few minutes. Each was surprised at how easy it was to talk with the other, someone who identified so readily. The spark of new friendship and familiarity was immediately present and, by the end of the evening, talking with hardly anyone else, they found themselves exchanging contact information and planning how they could get together again soon.

That was when the young man who had introduced them showed up again. He was handsome and charming, but a little reserved too, which made one of them comment to the other that he seemed like someone in charge of, or responsible for, something.

He invited them to meet the following day at a well-known hotel to discuss future possibilities. His manner and appearance fit. They agreed. When they arrived, they were met and ushered into a room. It was obvious the young man was no longer the key person with whom they were meeting. The older man to whom they were now being introduced was dark and stern—all business—and even though the young man they knew from the "meet & greet" was there with him, the older man did all the talking. They were offered the jobs they had now—placed in the context of technical training and developing specialized knowledge—which would somehow be used by the state.

They could ask only a few questions. Terse answers were given which included little information. Their benefits were explained. They would live together in the same building in adjoining spaces, and would be well paid. Their medical needs would be provided, and they would eat all meals in their space—meals that would be prepared elsewhere. They would have access to TV and other forms of entertainment, but no Internet access or phone calls. They would be confined to a large campus but could only move about or go to other locations away from their quarters under supervision or when monitored by compound surveillance. Clothing and personal amenities would be routinely provided.

Their contract would be for one year, and might be extended after that. They would be subject to the laws and rules of the State Security Service and would be held responsible for any breaches. They were required to give up their surface and biological identities and to take some personality inventory tests and surveys. They were given papers to sign and told they had to decide now.

Once they began their "training," they could no longer visit any family members in person, no matter what. This restriction did not seem that hard to tolerate for either woman since their family members had no idea what their skills were, let alone the sharp turn their lives had taken. There was little interest in them from their families. They were fine with separation for a year.

The offered salary was so much better than anything they had even heard of, and the other benefits seemed worth even more. They thought—each in their own way—that they could do anything for a year. Both signed.

Now they found themselves on the edge of something exciting—a form of graduation. They had just executed a successful insertion of malicious code that would "kill" the distant target computers. They were about to open the disk drive doors and retrieve the dangerous "training" capabilities on those disks, which at their direction had just flown out into the digital battlespace to wreak havoc, when the man behind them spoke.

He told them to stop what they were doing and to sit back in their chairs and relax. His apparent complete authority was palpable and they immediately complied. They were perspiring. Was this the moment they had been waiting for when the "monitor" would appear to congratulate them on their training progress and their technical achievements? The air went out of the room.

The man came around in front of them, placing one hand on the nearest screen as if he owned it. His manner was self-assured but not arrogant. The two women waited to hear what he had to say. Both noted that he was easy on the eye and very well-dressed. They could smell his expensive scent. This heightened their anticipation.

The man looked at both, with a business-like expression of interest in them. Each woman felt he was going to speak directly to her. He waited for a moment and then explained what was happening. They had each passed all the tests and achieved the expectations of their training cadre. They were now ready for "operational employment," and would be expected to leave the facility they were in and go on to a new and challenging role—which could not be fully explained—"at this time."

What could be explained now, the man said, was what their real targets had been for this final exercise. He reached into his coat pocket and withdrew a 3x5 card with three characters written on it. He showed each of the women the card by holding it so they could see it directly, then returned it to his coat pocket. He drew in a breath and spoke to them: "You attacked two computers in an office located in Seattle, Washington State, in the U.S. The computers you attacked will never work properly again—although it may take a few hours for the users to realize that. First, they will think the computers are running slow, then programs will fail to work, then data will disappear, and ultimately they will be unusable. The hard drives will be damaged beyond repair. At some point their information technology experts will be called in. The machines will be examined and the IT people will confirm their worst fears—that you, whoever you are, have attacked and destroyed their capability. What they may not immediately link with this event will be the timing of another activity in which their office is engaging, the success of which is completely dependent on the two dead computers. You should be proud of your efforts in this final test and you can rest assured that State Security will forever appreciate your skills and abilities."

He said this last sentence with a slight smile. They heard the compliments but they also knew that they were now linked directly to an actual attack against an actual target, one that would seek to find them and take them to task. They had joined the State Security team. The feeling was fearful as well as a source of pride.

The man thanked them, wished them well, and abruptly turned to leave, but then hesitated and turned back to the women. He smiled slightly and said: "I want you to know that you were right about me. I was insufferable when you first began, but now I admire your fine work for our country. I look forward to hearing of your future success."

The women were taken aback. How did he know what they thought of him? Of course, he was the "monitor." They could not help but think about what they had said about him, behind his back, but obviously in an environment in which his "insufferability," and their views of him, had been recorded in some way. Would they have to pay a price for that?

He looked at the nearest woman with something like reserved warmth, and addressed her by her given name. He said that she would be working with him in the future, and he looked forward to a great partnership. He did not say anything to the other woman, but quickly walked out through a side door. Two instructors came in—one for each woman—and escorted them out, one to the right and one to the left. They never saw each other again.

The future is there... looking back at us. Trying to make sense of the fiction we will have become.

-William Gibson, *Pattern Recognition*

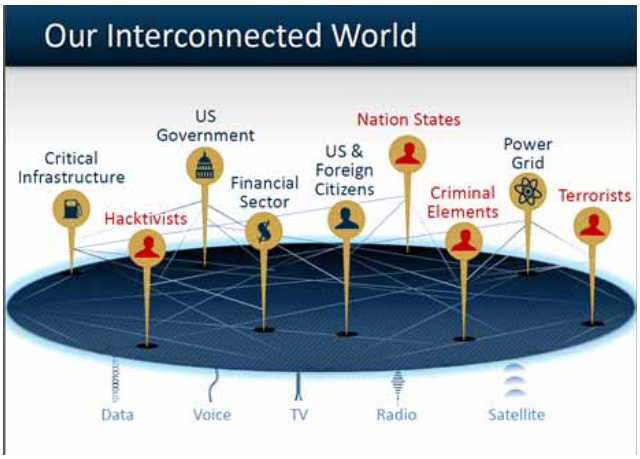
U.S. Cyber Command: An Overview

by CDR (USNR) Catherine S. Deppa

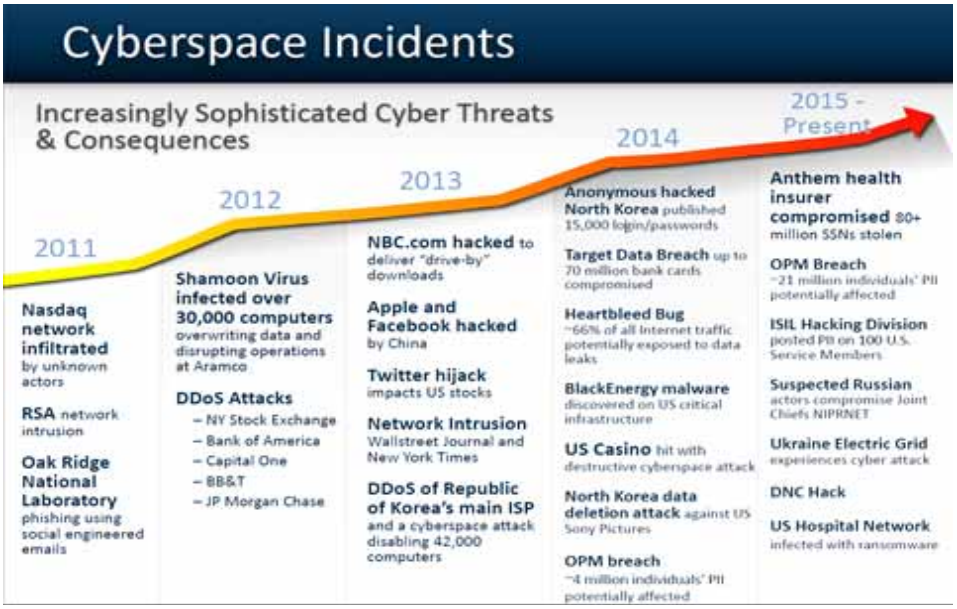
The cyberspace domain has enabled a golden age of innovation, information, and connectedness, vastly improving American quality of life. The complexity of this environment, however, is evolving at an exponential rate, resulting in unforeseen vulnerabilities and challenges. The promise of the Internet of Things (IOT), driverless cars, drones, smart appliances, quantum computing, big data, and artificial intelligence may result in catastrophes if not strategically managed, adequately protected, and vigorously defended.

Since the late 1990s, cyberspace incidents have increased in scale. Minor events such as distributed denial of service (DDOS) and website defacements have been superseded by major hacks such as the doxing campaigns targeting U.S. and European elections and attacks on critical infrastructure such as the Ukraine power grid hacks of 2015 and 2016.

Cyberspace offers asymmetric advantages to states, terrorists, criminals, and "hacktivists." New applications and devices improve our quality of life but also have unintended consequences, giving adversaries more attack surfaces.



The U.S. government continues to refine its approach to cyber security policy, which is executed by several governmental agencies and departments. As a part of its

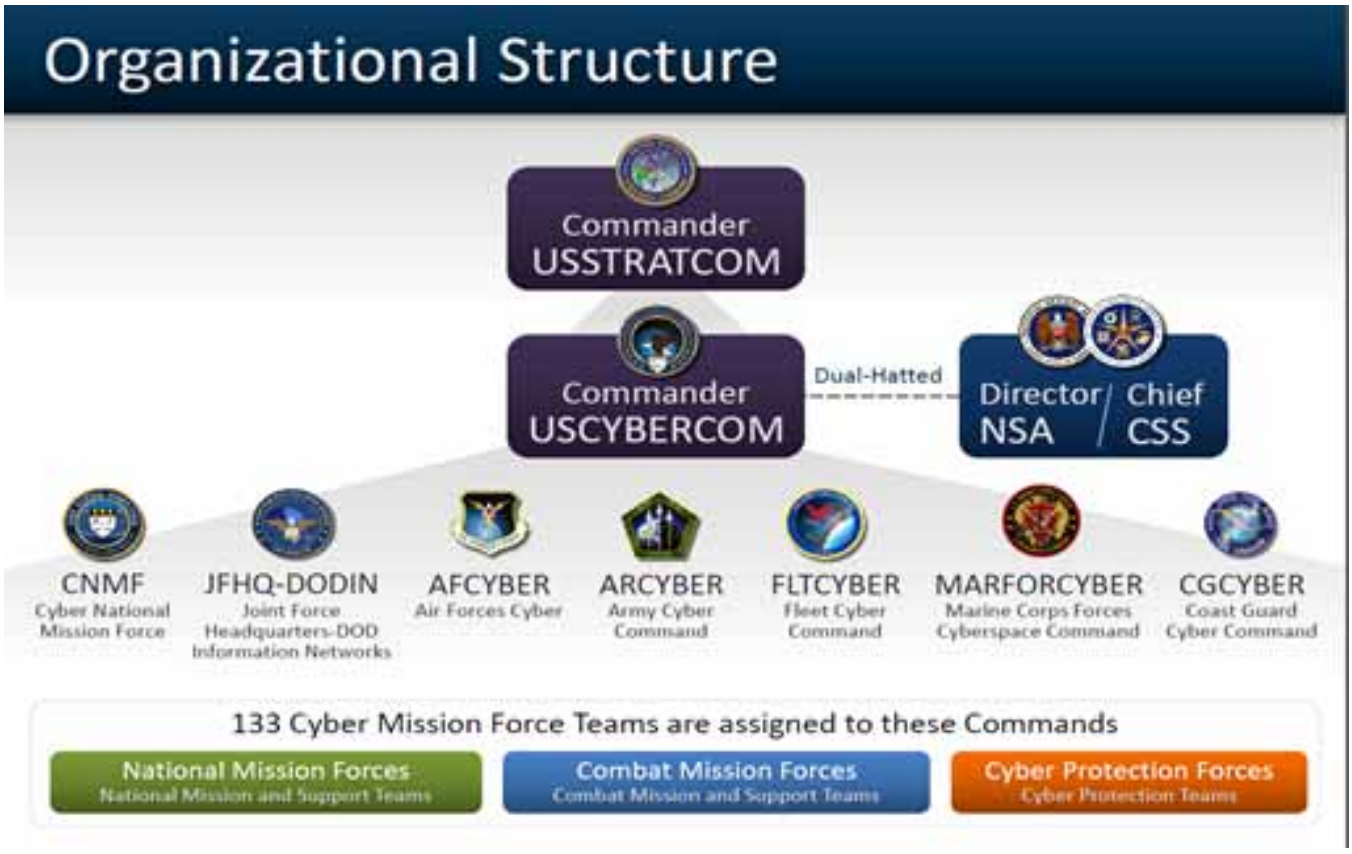


strategy, the Department of Defense (DoD) has evolved its cyberspace objectives over time. Milestones included the 1998 establishment of the Joint Task Force for Computer Network Defense, the 2004 stand-up of the Joint Task Force – Global Network Operations (whose missions were focused on defensive operations), and the 2005 establishment of the Joint Functional Command for Network Warfare (whose missions were focused on offensive cyber operations). The culmination of this evolution occurred in 2010 with the stand-up of U.S. Cyber Command, which, along with its subordinate elements, is now the nation's warfighting arm in cyberspace.

U.S. Cyber Command is now the nation's warfighting arm in cyberspace.

A sub-unified command under U.S. Strategic Command, U.S. Cyber Command (USCYBERCOM) is led by Admiral (USN) Michael Rogers, who is also dual-hatted as the Director of the National Security Agency (NSA). The Command's three lines of operations are to provide mission assurance for DoD operations and defend the DoD information environment; to support joint force commander objectives globally; and to deter or defeat strategic threats to U.S. interests and critical infrastructure. Full-spectrum military cyberspace operations are intended to enable actions in all domains, ensuring U.S. and allied freedom of action in cyberspace and denying the same to adversaries. [Editor's Note: Since this article was submitted, President Trump has approved a plan to elevate USCYBERCOM to full combatant command status, a move anticipated for months. This will give it more autonomy, power, and guaranteed funding, according to a story by Nancy Youssef in the August 19-20, 2017, edition of *The Wall Street Journal*. According to the same source, Trump stated he may boost the stature of the Command further by severing its ties with NSA, another long-rumored but more controversial effort. After promulgating his decision by executive order, in a separate statement the President said, "The elevation of United States Cyber Command demonstrates our increased resolve against cyberspace threats and will help reassure our allies and partners and deter our adversaries." A formal separation will not occur until a review is completed and SECDEF James Mattis has the opportunity to nominate another 4-star commander, according to the Pentagon.]

The Command includes six operational-level headquarters elements (Army Cyber Command, Fleet Cyber Command, Air Force Cyber, Marine Corps Forces Cyberspace Command, Joint Forces Headquarters – Department of Defense Information Network, and Cyber National Mission Force),



plus U.S. Coast Guard Cyber Command, a component of the Department of Homeland Security (DHS). USCYBERCOM's action arm is the Cyber Mission Force (CMF), which is continuing to build to a total of approximately 6,200 military and civilian personnel organized into 133 teams allocated against the three primary missions: Defend the Nation, Support the Warfighter, and Defend DOD Networks. Of these 131 teams, 21 are allocated to the Defend the Nation mission, the main objective of which is to defend the U.S. by identifying adversary activity, blocking attacks, and maneuvering to defeat them; 44 are allocated to the Support the Warfighter mission, which conducts military cyberspace operations in support of the joint warfighter; and 68 are dedicated to defending Department of Defense information networks and protecting DODIN priority missions.

The USCYBERCOM Commander's vision is embodied through three core pillars: Motivated by Mission, Powered through Partnerships, and Oriented toward Outcomes.

The USCYBERCOM Commander's vision is embodied through three core pillars: Motivated by Mission, Powered through Partnerships, and Oriented toward Outcomes. The CYBERCOM team is motivated by mission supporting three main command objectives: ensure DoD mission assurance, deter and defeat strategic threats to U.S. interests and infrastructure, and achieve joint force commander objectives. The four imperatives central to mission accomplishment are: defend the nation's vital interests in cyberspace, operationalize the cyber mission set, integrate cyberspace operations in support of joint force objectives, and accelerate full-spectrum capacity and capability development. Three lines of effort supporting command mission objectives are to protect U.S. cyberspace interests, project power in and through cyberspace, and partner with the interagency and other nations.

DOJ and FBI are the lead for investigation and enforcement, DHS is the lead for protection of the homeland, and DoD is the lead for national defense.

The second core pillar, Powered through Partnerships, recognizes that USCYBERCOM cannot successfully execute its mission without partnerships. No one department, agency, or even country has all of the answers to the complexities of the cyber domain. The command recognizes that only through the strengths of all can it tackle these complex threats. It partners with other departments, agencies, allies, academia, industry, and other actors because the nation's cybersecurity requires a collaborative team approach. Partners within the U.S. federal government include but are not limited to the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and DoD. Indeed, these agencies' national roles and responsibilities are symbiotic. DOJ and FBI are the lead for investigation and enforcement, DHS is the lead for protection of the homeland, and DoD is the lead for national defense.

The cyberspace operational environment is complex. Understanding this complexity is a cornerstone of the USCYBERCOM mission. There are many layers that underpin this environment including the cyber-personal, plus logical and physical layers. Each layer requires discovery and analysis by a highly trained workforce. Securing and operating cyberspace is truly a global challenge and requires a team approach.

The third core pillar, Oriented toward Outcomes, underscores USCYBERCOM's commitment to build increased capacity and technical capabilities that will improve joint force commanders' operational outcomes by integrating cyberspace operations into conventional air, land, and sea operations and providing contingency support. Collaboration, sharing, collective incident response, deterring, attributing, building capacity and capabilities, and a robust training and readiness program are all part of improving operational outcomes.

USCYBERCOM is committed to the concept embodied in the adage "fight like you train." Cyber Flag, Cyber Guard, and Cyber Knight are USCYBERCOM-led exercises. Cyber Flag fuses attack and defense across the full

spectrum of operations. Cyber Guard practices a whole-of-nation response to a major incident that impacts U.S. critical infrastructure, and Cyber Knight is a joint cyberspace training exercise certification and validation event.

The 2017 Cyber Guard was co-led by USCYBERCOM, DHS, and the FBI. Participants from across the U.S. government, academia, industry, and allies rehearsed a whole-of-nation response to destructive cyber-attacks against U.S. critical infrastructure. During the exercise, for the second year in a row, USCYBERCOM hosted a "Multinational Day" which involved almost 45 participants from 22 different countries, including several NATO countries which were invited to observe the complex, advanced training environment. "The thing I would highlight is how important the coalition is to this effort," said Navy Admiral Mike Rogers, USCYBERCOM commander and Director of NSA/CSS. "This is not just a domestic issue in the United States. We all know this is a worldwide challenge. With the events of last year, certainly you can see the challenges are just getting tougher."

Cyberspace is unique, complex, and manmade. The broad principles of strategy and conflict still apply. Warfighting skills are critical to this domain.

Cyberspace is unique, complex, and manmade. The broad principles of strategy and conflict still apply. Warfighting skills are critical to this domain. U.S. Cyber Command is ready to defend the United States and its interests in the Digital Age.

[Author's Note: The views and opinions expressed in this paper and/or its images are those of the author alone and do not necessarily reflect the official policy or position of the U.S. Department of Defense (DoD), U.S. Cyber Command (USCYBERCOM), or any agency of the U.S. government. Any appearance of DoD visual information for reference to its entities herein does not imply or constitute DoD endorsement of this authored work, means of delivery, publication, transmission, or broadcast.]

CDR (USNR) Catherine S. (Cassie) Deppa is the Senior Intelligence Officer assigned to the NSA/USCYBERCOM Combined Action Group, U.S. Cyber Command, at Fort George G. Meade, MD. In this position, she provides executive-level intelligence support to the Director of NSA and the CYBERCOM Commander. She received her commission upon graduation from American University with a BA in Russian and Soviet Area Studies. She has served in a variety of Naval cryptologic/information warfare commands and other diverse assignments including government and private sector positions. She has been assigned to the Naval Security Group Activity, Northwest, VA; the Naval Security Group Activity, Hanza, Okinawa; the Naval Reserve Security Group Activity, Orlando, FL; and the U.S. Special Operations Command, Tampa, FL. CDR Deppa also served as a Naval Reserve Officer Canvasser Recruiter for Atlanta, GA, and a Naval Reserve Mission Manager for HQ, Naval Reserve Security Group Command, at Fort Meade. Since 2005 she has held an NSA computer scientist position and led two profitable small businesses. Prior to her current assignment, CDR Deppa served as CYBERCOM J2P Deputy Plans Division Chief, J2P Europe Intelligence Planning Team Leader, J25 Special Projects Intelligence Planning Team Leader, J23 Counterterrorism Intelligence Team Leader, and J23 Intelligence Operations Officer, in which she supported U.S. Central Command and U.S. Africa Command cyber planning and operations in support of the Global War on Terror.

Alleged Chinese Cyberspies: An American Dilemma

by Dr. William E. Kelly

OVERVIEW

The issue of cyber spying directed toward the United States is not new. Allegations have been made for a long time. However, what is new is that in May 2014 the U.S. government for the first time indicted and publicly identified a number of Chinese state officials for espionage directed at American private enterprises involving hacking. The indictment is a complicated matter having potential economic, political, and military ramifications. Hence, the purpose of this article is to analyze the complexities of this important indictment relating to a Chinese-American relationship.

In May 2014 the U.S. government for the first time indicted and publicly identified a number of Chinese state officials for espionage directed at American private enterprises involving hacking.

THE INDICTMENT

On May 19, 2014, United States Attorney General Eric Holder held a press conference where he announced a U.S. indictment against five identified officers of the People's Republic of China, accusing them of engaging in cybersecurity violations from China directed against various American business entities. The charges emanated from a federal grand jury in Pittsburgh, PA. At this press conference it was also noted that in his 2013 State of the Union address, President Obama noted the seriousness of such a threat and here was an example of it as indicated by the indictment.[1] Alleged attempts at cyber spying obviously are not new. One source notes, however, that "while many countries engage in industrial espionage China has long been among the most aggressive collectors of economic secrets—both online and off, experts say," and it is assumed that many countries have engaged in it.[2]

Mr. Holder's announcement was somewhat historically important, however, because the indictment represents the first ever known charges against state officials allegedly engaging in cybercrime against the United States operating out of an office in China. In fact, the FBI issued "wanted" photos of the five Chinese officials. Another interesting aspect of the indictment was the accusation that the spying by the Chinese was directed against private businesses as opposed to strictly military targets. In his press conference Mr. Holder was quoted as indicating:

> When a foreign nation uses military or intelligence resources and tools against an American executive or corporation to obtain trade secrets or sensitive business information for the benefit of its state-owned companies, we must say, "enough is enough."
>
> The indictment makes clear that state actors, who engage in economic espionage, even over the Internet from faraway offices in Shanghai, will be exposed for their criminal conduct and sought for apprehension and protection in an American court of law."[3]

Another interesting aspect of the indictment was the accusation that the spying by the Chinese was directed against private businesses as opposed to strictly military targets.

Mr. Holder was followed in his presentation by the Assistant Attorney General for National Security, John Carlin, who described the hacking as criminal. He was quite specific in identifying the source of hacking as emanating from Unit 61398 located in Shanghai and noted that for the first time the faces and names of the individuals responsible for the hacking are identified. He noted that in the past, whenever the United States

expressed concerns to the Chinese government, it responded by challenging the U.S. to provide hard evidence that would stand up in court and today we are doing that. He indicated that members of the Chinese unit involved in the spying were "…stealing the fruits of our labor."[4]

TARGETS

Government officials naturally assume that hacking of their information by foreign countries usually focuses on military and defense matters. However, U.S. officials were quick to point out that the Chinese hacking in this instance was focused on private business categories of information designed to give the Chinese an economic advantage. Some of the American private industries identified by the FBI as having been subject to illegal Chinese hacking activities included: Westinghouse Electric Co. (Westinghouse); U.S. subsidiaries of SolarWorld AG (SolarWorld); United States Steel Corp. (U.S. Steel); Allegheny Technologies, Inc. (ATI); the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union (USW); and Alcoa, Inc. The FBI noted that information obtained from these companies would be advantageous to Chinese state-owned industries regarding their competitors and give them an economic advantage over them.[5]

TECHNIQUES USED BY THE CHINESE

Apparently, it was somewhat easy for the Chinese to hack into the American private firms with the intention of gaining access to information considered important to them. One source describes these Chinese techniques as mundane, such as tricking employees of the American firms into opening email attachments or clicking on websites. It also suggests that more effective antivirus software might have been helpful in protecting those companies subjected to the hacking. The source notes:

> "The U.S. says the break-ins were more Austin Powers than James Bond." In some cases, the government says, the hackers used "spear-phishing"—a well-known scam to trick specific companies or employees into infecting their own computers.
>
> The hackers are said to have created a fake email account under the misspelled name of a then-director of Alcoa and fooled an employee into opening an email attachment called "agenda.zip," billed as the agenda for a 2008 shareholders' meeting. It exposed the company's network. At another time, a hacker allegedly emailed company employees with a link to what appeared to be a report about industry observations, but the link instead installed malicious software that created a back door into the company's network."[6]

EFFECT ON AMERICAN NATIONAL SECURITY

Computer hacking of private industry in the United States by foreign governments obviously poses a threat to U.S. security. For example, the potential to access vital information about a corporation or private entity which is involved in sometimes providing items needed by the defense establishment gives a foreign country important information about the capability of the company to provide the items. In addition, knowing the names and roles of individuals associated with a private company involved in defense work provides the hacking country with possible capabilities of the company to render particular services associated with the national security of the United States. Hence, when the Chinese engage in hacking into private American enterprises it is probable that their defense and military capabilities will be increased as a result of knowledge gained from these efforts. As noted in his press conference on May 19, 2014, Holder pointed out, "Our economic security and our ability to complete fairly in the global marketplace are directly linked to our national security."[7]

When the Chinese engage in hacking into private American enterprises it is probable that their defense and military capabilities will be increased as a result of knowledge gained from these efforts.

REACTION OF THE CHINESE

As expected, the Chinese reaction to the U.S. indictment was one of criticism, denial, and suggestive of the United States as being a country that itself engages in the type of cyber-attack that it accused the Chinese of doing. "From WikiLeaks to the Snowden case, U.S. hypocrisy and double standards regarding the issue of cyber-security have long been abundantly clear," was the view presented by the Chinese Defense Ministry on its website.[8]

The source also noted the possibility of the Chinese government indicting Americans for their activities directed toward the Chinese in the area of cybersecurity.

In addition, this source suggested that the U.S. indictment might lead to a chilling effect on Chinese-American relations.

China's use of economic espionage can be attributed in part to its drive to modernize the country in recent decades, a transformation spearheaded by leaders including Deng Xiaoping.

In terms of the Chinese reaction another source noted the following:

> The charges of cyber espionage are "purely fictitious and extremely absurd," said Cui Tiankai, China's ambassador to the U.S. Other officials also reacted strongly to the indictment. In a meeting with the new U.S. ambassador to China, Max Baucus, China's Assistant Foreign Minister Zheng Zeguang warned that "China will take further action on the so-called charges by the United States," depending on how the situation proceeds. "The Chinese government and military and its associated personnel have never conducted or participated in the theft of trade secrets over the Internet," Zheng said to Baucus, per Chinese Foreign Ministry reports.[9]

However, in the discussion of hacking by countries, one should note a number of factors. For example, it is rather easy to find information indicating that China and the United States are not the only countries involved in hacking other countries. In fact, it is assumed that with advances in technology many countries are involved in it to one degree or another. In addition, the targets of hacking can be either economic or defense-related, or a combination of both. In explaining the reason for China's hacking a source noted: "China's use of economic espionage can be attributed in part to its drive to modernize the country in recent decades, a transformation spearheaded by leaders including Deng Xiaoping. The illicit acquisition of technology has helped China accelerate the process, bypassing problems that would otherwise require years of research and development to resolve, analysts say."[10]

Yet, while admitting that the United States does get involved in hacking, the American view is that it does not do it to enhance any advantage for its private domestic companies. However, its position is that the Chinese do it for a variety of reasons and certainly one of those reasons is to enhance the value of its state-owned industries and to give these industries a competitive economic advantage when dealing with foreign companies, which in turn hurts private American businesses. How receptive the American view is would seem to be an open question as some might say that any type of hacking by a country helps it in a variety of ways, domestic as well as defense-wise. In fact, after the indictment by the United States, the *China Daily* published an interesting article strongly suggesting that indeed the United States had engaged in industrial hacking for its own commercial benefit:

> Edward Snowden's revelations about the U.S. National Security Agency's surveillance programs let the whole world know that the U.S. is the biggest cyber spy; perhaps that is why it is so desperate to point a finger at China.
>
> According to Snowden's revelations, U.S. institutions have long been involved in large-scale and organized cyber theft as well as wiretapping and surveillance activities against foreign political leaders, companies, and individuals, and the intelligence it has obtained naturally includes a large number of business secrets. People cannot help but ask: Do all those countries, enterprises, institutions, and individuals around the world pose a threat to U.S. national security?
>
> In 1999 the European Parliament conducted a two-year investigation into U.S. intelligence agencies' theft of European countries' business secrets. It published a 200-page report on July 11, 2001, which concluded that the U.S. had been stealing European countries' business intelligence on a large scale for a long time. This information was handed over to the U.S. companies, helping them obtain enormous commercial advantages.
>
> The report by the European Parliament gave a large number of examples. For example, the National Security Agency provided Boeing and McDonnell Douglas with the negotiations that took place between Airbus and Saudi Arabia, the U.S. companies finally winning a $6 billion contract. For the same reason the French electronics company Thomson lost out on a $1.4-billion deal to the U.S.'s Raytheon Corporation.

In addition to the European countries, the report also listed a number of cases concerning the U.S.'s commercial espionage activities in countries such as Japan.[11]

As a result of the indictment, China has indicated that it will not cooperate in a joint venture with the United States regarding cybersecurity.

POSSIBLE EFFECTS OF THE INDICTMENT

Besides denial of the charges made by the United States against the Chinese government, there could be some other possible effects. For example, as a result of the indictment, China has indicated that it will not cooperate in a joint venture with the United States regarding cybersecurity. Secondly, one source noted that the indictment might force China to engage in more attempts to hide its cyber-attacks.[12] Of course, the indictment of the Chinese might be a wakeup call to the United States to work more diligently to protect its own cybersecurity assets. However, it should not be expected that the indictment will stop China or for that matter other countries from continuing with their attempts to engage in cyber-attacks against the United States. Some might rightfully ask why the Chinese should stop hacking. After all, the rewards to their country of continuing to hack far outweigh the criticism of the American government and its indictment.

CHANCES OF CONVICTION

The chances of a conviction of the five Chinese officials who were indicted are not good for a variety of reasons. For example, it would not be difficult to suggest that indeed the United States has hacked into the private affairs of its friends and foes, and this would suggest hypocrisy on the part of the United States. Pushing this indictment to the extent that more judicial action comes about might be embarrassing to the United States because matters about its hacking of other countries would become more public. Just by considering the Snowden revelations the United States might seem to be at a disadvantage in its case against the Chinese. In addition, it might be possible to suggest that other countries which have been subjected to cyber intrusion by the United States could file charges against Americans who helped their government in a similar fashion as the Chinese are alleged to have done. For example, Sean Lawson, a professor of public policy at the University of Utah, had some interesting quotes about the results of the U.S. indictment of the Chinese officials by indicating, "This could potentially open U.S. officials to similar charges, not just in China but other countries as well. Brazil could turn around and say:

> 'If you start charging foreign officials for cyberespionage against companies, maybe we'll do the same to officials at the NSA'."[13]

In addition, Eric King, who teaches at the London School of Economics, indicated: "If China wants to start prosecuting those who hack their infrastructure, NSA employees could be arrested on the exact same legal justifications as the Chinese who have been put on the FBI's most-wanted list."[14] One source notes that the U.S. laws violated by the Chinese include the Economic Espionage Act and the Computer Fraud and Abuse Act, but also quotes an Indiana University legal cyber security expert as noting:

> The U.S. government knows the likelihood of successfully prosecuting these individuals for violating U.S. criminal law is virtually nil because the cooperation of the Chinese government would be necessary for the U.S. government to gain custody and conduct a criminal trial in the U.S. … This move is really not about attempting to faithfully execute these laws.[15]

THE FUTURE OF HACKING

The U.S. indictment of Chinese officials in May 2014 is unique because it is the first time that such an indictment was directed toward specific individuals working for their government and alleged to have been involved in hacking our private industries. Although it is difficult to indicate what the future holds as a result of the indictment by the U.S. government against five Chinese government officials, it is possible to make some predictions. First, the chances of a conviction are not good considering the denial of the Chinese and their unwillingness to cooperate in the matter. Their suggestion that the United States itself is engaged in similar activities lessens this cooperation. Second, the obvious advantages to their country of continuing such hacking implies that they will not stop such activity. Third, the charge by the Americans may cause the Chinese to look for new, more sophisticated ways of securing information by cyber means.

The charge by the Americans may cause the Chinese to look for new, more sophisticated ways of securing information by cyber means.

For the United States the indictment is a public reminder that we must be continually on guard for such intrusions and that we must work more diligently to make it difficult

for Chinese hacking or any type of hacking of our resources to come about. In the American private sector the indictment is a call for a revamping of security measures designed to make it difficult for an unauthorized person or country to obtain its vital information. It is also a suggestion that both the private sector and the public sector must cooperate more fully to protect mutual interests. This means that more of our resources must be devoted to the challenge that cyber intrusions pose to our national security and domestic progress.

NOTES

[1] Eric Holder, May 19, 2014, "Attorney Justice Eric Holder Speaks at Press Conference Announcing U.S. Charges Against Five Chinese Military Hackers for Cyber Espionage," Washington, DC, May 19, 2014, http://www.justice.gov/iso/opa/ag/speeches/2014/ag-speech-140519.html. Accessed May 23, 2014.

[2] Charles Riley, May 20, 2014, "China's Long History of Spying on Business," http://money.cnn.com/2014/05/20/news/china-espionage-business/index.html. Accessed June 1, 2014.

[3] Eric Holder, May 19, 2014.

[4] John Carlin, May 19, 2014, "Assistant Attorney General for National Security John Carlin Speaks at Press Conference Announcing U.S. Charges Against Five Chinese Military Hackers for Cyber Espionage," http://www.justice.gov/nsd/opa/pr/speeches/2014/nsd-speech-140519.html. Accessed May 29, 2014.

[5] U.S. Department of Justice, Office of Public Affairs, May 19, 2014, "U.S. Charges Five Chinese Military Hackers with Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," http://www.fbi.gov/pittsburgh/press-releases/2014/u.s.-charges-five-chinese-military-hackers-with-cyber-espionage-against-u.s.-corporations-and-a-labor-organization-for-commercial-advantage. Accessed June 5, 2014.

[6] Jack Gillum and Eric Tucker, May 20, 2014, Associated Press, *San Jose Mercury News*. Posted May 20, 2014; 42: 58 MT 2014. Accessed May 29, 2014.

[7] Eric Holder, May 19, 2014.

[8] Bill Chappel, May 20, 2014,"In China, Anger at U.S Hacking Charges And Claims of Hypocrisy," http://www.gpb.org/news/2014/05/20/in-china-anger-at-u-s-hacking-charges-and-claims-of-hypocrisy.

[9] Danielle Wiener-Bronner, May 20, 2014, "Chinese Ambassador Calls U.S. Hacking Charges 'Absurd'," http://www.thewire.com/global/2014/05/china-reacts-to-hacking-charges/371266/. Accessed May 31, 2014.

[10] Charles Riley, May 20, 2014, "China's Long History of Spying on Business."

[11] *China Daily*, May 28, 2014, "US' INDUSTRIAL ESPIONAGE," http://www.china.org.cn/wap/2014-05/28/content_32513808.html. Accessed June 1, 2014.

[12] Sara Sorcher, May 27, 2014, "Security Insiders: Cyberspying Indictments Will Not Stop China From Hacking U.S. Businesses," *National Journal*, http://www.nationaljournal.com/defense/insiders-poll/security-insiders-cyberspying-indictments-will-not-stop-china-from-hacking-u-s-businesses-20140527. Accessed May 29, 2014.

[13] Andy Greenberg, May 19, 2014, "U.S. Indictment of Chinese Hackers Could Be Awkward for the NSA," http://www.wired.com/2014/05/us-indictments-of-chinese-military-hackers-could-be-awkward-for-nsa/. Accessed June 6, 2014.

[14] Ibid.

[15] Indiana University, May 19, 2014, "Cyber Espionage Indictment of Chinese Officials: IU Experts Comment," http://www.newswise.com/articles/cyber-espionage-indictment-of-chinese-officials-iu-experts-comment. Accessed May 27, 2014.

Dr. William E. Kelly earned his PhD degree from the University of Nebraska. His awards include being selected three times as the Outstanding Political Science Teacher at Auburn University by Pi Sigma Alpha, a Mortar Board Favorite Teacher of the Year Award at Auburn, and a teaching award from the American Political Science Association. He has also been nominated for the College of Liberal Arts as the outstanding advisor as well as by his department for an alumni professorship in political science. In addition, he has been nominated three times by his department as the outstanding teacher in the College of Liberal Arts. He has taught at military bases, community colleges, and a private religious college. Dr. Kelly teaches American government and criminal justice and also serves as the political science internship coordinator. He has published in The Journal of Education and Psychology, The New Review of East-European History, Public Sector, The Journal of the Alabama Academy of Science, *and* South Arkansas Historical Journal. *In addition, he has published over fifty book reviews and his review work has appeared in* Military Intelligence, Perspectives on Political Science, The American Political Science Review, The Journal of Politics, *and* American Intelligence Journal.

Social Media, Publicly Available Information, and the Intelligence Community

by COL (USA) Steven C. Henricks

The collection of information is the foundation of everything that the Intelligence Community does.

— Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction[1]

A "smart" government would integrate all sources of information to see the enemy as a whole… [T]he importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to "connect the dots."

— Final Report of the National Commission on Terrorist Attacks Upon the United States[2]

Social Media has taken the world by storm, with millions of users logging on every day and posting information for the world to see. [Author's Note: I have taken the liberty to write this term in upper case throughout to highlight its centrality to my argument.] While most of this publicly available information on Social Media is benign, some of it can reveal intelligence about those who desire to harm the United States and its citizens. The U.S. Intelligence Community (IC) must make use of this treasure trove of information, yet perceived uncertainty in the law and policy unfortunately leaves the IC reluctant to fully engage this vital information source.

The U.S. Intelligence Community (IC) must make use of this treasure trove of information, yet perceived uncertainty in the law and policy unfortunately leaves the IC reluctant to fully engage this vital information source.

This article describes a framework of legal and policy considerations which allows the IC to collect and review publicly available information that resides on Social Media. First, the article examines the World Wide Web and Social Media. Next, it reviews legal considerations applicable to the IC's collection of information found on Social Media. Third, it describes a legal framework that allows for the collection, analysis, and dissemination of publicly available information found on Social Media relevant to threats against the U.S. and its citizens. The article concludes by noting that, if the IC neglects to search fully for, collect, and use intelligence found within publicly available information on Social Media, this amounts to not adequately meeting the most basic intelligence responsibility: to search proactively for threats.

THE WORLD WIDE WEB AND SOCIAL MEDIA

The Surface Web, The Deep Web & The Dark Web

The World Wide Web (the Web)[3] was, is, and will remain a murky place, but always a place full of information awaiting discovery. Search engines, like Google or Bing, help us shine a beacon on the Web's opaque waters by aiding in our online search for information (imagine all the webpages we would never know about without search engines). These search engines rely on a process called indexing.[4] If Google, Bing, or some other standard search engine can index web information, that information becomes retrievable by the search engine—making it part of the Surface Web.[5]

Take, for example, Google. First, Google lets loose its information-seeking robots, called Googlebots, on the Web. These Googlebots systemically troll for webpages, find them, and upload them.[6] Second, Google relies on two different sets of servers to keep track of the webpages captured by a Googlebot: Index Servers and Document Servers.[7] Index Servers act like the local library's card catalogue system—listing webpages and what they contain, while Document Servers store the captured webpages and their webpage addresses in their entirety.[8]

This information sits in the Google servers waiting for a user to access it by typing a query into the search engine. When entered, a query hits the Google Web Server, which directs it to Google's Index Servers. The Index Servers try to match the query's search terms with results in the index. Hits are forwarded to Google's Document Servers, which retrieve the stored, responsive webpages and send the Internet link for that webpage to the user (along with summaries to show how a webpage matches the query), all in less than a second.[9]

Indexing captures a staggering amount of information but, relative to all the information available on the Web, indexing only accounts for approximately four to five percent of overall web information.[10] Consider the following example: A Google user wants to know if the State of Kansas currently incarcerates Jane Doe. Despite the cleverest of queries submitted to the Google search engine, the search results do not provide a definitive answer. The search results do, however, provide a link to the Kansas Department of Corrections' (KDOC) webpage. The KDOC webpage, in turn, provides a search box where the user can enter information about Jane Doe to determine Doe's KDOC status, including release dates and infractions while imprisoned.[11]

The Dark Web exists as part of the Deep Web, and has earned its ominous name both because of the difficulty for users to access it and for much of the activity that occurs within it.

The Jane Doe example illustrates the difference between the Surface Web and the Deep Web. Google can index the information found on the KDOC's webpage, but a Googlebot cannot take that next step and capture information about Jane Doe found within the KDOC's records, which are accessible only via the KDOC's webpage. The KDOC's webpage constitutes part of the Surface Web, while Jane Doe's KDOC status, accessible via KDOC's search box, exists in the Deep Web below the indexable surface. Further illustrative examples of information and services found in the Deep Web include medical records, legal documents, databases, chat servers, academic journals, and other information (including parts of Social Media) that require at a minimum extra search tools, internal secure logins, or permissions to access.[12] The Deep Web, then, constitutes the unindexable part of the Web, even though both the Surface Web and much of the Deep Web remain accessible through a standard web browser.[13] Parts of the Dark Web, discussed next, stand as the exception to standard web browser access.

The Dark Web exists as part of the Deep Web, and has earned its ominous name both because of the difficulty for users to access it and for much of the activity that occurs within it. Consisting of at least 30,000-40,000 websites intentionally hidden behind heavy encryption and special access tools (such as non-standard web browsers), illicit activity abounds.[14] A sampling of this activity includes child pornography and exploitation, illegal marketplaces,[15] and hacking tools and tutorials.[16] The Dark Web, however, also provides a free speech forum where dissidents or journalists can post and exchange ideas and information that oppressive governments might otherwise suppress.[17] For this reason, the Dark Web represents an eternal tradeoff between good and evil.

The Onion Router (TOR) presents the best known method to access the Dark Web.[18] Relying on a system of volunteer nodes and heavy encryption, a user need only download TOR software (accessible from the Surface Web and first developed by the U.S. Naval Research Laboratory[19]) to begin a possibly anonymous and untraceable journey into the Web's deepest recesses. The Onion Router accomplishes this by the volunteer nodes making a random circuit for TOR users, and separately encrypting every node communication within the circuit. The node-to-node layered encryption is designed to prohibit tracing back to where the initial communication originated or who communicated it.[20]

Social Media operates on all Web levels, and Facebook provides a prominent example. A search engine may tell us if someone has a Facebook account, and our review of what that account contains may delve into the Deep Web (depending on how a Facebook user sets privacy settings) as we try to access Facebook photos and postings. Perhaps as a marketing strategy to appeal to users' privacy desires, or out of a sense of civic obligation, or both, Facebook also allows access from the Dark Web with TOR software. On October 31, 2014, Facebook announced that TOR users could now use Facebook anonymously.[21] One simply needs to download TOR software and then connect to Facebook at https://facebookcorewwwi.onion/.[22]

Although Facebook did not state why it granted this anonymous access, such a gateway allows a work-around against those countries which prohibit or frustrate Facebook access, such as Cuba, Iran, China, and North Korea.[23] Downplaying the anti-government angle, however, a Facebook consultant explained that a user still has to log into his/her Facebook account on the Surface Web, but doing so from the TOR network offers more privacy. "It's not so much protecting people from governments, but protecting from people who are spying on communications—that could be anyone from criminals

to marketers."[24] The Onion Router does this by blocking access to the user's operating machine (that first accessed TOR's network of random nodes) and therefore blocking the user's location and Web browsing habits.[25]

WEB 2.0: The Rise of Social Media and User Interaction

In the initial days of the Web, a user's web interface was both static and relied mostly on desktop software. Users would log onto their computers, open their browsers to access the Internet, then begin "simply acting as consumers of content."[26] Craigslist is a classic example of a Web 1.0 website, because users do not enjoy ways to interact actively with the online content.[27] The term "Web 1.0" describes this static, desktop- based model of Web usage and, as the Craigslist example shows, many Web 1.0 websites remain on the Web today.

In 1999 information architect and author Darcy DiNucci presciently predicted the coming of Web 2.0, writing:

> The Web we now know, which loads into a browser window in essentially static screenfuls, is only an embryo of the Web to come. The first glimmerings of Web 2.0 are beginning to appear, and we are just seeing how that embryo might develop…
>
> The Web will be understood not as screenfuls of texts and graphics but as a transport mechanism, the ether through which interactivity happens.[28]

DiNucci went on to envision correctly our Web access expanding from our computer desktops to a wide variety of consumer products, including televisions, cell phones, vehicle dashboards, and kitchen appliances.[29]

Looking at the Web as a business, entrepreneurs and authors Tim O'Reilly and John Battelle observed that the term "Web 2.0" describes a gravitational core for successful Web business models.[30] After the "dot-com" collapse of the late 1990s, the inevitable shakeout showcased websites which capitalized on Internet applications instead of software tied to a personal computer. Google serves as a typical example of "the Web as a Platform" because the user never need install an upgrade.[31] Despite difficulties in providing a comprehensive definition of Web 2.0, a key component of this new, dynamic Web allows users to create content and access that content in ever new and clever ways.[32] Social Media serves as a primary method for users to dynamically interact with Web content.

The *Merriam-Webster Online Dictionary* provides a simple definition of Social Media: forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos).[33] That definition contains a host of different web capabilities, such as social networking, blogging, and bookmarking. Indeed, Social Media touches on at least eight different types of Web platforms, most of which overlap in their capabilities:

(1) Personal/Relationship Networks. The ubiquitous Facebook, LinkedIn, and romantic relationship networks offer extensive information about a user (in a user profile), allow the user to place communications and content on the Web (a wall and timeline), provide a private messaging function, and allow a user to share updates with the user's entire network of other platform users.

(2) Media Sharing Networks. Instagram, Flickr, YouTube, Vimeo, Vine, and Snapchat serve as primary examples of this kind of Social Media because a user must first upload a picture or video before providing captions or other information.

(3) Online Reviews. Popular websites where users go to read what other users have to say about a business or enterprise fit this category. Examples are Yelp and Urbanspoon.

(4) Discussion Forums. Reddit, Quara, and Dig offer the oldest type of Social Media—forums for users to examine any topic. These platforms offer anonymity because a user typically does not have to provide his/ real name to register or to post content.

(5) Social Publishing. This category covers a broad range of blogging activity, such as traditional blogs (WordPress and Blog) and microblogging/real-time interaction networks (Twitter, Medium, and Tumblr).

(6) Bookmarking Sites. Pinterest and Flipboard provide the best examples of this kind of Social Media, where users gather diverse information from across the Web and then save that information on their platform account for others to access.

(7) Interest-Based Networks. As the rubric states, these are networks devoted to specific interests and niches, such as last.fm for music lovers and Goodreads for book lovers.

(8) E-Commerce. With Amazon and smaller purchasing sites like Polyvore, the user can provide and read other prominently displayed user reviews, search for goods, and read what other users search for and purchase (trending items).[34]

What Social Media Can Reveal

The Pulitzer Prize-winning author Cormac McCarthy wrote in *Blood Meridian*, "Before man was, war waited for him. The ultimate trade awaiting its ultimate practitioner."[35] That same idea also applies to the Web and Social Media. For those inclined to share their thoughts, interests, and activities with anyone who may be interested, Social Media appeared to await discovery and use. The Pew Research Center reports almost two-thirds of Americans now use Social Media, with 90 percent of young adults (18- to 29-year-olds) maintaining a Social Media presence.[36] Worldwide, of the 7.2 billion souls that now inhabit the earth, 3.1 billion use the Internet and just over 2 billion maintain active Social Media accounts.[37] Facebook has almost 1.5 billion users, and Twitter has just over a quarter-billion active users producing half a billion tweets per day.[38]

With all this information output occurring, what type of content resides in Social Media for analysis by the Intelligence Community? The Federal Bureau of Investigation lists four uses of Social Media information relevant to the IC, ranging from pinpoint targeting to background:

(1) Detect. Social Media can help detect both positive and negative information. Positive information includes the ability to detect specific and credible threats and monitor adversarial situations. Negative information includes deception concerning intent or actions to mislead adversaries.

(2) Locate. Social Media can reveal the location of people and objects and provide information to analyze movements, vulnerabilities, and limitations.

(3) Develop. Social Media analysis can provide assessments for a given area of interest (the process of taking a sample from the larger domain and analyzing that sample to help gain a better understanding of the larger domain).

(4) Predict. Social Media can help predict both future actions by bad actors and how situations may develop by using trend, pattern, and other types of forward-looking analytics.[39] Academia, sometimes with industry partnership (and with a tip of the hat to Isaac Asimov and his science fiction *Foundation* series[40]), produce some truly fascinating work in this regard.[41]

LEGAL CONCERNS

General

To make use of the information available on Social Media, the Intelligence Community needs to do five things: collect it, store it, analyze it, distribute it, and synthesize it. This process raises several legal issues, such as whether individuals have a protected privacy interest over content they place on the Web via Social Media, whether the First Amendment allows the IC to keep records of what someone says and does on Social Media, and what other rules govern the IC in this process?

To make use of the information available on Social Media, the Intelligence Community needs to do five things: collect it, store it, analyze it, distribute it, and synthesize it. This process raises several legal issues.

The U.S. Congress, for one, wants this capability fully realized, declaring in 2006:

> Open-source intelligence (OSINT) is intelligence that is produced from publicly available information and collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.
>
> With the Information Revolution, the amount, significance, and accessibility of open-source information has expanded significantly, but the intelligence community has not expanded its exploitation efforts and systems to produce open-source intelligence.
>
> The production of open-source intelligence is a valuable intelligence discipline that must be integrated into intelligence tasking, collection, processing, exploitation, and dissemination to ensure that United States policy makers are fully and completely informed.[42]

Web 2.0 and Social Media fall squarely in the Information Revolution referenced by Congress. Unfortunately, some in the IC remain unsure of the legal and policy framework that allows them to collect this information, resulting in reluctance to use these authorities fully to support their mission to protect the United States and its citizens.

CONSTITUTIONAL CONCERNS

The Fourth Amendment[43]

The U.S. Constitution's Fourth Amendment protects against unreasonable searches and seizures by the government.[44] With noted exceptions, when a reasonable expectation of privacy exists in the place to be searched or item to be seized, the government must first obtain a warrant to make the search or seizure reasonable and therefore constitutional.[45] An initial question for any Fourth Amendment analysis accordingly turns on whether individuals possess a reasonable expectation of privacy.

Supreme Court precedent strongly suggests that Social Media users do not possess a reasonable expectation of privacy in their posted content which the public can view online. In *Katz v. United States*, Mr. Katz used a public phone booth with the phone booth door closed to place illegal bets over the phone.[46] The FBI had placed, without benefit of a warrant, a hidden electronic monitor on the outside of the booth to record what was said inside the booth.[47] The Supreme Court found that Mr. Katz did maintain a reasonable expectation of privacy in what he said in the telephone booth while on the phone, relying on this distinction:

> What a person knowingly exposes to the public, even in his own home or office, is not a subject of *Fourth Amendment* protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[48]

Although the case was decided in 1967, the quotation from *Katz* seems particularly relevant to untangling the Gordian knot of privacy and Social Media. If a Social Media user does not take steps to preserve Social Media content as private, then the public broadcast of that information on the Web removes any privacy expectation. In *United States v. Meregildo*, for example, a federal district court in New York's Southern District recognized that, when a user takes advantage of Facebook's different privacy settings, such actions could provide Fourth Amendment protection to the non-public content.[49] When, however, "a Social Media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment."[50]

Over thirty years after *Katz*, the Supreme Court in *United States v. Jones* again reviewed a case in which law enforcement officers attached an electronic device to something without the benefit of a properly executed warrant—in this case a Global Positioning System tracker to the car of Mr. Jones' wife.[51] The majority opinion relied on a common law trespass to conclude the government's actions violated the Fourth Amendment, observing that *Katz*'s reasonable expectation of privacy test did not supplant a long-standing Fourth Amendment concern to protect property.[52]

Jones is important for our purposes because of what Justice Sotomayor said in concurrence. The Justice wondered whether some types of information voluntarily disclosed to others should retain Fourth Amendment protections.[53] Her questions seemed to implicate Social Media and the Web without specifically mentioning them. However, Sotomayor carefully hedged her questions by limiting their scope, and did not go so far as to include information that is made available to all, just information provided to a third party.[54] By raising these questions, Justice Sotomayor signaled at least one Justice's willingness to reconsider past Supreme Court precedent, holding information given to third parties does not enjoy a reasonable expectation of privacy by the first party.[55] This issue—information held by a third party—is important as we consider what constitutes publicly available information.

The First Amendment

The First and Fourth Amendments protect different interests. The Fourth Amendment protects our privacy interests against the government seizing information under certain conditions. The First Amendment protects a host of other freedoms, such as our freedom of beliefs and speech, our right to assemble, freedom of the press, and our right to learn of ideas.[56] As law professor Daniel Solove explains, the Supreme Court has not yet answered how the First Amendment might apply to government information collection practices, but argues that such collection could have an improper chilling effect on many First Amendment rights.[57]

In the absence of such precedent, Professor Solove envisions three ways the First Amendment may offer protection when the government gathers information:

> (1) The First Amendment would not apply unless a reasonable expectation of privacy exists. In this scenario, the First Amendment relies exclusively on the Fourth Amendment to protect its interests when the government collects information.

(2) The First Amendment helps inform what is reasonable under the Fourth Amendment. In this scenario, the First Amendment still relies on the Fourth Amendment to protects its interests, but its principles help inform a court whether the government collection of information is reasonable, notwithstanding the existence or absence of a reasonable expectation of privacy.

(3) The First Amendment does not rely on the Fourth Amendment at all, and instead provides an independent basis to protect against overly intrusive government information collection practices.[58]

Solove goes on to argue that courts should adopt the third scenario, but justifies his arguments by noting the ease in which the government can obtain information by subpoena.[59] Although this article concerns itself with Congress' demand for the IC to obtain publicly available information without the need to use subpoenas or other legal processes, the IC should still maintain a heightened sensitivity to whether its actions cut too close to the First Amendment and other civil liberty concerns, as discussed next.

Other Legal Concerns

Three 1970s government investigations continue to impact the Intelligence Community today. Partly in response to alleged IC excesses that violated civil liberties, the

Table 1[65]

IC Element	Collection Mission	Mission Caveats	Collection Method
CIA	Info, FI & CI	None	Clandestine
DIA	Info, FI & CI	To Support National & Departmental Missions	Clandestine
NSA	Info, SII, FI & CI	To Support National & Departmental Missions	Clandestine
U.S. Military	Info, DI, DRI & CI	To Support National & Departmental Requirements	Clandestine
FBI	Info, FI & CI	To Support National & Departmental Missions Under AG Supervision & Regulation	Clandestine
ODNI	Info, I & CI	To Support ODNI, NCTC, & Other National Missions	Overtly or PAS
DHS	Info, I & CI	To Support National & Departmental Requirements	Overtly or PAS
DoS	Info, I & CI	To Support National & Departmental Requirements	Overtly or PAS
DEA	Info, I & CI	To Support National & Departmental Requirements	Overtly or PAS

Terms	Acronyms	Definitions
Counterintelligence	CI	Information gathered . . . to identify, exploit, disrupt, or protect against espionage, or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.
Clandestine	None	Not further defined. Generally understood to mean hidden or under false pretenses.
Defense Intelligence	DI	Not further defined.
Defense-Related Intelligence	DRI	Not further defined.
Foreign Intelligence	FI	Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.
Intelligence	I	Includes FI and CI (implying a broader definition than just FI and CI).
Information	Info	Not further defined.
Overtly	None	Not further defined. Generally understood to mean attributable actions.
Publicly Available Sources	PAS	Not further defined.
Signals Intelligence Information	SII	Not further defined.

Rockefeller Commission (more formally known as the President's Commission on CIA Activities Within the United States), the Church Committee (more formally known as the Select Committee to Study Governmental Operations with Respect to Intelligence Activities), and the Pike Committee (more formally known as the United States House Permanent Select Committee on Intelligence) investigated and produced numerous reports about the IC.[60]

These investigations and reports led to federal laws to curtail abuses of civil liberty done in the name of foreign intelligence and national security, such as the Foreign Intelligence Surveillance Act of 1978—originally enacted to regulate the electronic surveillance of United States Persons abroad.[61] Additionally, Presidents Ford and then Reagan published executive orders, resulting in Executive Order 12333, to govern the activities of the Intelligence Community's various members.[62] Finally, although not specifically aimed at the IC, the Privacy Act of 1974 also regulates how the executive branch collects and stores information about U.S. Persons.[63]

EXECUTIVE ORDER 12333, UNITED STATES INTELLIGENCE ACTIVITIES

Executive Order 12333, most recently amended in 2008, consists of 16 pages of dense writing, which lays out such things as intelligence collection missions and lawful collection methods for IC elements.[64] Table 1 on page 22 summarizes these collection missions and methods.

A review of the above information reveals three important points. First, the President charges the entire IC with a counterintelligence collection mission. That mission—to protect the United States against a host of activities tied to foreign powers or international terrorism—has no geographical limitation and thus provides authority to conduct such collection missions inside the United States in certain circumstances. Second, some elements of the IC may collect both intelligence and the presumably broader (but undefined) category of information, likewise with no geographic limitation. Third, every element of the IC may conduct such collection missions overtly or by using publicly available sources, while a few may also use clandestine methods. With these overarching principles in mind, Executive Order 12333 also provides the IC with further authorities and restrictions concerning collection applicable to Social Media.

First, Paragraph 2.7 of Executive Order 12333 authorizes the IC to enter into contracts to purchase goods or services from U.S. organizations.[66] This contracting authority is consistent with collecting information from publicly available sources because, as we saw above, Fourth Amendment precedent provides no reasonable expectation of privacy in information held by a third party. Second, Paragraph 2.9 of Executive Order 12333 prohibits (with certain exceptions) undisclosed participation by the IC in organizations within the United States.[67] Any participation must also not attempt to influence the organization or any of its members (also with limited exceptions).[68]

Third, Paragraph 2.3 contains significant limitations on the IC's ability to collect, retain, and disseminate information on U.S. Persons (wherever located), and requires all IC elements to use Attorney General-approved procedures.[69] Collecting publicly available information is one method Paragraph 2.3 specifically mentions that the Attorney General may approve.[70] Fourth, Paragraph 2.4 requires the IC to use the least intrusive means available when collecting information in the United States or against a U.S. Person.[71] The Attorney General's most recently approved guidelines are those for the FBI's domestic operations, which were approved in 2008, per Paragraph 2.3's directive.

THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS[72]

The Attorney General's Guidelines for Domestic FBI Operations (the Guidelines)[73] make clear the FBI should collect publicly available information from Social Media to protect the United States. Organizing FBI domestic information collection into three levels, the lowest level—assessments—may be done without any factual predicate to suspect wrongdoing, and only requires the assessment be tied to an authorized purpose (such as protecting the United States).[74] The first example the Guidelines give as proper assessment activity is collecting publicly available information.[75] To ensure the priority stands out clearly, the Guidelines go on to say, "[A]ssessment activities may involve proactively surfing the Internet to find publicly accessible websites and services through which recruitment by terrorist organizations and promotion of terrorist crimes is openly taking place."[76] Furthermore, just in case the Guidelines did not make the point strongly enough, they also state that obtaining publicly available information is of "relatively low intrusiveness" when determining if collectors are using the least intrusive means of collection.[77]

Given the emphasis the Guidelines place on publicly available information, they also provide a definition of the term: "[I]nformation that has been published or broadcast for public consumption is available on request to the public, is accessible on-line or otherwise to the public,

[and] is available to the public by subscription or purchase, . . ."[78] This definition is consistent with the *Katz/Meregildo* test of publicly available, but readers must take care to note that the public cannot access everything that resides online, as explained previously.

For example, information found on the Surface Web by a search engine would come from publicly available information. Information found on the Deep Web may or may not come from a publicly available source. If a user need only use a search box to find information, like in the KDOC example previously, such information continues to come from a publicly available source. If one sets his/her Facebook account postings for viewing by friends only, such actions would make this information no longer available from a public source, as explained in *Meregildo*.

The Dark Web presents an intriguing question of whether it presents a publicly available source of information. As the Surface and Deep Web show, the mere act of using an Internet browser to access the Web does not turn Web information private. Downloading TOR software to access the Dark Web seems no different than this, and information that becomes collectible after such a download would then originate with a publicly available source. This is true even though the information's creator may remain hidden from view behind encryption (making encrypted identity not available to the public). Additional acts taken to shield information from public view in the Dark Web, just as in the Deep Web, will likely make such information private.

THE PRIVACY ACT OF 1974

The Privacy Act of 1974[79] (the Privacy Act) recognizes that, as the federal government goes about its business,

it acquires a large amount of information about individuals.[80] To protect the integrity and privacy of this information, the Privacy Act places many requirements on the federal government when maintaining records that identify individuals. For example, the Privacy Act requires that executive branch agencies give public notice when maintaining any "system of records" that contain information protected by the Privacy Act.[81] Additionally, nestled in a sub-section of the Privacy Act lies this prohibition: agencies will not maintain a record on how an individual goes about exercising his or her First Amendment rights . . . "[82] Many Privacy Act requirements, however, do not apply when records are kept for a law enforcement purpose or a statute authorizes the collection of information.[83]

For this reason, the Guidelines make quick work of finding an applicable Privacy Act exception, saying collection activity performed pursuant to the Guidelines is either authorized by statute or is a law enforcement activity, or both. This conclusion passes the common sense test, for to give notice or follow many other Privacy Act requirements when collecting and analyzing information for possible threats against the United States would likely defeat the purpose of the investigation. Accordingly, federal appellate courts are willing to extend this law enforcement exception to IC activity. For example, in 1982, the Sixth Circuit Court of Appeals stated the law enforcement exception applies "to an authorized criminal investigation or to an authorized intelligence or administrative one."[84] More recently, in 2006, the Seventh Circuit Court of Appeals stated "the realm of national security belongs to the executive branch, and we owe considerable deference to that branch's assessment of matters of national security" when holding the FBI may keep records related to national security even in the absence of a current investigation.[85]

ADOPTING A POLICY TO COLLECT, ANALYZE, AND DISSEMINATE INTELLIGENCE DERIVED FROM PUBLICLY AVAILABLE INFORMATION FOUND ON THE WEB

As our review of Executive Order 12333 shows, Intelligence Community members (acting in their official capacities) can receive publicly available information in three ways: (1) they can buy it; (2) they can collect it themselves; or (3) another member of the Intelligence Community can give it to them. Perhaps because of uncertainty over a host of issues, such as the rules regarding collecting information on U.S. Persons, privacy, the First Amendment, and the Privacy Act, members of the IC remain uncertain how to fully engage the Web and Social Media. It is up to policymakers within the IC to overcome these concerns through education and the adoption of policies to fully encourage and require that its members look for relevant information in plain sight on the Web.

Accordingly, any policy or implementing guidance should address at a minimum the following topics:

(1) Ensure the collection is tied to a proper mission, as set forth in Executive Order 12333.

(2) Address whether the collection requires joining or participating in a U.S. organization. For example, one may need to create a Social Media account to view some publicly available information (e.g., posts that are available by request or by subscription). Regardless of a particular Social Media's terms of use to join, joining U.S.-based Social Media could trigger the requirements of Executive Order 12333,

Paragraph 2.9, requiring disclosure to the organization and other appropriate approvals.[86]

(3) Address if collection will seek information about a U.S. Person. If so, ensure that the collection, retention, and dissemination of that information is in accordance with the IC's element's Attorney General-approved guidelines.[87]

(4) Ensure the collection seeks to obtain publicly available information only. If the collection is the purchase of information held by a third party, absent a change in Supreme Court precedent this constitutes publicly available information. If the information sought resides on Social Media or otherwise on the Web, were any steps taken to shield the information from public view? If not, the information is publicly available.

(5) Determine if the information's collection will trigger any Privacy Act obligations. Coordination with the relevant legal and compliance offices can help determine (a) whether the storage of information triggers any of the Privacy Act's obligations; (b) whether reliance on the Privacy Act's law enforcement exception is appropriate as a matter of both law and policy; and (c) to what extent the policy will follow the Privacy Act prohibition against collecting information on the exercise of First Amendment rights.

(6) Implement a retention policy that includes a duty to review and delete collected publicly available information that proves not relevant or no longer relevant to any proper collection mission.

(7) Determine how and when collected or purchased publicly available information can be shared with others.[88]

(8) Square any policy specific to the Web and Social Media with Attorney General Guidelines applicable to the specific member of the IC.[89]

CONCLUSION

The Intelligence Community may legally collect and use publicly available information from the Web and Social Media, even when that information is about U.S. Persons. To avoid mission failure in identifying threats against the United States and its citizens, the IC must adopt a comprehensive policy that fully enables the collection and use of this source of information. The adoption and implementation of such a policy will provide the necessary guidance the IC requires to fully engage Social Media and the Web as intelligence sources.

NOTES

[1] *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* 351 (2005), https://fas.org/irp/offdocs/wmd_report.pdf.
[2] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* 401, 408 (2004), https://www.gpo.gov/fdsys/pkg/GPO-911REPORT/content-detail.html.
[3] The Internet and the World Wide Web are not synonymous. The Internet offers a network that allows any computer connected to the Internet to communicate with any other Internet-connected computer. Built on top of the Internet stands the World Wide Web platform, providing one means for connected Internet computers to share information. Email, by contrast, provides another Internet platform, but email typically is not part of the World Wide Web. *See* Abraham Reisman, MOTHERBOARD.VICE.COM, *The Web Is Not The Internet (You're Probably Getting That Wrong)*, http://motherboard.vice.com/blog/the-web-is-not-the-internet-you-re-probably-getting-that-wrong (July 17, 2012).
[4] *See* GOOGLE INSIDE SEARCH, *Crawling and Indexing*, https://www.google.com/ insidesearch/howsearchworks/ crawling-indexing.html (last visited January 20, 2016).
[5] *See* Kristin Finklea, CONGRESSIONAL RESEARCH SERVICE REPORT, *Dark Web*, https://www.fas.org/sgp/crs/misc/R44101.pdf (July 7, 2015) (hereafter *Dark Web*).
[6] *See* GOOGLEGUIDE: MAKING SEARCHING EVEN EASIER, *How Google Works*, http://www.googleguide.com/google_works.html (last modified February 2, 2007). If an individual or business does not want to wait for a Googlebot to locate a webpage, Google also accepts submissions of webpages and the corresponding webpage addresses for indexing. *See id*.
[7] *See id*.
[8] *See id*.
[9] *See id*.
[10] DONALD I. BARKER and MELISSA BARKER, INTERNET RESEARCH ILLUSTRATED C-4 (2013).
[11] *See* KANSAS DEP'T OF CORRECTIONS, *KASPER – Offender Population Search*, http://www.doc.ks.gov/kasper_old/index_html?YesNo=Please+Wait... (last visited November 28, 2016).
[12] *See generally Dark Web*, *supra* note 3.
[13] *See id*.
[14] *See generally* Kim Zetter, WIRED.COM, *DARPA Is Developing a Search Engine for the Dark Web*, http://www.wired.com/2015/02/darpa-memex-dark-web/ (February 10, 2015).
[15] The most famous Dark Web marketplace was the so-called Silk Road, before dismantling and prosecution by United States law enforcement.
[16] *See* Michael Chertoff and Toby Simon, CIGIONLINE.ORG, *The Impact of the Dark Web on Internet Governance and Cyber Security*, https://www.cigionline.org/sites/default/ files/gcig_paper_no6.pdf (February 2015).
[17] *See id*.
[18] *See id*.
[19] *See id*.

[20] Identification of TOR users usually occurs when a user inadvertently reveals personal information, although rumors continually surface in open source information hinting that the National Security Agency has cracked TOR. *See* generally Jason Koebler, MOTHERBOARD.COM, *How the NSA (or Anyone Else) Can Crack TOR's Anonymity*, http://motherboard.vice.com/read/ how-the-nsa-or-anyone-else-can-crack-tors-anonymity (November 19, 2014).
[21] *See* FACEBOOK.COM, *Making Connections to Facebook more Secure*, https://www.facebook.com/notes/protect-the-graph/making-connections-to-facebook-more-secure/1526085754298237 (October 31, 2014).
[22] Matthew Hughes, MAKEUSEOF.COM, *How You Can Officially Browse Facebook Over TOR*, http://www.makeuseof.com/tag/can-officially-browse-facebook-tor/ (November 6, 2014).
[23] *See id.*
[24] *See* David Lee, BBC.COM, *Facebook Sets Up "Dark Web" Link to Access Network via TOR*, http://www.bbc.com/news/technology-29879851, *quoting Dr. Steven Murdoch* (November 3, 2014).
[25] *See id.*
[26] Graham Cormode and Balachander Krishnamurthy, FIRSTMONDAY.ORG, *Key Differences Between Web 1.0 And Web 2.0*, http://firstmonday.org/article/view/2125/1972 (June 2, 2008).
[27] *See id.*
[28] Darcy DiNucci, *Fragmented Future*, PRINT, April 1999, at 32, http://www.darcyd.com/ fragmented_future.pdf.
[29] *See id.*
[30] John Battelle and Tim O'Reilly, WEB 2.0 CONFERENCE, *Opening Welcome: The State of the Internet Industry*, http://conferences.oreillynet.com/cs/web2con/view/e_sess/5854 (last visited November 28, 2016).
[31] *See generally id.*
[32] *See* David Best, BARION.NET, *Web 2.0: Next Big Thing or Next Big Internet Bubble, at* http://www.ibrarian.net/navon/paper/Web_2_0_Next_Big_Thing_or_Next_Big_Internet_Bubbl.pdf?paperid=9991672 (January 11, 2006).
[33] *Social Media Definition*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/social%20media (last visited November 28, 2016).
[34] *See* Olsy Sorokina, HOOTSUITE.COM, *8 Types of Social Media and How Each Can Benefit Your Business, at* blog.hootsuite.com/types-of-social-media (March 12, 2015).
[35] The complete quote: "It makes no difference what men think of war, said the judge. War endures. As well ask men what they think of stone. War was always here. Before man was, war waited for him. The ultimate trade awaiting its ultimate practitioner. That is the way it was and will be. That way and not some other way." CORMAC MCCARTHY, BLOOD MERIDIAN OR THE EVENING REDNESS IN THE WEST 248 (Modern Library Edition, Random House, 2001) (1985).
[36] *See* PEWINTERNET.ORG, *Social Media Usage: 2005-2015, at* http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/ (October 8, 2015).
[37] *See* JEFFBULLAS.COM, *33 Social Media Facts and Statistics You Should Know in 2015, at* http://www.jeffbullas.com/2015/04/08/33-social-media-facts-and-statistics-you-should-know-in-2015/ (last visited November 28, 2016).
[38] *See id.*
[39] *See* Patrick Marshall, GCN.COM, *Don't Look Now, But Everybody (CIA, DHA, etc.) Is Watching*, https://gcn.com/Articles/2012/04/02/Social-media-analytics-hits-privacy-line.aspx?Page=1 (March 28, 2012).
[40] Asimov begins his *Foundation* series with the idea that mathematics can predict the future in broad terms.
[41] Jaime Arredondo, Feng Chen, Ting Hua, Chang-Tien Lu, David Mares, Naren Ramakrishnan, and Kristen Summers, *Analyzing Civil Unrest through Social Media*, http://people.cs.vt.edu/naren/papers/80-84.pdf (last visited November 28, 2016); Jose Cadena, Gizem Korkmaz, Chris J. Kuhlman, Achla Marathe, Naren Ramakrishnan and Anil Vullikanti, *Combining Heterogeneous Data Sources for Civil Unrest Forecasting*, http://people.cs.vt.edu/naren/papers/multiple_data_sources_cu_asonam15.pdf (last visited November 28, 2016); Jamie Arredondo, Lisa Getoor, Bert Huang, Graham Katz, David Mares, Sathappan Muthiah, and Naren Ramakrishnan, THE EMBERS PROJECT, *Planned Protest Modeling in News and Social Media*, http://people.cs.vt.edu/~ramakris/papers/plannedProtest_IAAI15.pdf (last visited November 28, 2016).
[42] 119 Stat. 3411 (2006).
[43] Beyond the scope of this article is how to account, if at all, for European concerns about privacy, such as the European right to be forgotten—interpreted to mean individuals can in certain circumstances delete information found online about themselves and require others to delete that information too—and an ongoing negotiation for European safe harbor privacy provisions. See EXPORT.GOV, *Helping U.S. Companies Export*, http://export.gov/safeharbor/ (last updated February 11, 2016).
[44] U.S. CONST. amend IV.
[45] *See* Smith v. Maryland, 442 U.S. 735, 740 (1979).
[46] 389 U.S. 347, 348 (1967).
[47] *Id.*
[48] *Id.* at 351 (internal citations omitted).
[49] 883 F.Supp.2d 523, 525 (S.D.N.Y. 2012), *aff'd* United States v. Pierce, 2015 U.S. App. LEXIS 7717 (2nd Cir. 2015).
[50] *Id.*
[51] 132 S.Ct. 945, 948 (2012).
[52] *Id.* at 952.
[53] *Id.* at 954-957.
[54] *Id.*
[55] *See* United States v. Miller, 425 U.S. 435 (1976) (no expectation of privacy in financial records held by a financial institution); Smith v. Maryland, 442 U.S. 735 (1979) (no expectation of privacy in phone records); Guest v. Lies, 255 F.3d 325 (6th Cir. 2001) (by knowingly providing information to Internet Service Provider, result is no Fourth Amendment protection); United States v. Hambrick, 55 F. Supp. 2d 504 (W.D. Va. 1999) (third party doctrine results in no reasonable expectation of privacy in Internet Service Provider records); United States v. Kennedy, 81 F. Supp. 2d 1103 (D. Kan. 2000) (Fourth Amendment offers no protection to Internet Service Provider records). These precedents provide an understanding how the government could proceed in a lawful way to collect metadata (and not the contents of the underlying conversations) from phone companies.
[56] U.S. CONST. amend I.
[57] Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U.L. REV. 112 (2007).
[58] *Id.* at 128-32. Current Supreme Court *dicta* most closely supports scenario number two. In Stanford v. Texas, 379 U.S. 476, 485 (1965), the Court said, "In short . . . the constitutional

requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books and the basis for their seizure is the ideas which they contain. No less a standard could be faithful to First Amendment freedoms."

[59] *Id*.

[60] *See* Sherri J. Conrad, *Executive Order 12333: Unleashing the CIA Violates the Leash Law*, 70 CORNELL L. REV 968, 968-80 (1985), http://scholarship.law.cornell.edu/clr/vol70/iss5/6 (internal citations omitted).

[61] *See* Pub.L. No. 95–511, 92 Stat. 1783, 50 U.S.C. ch. 36 (1978).

[62] *See* Conrad at 968.

[63] 5 U.S.C. § 552a.

[64] Executive Order 12333: United States Intelligence Activities, 40 Fed. Reg. 59,941 (December 4, 1981), as amended by Executive Order 13,284, 68 Fed. Reg. 4,077 (January 23, 2003), and by Executive Order 13,355, and further amended by Executive Order 13,470, 73 Fed. Reg. 45,328 (2008) (July 30, 2008).

[65] *Id*. at 6-16.

[66] *Id*. at 14.

[67] *Id*.

[68] *Id*.

[69] *Id*. at 12-13.

[70] *Id*. at 12.

[71] *Id*. at 13.

[72] The Attorney General has adopted guidelines for other members of the Intelligence Community. In the author's review of other unclassified guidelines, the Attorney General's Guidelines for Domestic FBI Operations provide the most relevant guidance for Web activities. See *infra* text accompanying notes 73-78 and PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *Status Of Attorney General Approved U.S. Person Procedures Under E.O. 12333* (February 10, 2015), https://www.pclob.gov/library/EO12333-AG-Guidelines-February-10-2015.pdf (last visited February 25, 2016).

[73] *The Attorney General's Guidelines For Domestic FBI Operations* (2008), http://www.justice.gov/sites/default/files/ag/legacy/2008/10/03/guidelines.pdf.

[74] *Id*. at 17.

[75] *Id*. at 20.

[76] *Id*. at 17.

[77] *Id*.

[78] *Id*. at 44.

[79] 5 U.S.C. § 552a.

[80] *See* Cardamone v. Cohen, 241 F.3d 520, 524 (6th Cir. 2001).

[81] 5 U.S.C § 552a(a)(4), (5), and (e)(4).

[82] *Id*. at (e)(7).

[83] *Id*. Section (e)(4) of the Privacy Act requires federal agencies to publish in the *Federal Register* notice of a system of records. Privacy Act sections (j) and (i), however, provide exceptions to some of the requirements of section (e)(4) for law enforcement purposes. Notwithstanding extending the law enforcement exception to the Intelligence Community, at least one member of the Intelligence Community provided notice in the *Federal Register* pursuant to Privacy Act section (e)(4) concerning its efforts to monitor Social Media. Department of Homeland Security, *Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records*, https://www.federalregister.gov/articles/2015/05/27/2015-12692/privacy-act-of-1974-department-of-homeland-security-office-of-operations-coordination-and. The Department of Homeland Security also provided a privacy impact assessment of this initiative pursuant to the E-Government Act of 2002, https://www.dhs.gov/sites/default/files/ publications/privacy-pia-ops-publiclyavailablemediamonitoring-may2015.pdf.

[84] Jabara v. Webster, 691 F.2d 272, 280 (6th Cir. 1982).

[85] Bassiouni v. FBI, 436 F.3d 712, 724 (7th Cir. 2006).

[86] When a member of the Intelligence Community creates a Social Media account, it is not at all clear whether this act triggers the "joining or participating in a U.S. organization" requirements found in Executive Order 12333, paragraph 2.9. This action seems to go beyond "surfing the Internet" authorized by the Guidelines. Future Guidelines promulgated by the Attorney General will hopefully address this issue. In the author's view, creating a Social Media account for the mere purpose of reviewing and possibly collecting publicly available information found on that Social Media is most analogous to subscribing to publicly available information. So long as the activity within the Social Media remains passive, the Intelligence Community member should not be viewed as having joined or participated in a U.S. organization. Passive activity coupled with overt actions would include answering truthfully all information requested by the Social Media necessary to view content and would require not interacting with other Social Media members online.

[87] In the author's experience, Intelligence Community members outside the FBI view the Guidelines as persuasive to help govern their own information collection practices of publicly available information, in conjunction with any guidelines adopted for a specific Intelligence Community element. See *supra* notes 72-78 and accompanying text.

[88] See generally, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, *IC Information Sharing Executive*, http://www.dni.gov/index.php/about/organization/ic-information-sharing-executive (last visited April 17, 2017). Note that purchased information can be shared pursuant to the terms of the license/contract only.

[89] See *supra* note 72.

COL (USA) Steven C. Henricks currently serves as the Staff Judge Advocate (SJA) for I Corps & Joint Base Lewis-McChord, WA. He most recently served as the National Security Fellow at the U.S. Army War College, under the Office of the Director of National Intelligence. Previous assignments include SJA, 10th Mountain Division (Light Infantry) & Fort Drum, NY (2013-15); SJA, Combined Joint Task Force 10, Bagram, Afghanistan (2014); and prosecutor in a capital court-martial (2009-13). Henricks holds a BA in History and Political Science from Bethany College (1988), a JD from the University of Kansas School of Law (1991), and an LLM from the Judge Advocate General's Legal Center and School, Charlottesville, VA (2003). His publications include "A Fourth Amendment Privacy Analysis of the DoD's DNA Repository," 181 Military Law Review *69 (2004). He has also lectured on death penalty prosecutions and the rule of law missions in Iraq and Afghanistan.*

Social Media and Intelligence: The Precedent and Future for Regulations

by Nicole A. Softness

BACKGROUND

In 1977 Senator Ted Kennedy introduced legislature to create what would become the Foreign Intelligence Surveillance Act (FISA), following substantial Senate investigations into the legality of domestic intelligence activities.[1] The FISA was created to allow for oversight without detracting from national security demands. The subchapters accounted for several categories of surveillance, primarily electronic and physical. Over the past several decades, legislation has evolved to further refine the limitations on government surveillance in these arenas, as well as the boundaries of privacy.

However, following the promulgation of popular social media platforms and the regulations associated with millions of online users, the FISA has become an insufficient tool of measuring these limitations. The characteristics of social media content have increasingly challenged preconceived notions of privacy and security, including the diminished importance of geographical boundaries, the increasing availability of personal information in public and private spheres, and the blending of domestic and international jurisdictions. Legislation has struggled to account for these changes in a timely fashion and, as a result, norms for social media intelligence gathering have been largely defined by private sector and international norms. Moving forward, with the historic snail pace of domestic legislation it seems likely that these norms will continue to be defined by these actors, with aggressive post-Snowden-instigated input from the public domain.

USE OF SOCMINT

First, it is imperative to establish just how widespread the Intelligence Community's use of social media has become. In 2016 the Central Intelligence Agency's (CIA) venture capital firm, In-Q-Tel, reportedly invested in several technological companies capable of collecting and analyzing social media information to identify aberrations.[1] These investments in particular assign threat scores to people based on their online speech. Although first publicly reported in 2016, it is publicly understood the CIA has been partnering with similar organizations for years, and incorporating social media intelligence (referred to within the Intelligence Community as SOCMINT) into standard analytical schedules.

There are a number of other companies that have professed similar capabilities, and both private and public sector organizations have been heavily researching ways to both monitor and interpret online behavior on these platforms, as well as methods to identify warning behaviors online before people become tangible threats. The Defense Advanced Research Projects Agency (DARPA) in particular has prioritized this type of online predictive analysis, as have law enforcement organizations and police forces.[2] They and others have acclaimed that social media is regarded as a unique way to identify behavioral trends online and simultaneously predict future individual behavior.

These investments and priorities are not astonishing, considering just how useful social media intelligence can be for the Intelligence Community and law enforcement, and how efficient this surveillance is compared with older methods. The *International Journal of Law and Information Technology* highlights that "the net effect of this deluge of material is that where once LEAs (law enforcement agencies) had to spend an enormous amount of resources in acquiring intelligence about those under suspicion, often by covert operations, now simple, cheap, and easy technological means exist to monitor us all. Much of what we all say, do, think, and feel can now be absorbed simply by reading networks such as on Facebook and Twitter."[3]

For a community whose mission is generally defined as the ability to identify and analyze information quickly and accurately for the use of policymakers, social media is the perfect decentralizer of such intelligence. A 2014 study showed that more than 80% of federal, state, and local law enforcement officials regularly depended on social media platforms as a means of intelligence.[4] This number is surely astronomically higher in 2017, considering how many more people worldwide have joined platforms as committed users.

Part of this increase is likely to stem from the public's pressure for faster absolution of criminal activities. Following public crimes, especially those highlighted or captured online, the citizenry demands swifter policing. Every day the government has a smaller window of appropriate response time before the onslaught of condemnation appears from blogs and news websites. Online influence is increasingly accessible for citizens, who can more rapidly ascertain government failures and share their criticisms with the world.

It is publicly known that content analysis (the observation of how often words appear in someone's language) can provide uniquely valuable insights into a person's intent, emotional stability, and opinions.

Additionally, there are those who retroactively criticize officials for failing to recognize threatening actors ahead of time, arguing that proper analysis of social media posts would have revealed a person's intention to act maliciously. Although a substantially loud portion of the citizenry denounces such invasions of privacy, these first groups that demand faster government action are not ignored.

BENEFITS OF SOCMINT

It is publicly known that content analysis (the observation of how often words appear in someone's language) can provide uniquely valuable insights into a person's intent, emotional stability, and opinions. Many of the arguments surrounding the morality and legality of SOCMINT focus on this area of the issue, and the government's legal right to observe these characteristics of different parts of domestic and foreign populations.

However, SOCMINT offers a number of other benefits for the Intelligence Community. By monitoring suspects' Facebook accounts, one can establish their position with social networks, their influence and influencers, their geographic location, their history of content "likes," and more. This intelligence provides valuable insights. As alternative methods of analysis become more publicly understood, including network analysis and influence mapping, the domestic population will no longer settle for regulations singularly limited to the content of users' Facebook posts or tweets.

LIMITATIONS OF SOCMINT

Of course, it would be premature to argue that SOCMINT has revolutionized intelligence surveillance, or that it has diminished the need for auxiliary surveillance by other means. While surveying a user's online activity and presence has real benefits, the accuracy is not 100% dependable or achievable. Observers often run into the issue of "context collapse," when messages originally meant for a cultivated, small audience become misconstrued once applied to a larger audience. SOCMINT does not solve these issues of context or nuance. It merely broadens the scope of data collection available.

Additionally, observing this part of someone's life cannot provide unlimited access into his or her motivations or intentions. No intelligence can provide that, yet there are those who would construct entire profiles based on someone's social media use. The Department of Homeland Security (DHS) refers to SOCMINT in an appropriately humble manner, defining it as a "tool for situational awareness—an active awareness of their surroundings and possible threats thereof, made possible through monitoring social media feeds about events in localized geographies."[5]

SOCMINT REGULATIONS

In light of the vast benefits of using SOCMINT for intelligence gathering and law enforcement, various legal communities have worked tirelessly to define the boundaries of SOCMINT use. These competing definitions and regulations come from a number of sources, including the social media companies, domestic legal communities, and international legal communities.

United States Legislative Regulations

The primary legislators of intelligence regulation in the United States are the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. Emerging in the 1970s, their respective jurisdictions included electronic surveillance, and currently include the National Intelligence Program (NIP), the intelligence budget, and all agencies funded by the NIP.[6] Naturally, these oversight committees aim to shape and control the direction of the Intelligence Community's relationship with all sources of intelligence, although precedent has shown that the committees do not often or quickly transform to meet evolving intelligence climates.

Private Sector Regulations

As tempting as it could be to discredit or ignore the validity of private sector regulations in this area, this jurisdiction has perhaps proved the most influential. Social media companies

own and manage entry into their platforms and, with the ability to ban and control user experiences, as well as the ability of the IC and law enforcement to buy or request analytical data of those experiences, they have certain unprecedented powers.

Major social media companies, namely Twitter, Slack, and Facebook, have published comprehensive community guidelines for those wishing to use or access their platforms. These guidelines highlight those protections users can expect, and reiterate the ownership that the companies ultimately have over their data for research and marketing purposes.

TWITTER

Twitter's guidelines on user protection state:

> One will not knowingly: (1) allow or assist any government entities, law enforcement, or other organizations to conduct surveillance on Content or obtain information on Twitter's users or their Tweets that would require a subpoena, court order, or other valid legal process, or that would otherwise have the potential to be inconsistent with our users' reasonable expectations of privacy.[7]

This demonstrates Twitter's supposed prohibition of government and law enforcement surveillance that would fall outside previously established privacy legislation, signifying a rather old-fashioned, conventional approach toward content typically considered "private," such as private messages and personal information only accessible by confirmed online friends.

However, others argue that the majority of information on these platforms is public anyway, and would not require the use of a subpoena. They claim that Twitter's guidelines are irrelevant, and that governments continue to survey the information they need without ever requesting access or demonstrating sufficient cause. Controversy largely focuses on this boundary between information that would require a subpoena and information that would not, irrespective of whatever guidelines Twitter professes to enforce.

SLACK

Slack's guidelines are nearly a perfect copy of Twitter's published rules. However, they distinctively mention the United Nations Universal Declaration of Human Rights, saying:

> You will not knowingly (1) allow or assist any government entities, law enforcement, or other organizations to conduct surveillance or obtain data using your access to the Slack Application Programming Interface (API) in order to avoid serving legal process directly on Slack. Any such use by you for law enforcement purposes is a breach of these API Terms of Service.[8]

This inclusion of international law in their surveillance guidelines signifies the need for standards that transcend domestic law. Slack and Twitter may be based in the United States, but their employees and consumers span the globe, and demand individualized legal considerations. Senior executives at these companies have stated how difficult it is, both morally and legally, to alter their user regulations and technological design to appeal to different countries. It seems unrealistic to expect companies like Slack to provide individualized guidelines for every country, accounting for each of those nation's domestic surveillance laws. This demonstrates the clear need for comprehensive international involvement, even though citizenries often profess the worthlessness of international governing bodies.

Even though one could argue social media companies have created their own hegemonic rule over online content, law enforcement officials and the Intelligence Community are still held accountable under existing domestic regulations on privacy.

Social media companies have naturally faced severe criticism toward these guidelines, from both sides of the surveillance aisle. Citizens have argued for increased protections for their personal information, while the government has argued for surveillance in the name of national security. A former Deputy Director of NSA stated, "If Twitter continues to sell this [data] to the private sector, but denies the government, that's hypocritical."[9]

Domestic Regulations

Of course, even though one could argue social media companies have created their own hegemonic rule over online content, law enforcement officials and the Intelligence Community are still held accountable under existing domestic regulations on privacy. Current standards in the United States stem from several influential Supreme Court cases, including *Clapper v. Amnesty International* (2013), *Riley v. California* (2014), and *Packingham v. North Carolina* (2017).

CLAPPER V. AMNESTY INTERNATIONAL (2013)

In 2012 a group of human rights organizations, journalists, and attorneys challenged a new subset of the FISA (Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U. S. C. §1881a) that authorized unprecedented electronic surveillance capabilities to the United States for foreign intelligence purposes. Section 702 allowed the Director of National Intelligence to acquire foreign intelligence by surveilling those reasonably believed to reside outside the United States, without stating the "nature and location of each of the particular facilities or places at which the electronic surveillance will occur."[10]

The respondents argued that the procedure violated the Fourth Amendment, and forced them to take costly measures to protect their communications data with those outside the United States. Ultimately, the majority opinion, delivered by Justice Samuel A. Alito, determined in 2013 that the group was not harmed by the new provisions, setting a new precedent abolishing the need for warrants in electronic intelligence gathering, which likely played a large part in setting norms for SOCMINT.[11]

RILEY V. CALIFORNIA (2014)

The Supreme Court determined in 2014 that the police could not, without a warrant, monitor and analyze digital information on a cellphone belonging to someone who had been arrested.[12] The majority opinion argued that digital data were unprecedented, deserving of more nuanced privacy considerations than physical manifestations of personal data. As Chief Justice John Roberts put it, a cell phone possesses more unique data than any isolated personal item could hope to store, including information dating back years.[13] This case represented a clear distinction between accessible information on a person and information that would be inaccessible in any other situation. It also highlighted how much more invasive surveillance of digital data could be, as it provided a much larger window into a person's behavioral history.

PACKINGHAM V. NORTH CAROLINA (2017)

In a recent case, the Supreme Court determined that social media could, in fact, represent a human right, one that cannot be removed from a person convicted of criminal activities. Following the respondent's (a convicted sex offender) appeal against a regional ruling banning him from social networking sites following his conviction, the decision stated that "the State may not enact this complete bar to the exercise of First Amendment rights on websites integral to the fabric of modern society and culture."[14]

By responding in the affirmative, the Supreme Court essentially set a precedent against monitoring individuals on social media platforms. Many of the arguments against privacy say that participation on websites like Facebook and Twitter are voluntary, and users should have no reasonable expectation of privacy from the Intelligence Community. If social media is an inherent right, in line with access to global economic and political online networks, this argument will be vastly diminished.

Associate Justice Elena Kagan has suggested that "social media sites like Facebook and Twitter are 'incredibly important parts' of the country's political and religious culture. People do not merely rely on those sites to obtain virtually all of their information...but even 'structure their civil community life' around them."[15] Associate Justice Ruth Bader Ginsberg agreed, citing the importance of the online marketplace of ideas.[16]

Public Sentiment

Of course, although company regulations and domestic law continue to play an important part in defining the relationship between the Intelligence Community and social media, one must not discount the validity and influence of the court of public opinion in establishing norms.

The important takeaway from these company declarations is the ultimate influence of the public in shaping surveillance regulations for social media.

In 2016, following a report by the American Civil Liberties Union (ACLU), Facebook, Instagram, and Twitter cut off the access of Geofeedia (an online tool capable of rapidly sifting through social media content) to their websites.[17] The ACLU argued that "online spying tools" such as Geofeedia presented cultivated data for law enforcement in unseemly manners, which resulted in the identification of and arrests of people involved in protests.[18] The ACLU and other similar groups have continued to sway the private sector on this issue. In March 2017, Facebook revoked access for its developer groups from using Facebook and Instagram data in a surveillance tool.[19] Twitter also cut off access for Snaptrends and Media Sonar, social media monitoring tools, after Media Sonar tracked the hashtag #BlackLivesMatter to geolocate and identify activists for law enforcement.[20] Now that Facebook and others have set this precedent of responding to ACLU data reports, they are likely to continue altering their business operations based on this specific representation of public opinion.

Companies like Geofeedia, which originally emerged as tools to better direct marketing campaigns, have provided crucial intelligence avenues for the government, by scraping content for websites and allowing access to complete streams of social media posts (referred to as firehoses). Geofeedia fits within a large community of online surveillance and data scraping tools, in the company of others such as LifeRaft, Media Sonar, CES Prism, Snaptrends, and many more.[21]

The important takeaway from these company declarations is the ultimate influence of the public in shaping surveillance regulations for social media. Perhaps uniquely, in this fast-moving arena dominated by fast-growing technologies, the power of the public to sway private sector movements is impressive, even if the U.S. public outcry continues to fall behind that in countries with stronger policing forces, such as Germany.

International Law

In recognition of the multitude of factors shaping the opportunities and limitations for the Intelligence Community's use of SOCMINT, it is likely that a combination of domestic and international legal influences will continue to define its use. There are a number of reasons that international law, often relegated as a toothless enforcer of international norms, might play a larger role in this arena.

UNRESOLVED INTERNATIONAL LAW FOR ESPIONAGE

In providing context for the role of international law in intelligence communities, it is imperative to note the severe lack of literature, both academic and legislative, on this space. Scholar A. John Radsan states that "[t]raditional international law is remarkably oblivious to the peacetime practice of espionage. Leading treatises overlook espionage altogether or contain a perfunctory paragraph that defines a spy and describes his hapless fate upon capture."[22] Radsan explains that international and foreign national laws account for espionage and intelligence in three ways. The first category suggests that peacetime espionage is legal under international law, while the second disagrees. The third group suggests that peacetime espionage goes "beyond good and evil," as Nietzsche would say, and even others suggest that the collection of foreign intelligence demonstrates a clear right to self-defense.[23]

Specifically relating to surveillance, several schools of thought dominate the international legal conversations and attempts to establish precedent. Some argue that bulk electronic surveillance violates the rights of privacy guaranteed by the International Covenant on Civil and Political Rights (ICCPR), while others focus on the supposed violation of the Vienna Convention on Diplomatic Relations.[24] States have also said that this surveillance violates customary "norms" of sovereignty and territorial integrity. Although states have conceded that the laws of war apply to intelligence during armed conflicts, the use of surveillance during peacetime has complicated these arguments. Irrespective of these groups and schools of thought, the reality is that international law is lackluster in its accounting for intelligence, let alone the surveillance of online data on platforms that are owned by one country, and accessible in another.

PEER CONSTRAINTS

Nonetheless, legal scholar Ashley Deeks, in an article for the University of Virginia, argues that national intelligence communities are actually uniquely held accountable by other states' intelligence regulations, in ways that other communities, and the private and public sector, are not.[25] She claims that foreign intelligence organizations are incentivized to play by the rules of others, if they wish to achieve collaborative benefits such as information sharing, which are of incredible value for intelligence analysts.[26]

Although Deeks does agree with Radsan regarding the lack of international law, she implies that the choice is more purposeful, asserting that "most states neither proclaim the legality nor concede the illegality of their intelligence activities under international law, seeming to prefer the ambiguity of the status quo."[27]

Intelligence communities need each other, especially in newer, cross-boundary arenas like SOCMINT.

However, her work focuses more on the inherently collaborative nature of intelligence, suggesting that these incentives will occur regardless of specific "collaborative" laws.[28] Deeks explains how intelligence communities end up following legislation and legal interpretations enacted by some other states, since they recognize the benefits of working together and sharing findings. Intelligence communities need each other, especially in newer, cross-boundary arenas like SOCMINT. She insists:

> If one IC had the capacity to obtain all of the intelligence it needed on its own—using signals intelligence, human intelligence, and other sources of information—it would not need to turn to liaison services to obtain information. Likewise, if one IC had the capacity to conduct covert operations, unfettered, worldwide, that IC would not need to work with liaison services. But that is not the state of the world.[29]

SOCMINT further highlights the benefits of this collaboration. As mentioned before, analyzing snapshots of information on social media platforms requires cultural contexts, such as the recognition of local references and local slang. These cannot occur without the cooperation of international partners, whether through direct information sharing or the allowance of intelligence centers in other states.

The implications of these collaborative demands suggest that certain states have to adhere to norms with which their domestic citizenries may disagree. If the U.S. Intelligence Community hopes to work with other states, it may have to accept that these partners have different considerations of privacy and surveillance. This demonstrates a clear likelihood that international cooperative norms will play a large part in defining the relationship between the Intelligence Community and social media surveillance.

CONCLUSION

Regardless of any findings on the "inherent human right" to social media access and use, online networks are unlikely to disappear anytime soon, and intelligence communities are unlikely to abandon their work in more efficiently monitoring and identifying actionable intelligence on these platforms. However, although one must recognize the broader inability of domestic legislation to account for technological issues in a timely manner, there is an enormous need to define the regulations for SOCMINT, especially in a time where public opinion can be overwhelmingly loud and influential.

Perhaps the need for the U.S. Intelligence Community to abide by other states' norms will play the biggest part in this debate. Perhaps the domestic legislative branch will continue its work to define what level of privacy citizens can expect, or to what extent private sector companies will be forced to collaborate with intelligence actors. Nonetheless, even though intelligence has remained a vague and unregulated space in the past, with the magnifying accessibility and impact of social media, a space dominated by so many players with varying concerns and levels of influence cannot remain unregulated.

Notes

[1] Risen, Tom. "CIA Tech Firm Seeks More Social Media Spying." *U.S. News and World Report*, April 15, 2016. Accessed April 22, 2017.
[2] Leopold, George. "DARPA looks to tap social media, big data to probe the causes of social unrest." *Defense Systems*, March 11, 2016. Accessed April 22, 2017.
[3] Edwards, Lilian, and Lachlan Urquhart, "Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence?" (December 11, 2015). *International Journal of Law and Information Technology* (Autumn 2016), 24 (3), 279-310.
[4] Mateescu, Alexandra, Douglas Brunton, Alex Rosenblat, Desmond Patton, Zachary Gold, and Danah Boyd. "Social Media Surveillance and Law Enforcement." *Data & Civil Rights: A New Era of Policing and Justice*, October 27, 2015. Accessed April 22, 2017.
[5] Ibid.
[6] Congressional Oversight of the Intelligence Community. July 2009. Accessed April 24, 2017. http://www.belfercenter.org/publication/congressional-oversight-intelligence-community.
[7] Leetaru, Kalev. "When Twitter Cut Off the US Intelligence Community: Social Media and Surveillance." *Forbes*, May 9, 2016. Accessed April 22, 2017.
[8] Ibid.
[9] Ibid.
[10] James R. Clapper, Jr., Director of National Intelligence, et al. Petitioners v. Amnesty International USA et al., U.S. 568 (2013).
[11] Ibid.
[12] David Leon Riley v. California, U.S. 573 (2014).
[13] Ibid.
[14] Packingham v. North Carolina, U.S. 582 (2017).
[15] Ibid
[16] Ibid.
[17] Cameron, Dell. "Dozens of policy-spying tools remain after Facebook, Twitter crack down on Geofeedia." *The Daily Dot*, October 11, 2016. Accessed April 22, 2017.
[18] Ibid.
[19] Conger, Kate. "Facebook tells developers to not use data for surveillance." *TechCrunch*, March 13, 2017. Accessed April 23, 2017.
[20] Ibid.
[21] Ibid.
[22] A.J. Radsan, "The Unresolved Equation of Espionage and International Law," 28 *Mich. J. Int'l L.* 595 (2007).
[23] Ibid.
[24] Deeks, Ashley, "Intelligence Communities, Peer Constraints, and the Law" (February 1, 2016). 7 *Harv. Nat'l Security J.* 1 (2016); Virginia Public Law and Legal Theory Research Paper No. 16.
[25] Deeks, Ashley, "Intelligence Communities and International Law: A Comparative Approach" (2015). *Comparative International Law*, 2016, forthcoming; Virginia Public Law and Legal Theory Research Paper No. 1.
[26] Ibid.
[27] Ibid.
[28] Deeks, "Peer Constraints and the Law."
[29] Deeks, "Peer Constraints and the Law."

Nicole A. Softness is a graduate student at Columbia University's School of International and Public Affairs, studying International Security and Cyber Policy. Her research focuses on the intersection of counterterrorism and social media, following up an undergraduate thesis on al Qaeda's messaging strategies. Nicki is currently the Research Assistant for Columbia's Initiative on the Future of Cyber Risk, and has published articles on cyber policy and cybersecurity in the Yale and Columbia journals of international affairs.

Darknet Markets:
A Modern Day Enigma for Law Enforcement and the Intelligence Community

by Sarah Heidenreich and Dr. Dennis A. Westbrooks II

EXECUTIVE SUMMARY

In October 2013, the Federal Bureau of Investigation (FBI) and Operation MARCO POLO task force members planned and executed a sting operation to apprehend Ross William Ulbricht. Also known as "Dread Pirate Roberts," this criminal mastermind created and managed the first and largest drug trafficking marketplace on the Darknet, called the "Silk Road."[1] This first of its kind operation highlighted the formidable challenges Darknet Markets pose to U.S. Intelligence Community (IC) and Law Enforcement (LE) counternarcotics agencies, to include resource-intensive investigations and operations, and short-lived successes. These challenges are largely existent because the Darknet enables the technical obfuscation of online criminal identities, and the decentralized structure of Darknet Markets enables drug vendors and consumers to be minimally affected by IC/LE takedown operations. As such, the IC/LE community must establish a structured, holistic approach in tackling the challenges presented by Darknet Markets, to include integrating technological proficiency, international partnership and engagement, and social exploitation methodologies to effectively deter Darknet drug trafficking and avoid the resource-intensive and limited impact pitfalls that already plague the U.S. "War on Drugs."[2]

INTRODUCTION

The national security risks posed by traditional drug trafficking, such as community violence and degraded public health, are clearly outlined in the U.S. National Drug Control Strategy.[3] However, there is limited legislation or policy guidance that addresses how Darknet drug trafficking inherently presents its own set of unique and technical challenges that flout current U.S. drug laws and safeguards, as well as complicate prosecution efforts for the IC/LE communities. In 2011 U.S. Senator Charles Schumer declared that Darknet Markets had a detrimental effect on U.S. development as a society; consequently, he spearheaded a federal campaign against Darknet Markets by petitioning the Department of Justice (DOJ) to interdict the Silk Road. In 2014, after the takedown of Silk Road and the subsequent appearance of "Silk Road 2.0," Senator Schumer wrote a letter to the U.S. Attorney General requesting an expansion of prosecutorial efforts to combat Darknet drug trafficking.[4]

The "Darknet" first began as password-protected, peer-to-peer file sharing of copyright materials in the late 1990s.

BACKGROUND

The concept of a "Darknet" consistently developed alongside the evolution of the Internet. The "Darknet" first began as password-protected, peer-to-peer file sharing of copyright materials in the late 1990s, which was soon streamlined by the creation of "Freenet" by software developer Ian Clarke in 2000.[5] Freenet was an open-source server that formalized the concept of decentralized peer-to-peer network sharing, in which Freenet users would share hard drive space to maintain a private file-sharing network. Freenet provided encrypted anonymity to its users for peer-to-peer transactions; however, anonymity for actual network communications, characterized as "Internet traffic," was not established until the creation of "The Onion Router" (TOR) by the U.S. Naval Research Laboratory in 2002. TOR was originally developed to protect U.S. government communications and provide an avenue for individuals in repressed countries to access the Internet without censorship; however, it quickly became a safe-haven and worldwide platform for cyber criminals to conduct illicit exchange of copyright materials and child pornography, and to facilitate other nefarious online activities.[6]

Although there were illegal activities frequently occurring on the Darknet throughout its evolution, these activities were not effectively commercialized until the creation of the first formal Darknet Marketplace in February 2011, known as the "Silk Road." Ross Ulbricht, the creator of the Silk Road, revolutionized the Darknet's illicit industries in a manner

similar to how entrepreneur Jeff Bezos revolutionized the online shopping industry with the creation of Amazon. Silk Road was a Darknet Marketplace that did not specifically sell, but facilitated, the sale of illicit goods by providing a controlled, trusted, and anonymous venue for vendors and consumers to conduct trusted transactions. Silk Road was the first known Darknet Marketplace and hosted the first Darknet Markets that sold illegal narcotics to a worldwide consumer base. While it is possible that drug trafficking occurred on the Darknet on a small scale prior to the Silk Road, there were few options for concealing money exchanged in these transactions, which posed an increased risk of IC or LE discovery of the Darknet users. This issue of anonymity was resolved with the development of the pseudonymous cryptocurrency, Bitcoin, which was implemented as the primary form of currency on Darknet Markets.[7]

METHODOLOGY

Research for this article utilized a qualitative methodology. The qualitative research approach is an effective tool for researching open-ended questions and emerging topics, because it prescribes a large pool of unique data sources to enable inductive analysis.[8] This approach is flexible and allows researchers to adapt their perspectives or analysis based not just on statistical or research data but on the personal experiences of individuals involved in the subject matter, also known as data collection from the "natural setting."[9] The research design for this article was a case study. The case study research design is a popular social sciences approach and is commonly used with qualitative research methodology because it complements the qualitative inductive approach to research and analysis. It is especially effective for exploring new and unknown situations for which there is limited available information or limited understanding.[10]

CASE STUDY

The purpose of this study was to explore the risk of Darknet drug trafficking to U.S. national security through the lens of both international and U.S. policy and strategic frameworks regarding traditional drug trafficking. Particular focus was placed on drug- affiliated violence and crime, illicit economies, and the threats from criminal and terrorist organizations. The 2013 indictment of Ross Ulbricht, the leader of the largest Darknet Market "Silk Road," was used as a case study to evaluate the IC/LE capabilities and strategies for detecting and deterring Darknet drug trafficking.

This case study articulated multiple challenges that IC/LE counternarcotics communities experience when confronting the Darknet Market phenomenon. Challenges include developing and maintaining access to the appropriate investigative tools in order to de-anonymize Darknet users, maintaining the privacy of U.S. and foreign citizens, adhering to jurisdictional limitations on transnational crime, and establishing the necessary legal authorities to conduct new types of cyber investigations and operations.[11] This case study also revealed that IC/LE community efforts yield some positive results due to continuous improvement of investigative and legal endeavors to overcome the identified challenges.[12] However, there remains no research regarding analysis of IC/LE counternarcotics efforts expended to combat Darknet drug trafficking versus their level of success. Moreover, the measure of "success" in combating Darknet drug trafficking remains undefined. This is because some of the IC/LE efforts only target the webmasters for the Darknet Markets, rather than individuals who are actually selling the illicit goods.[13]

THE THREAT TO U.S. NATIONAL SECURITY

There is a negligible amount of reporting that evaluates the threat of Darknet Market drug trafficking in comparison to street-market drug trafficking, or addresses the threat of this phenomenon to U.S. national security. The reporting that does exist comparing street-market drug trafficking to Darknet drug trafficking indicates that, while not without risks, Darknet drug trafficking is generally considered safer for both vendors and consumers.[14] The rationale behind this assessment is that the risks associated with traditional drug trafficking, which include physical violence, being caught by law enforcement or family members, and receiving or consuming tainted products, are negligible on the Darknet. However, this argument as a defense has been rejected in public courts of law.[15]

Both the U.S. National Drug Strategy and the United Nations Office on Drugs and Crime posit that there is an inevitable nexus among all types of drug trafficking, transnational organized crime, and terrorism, which poses a serious threat to national security.

Rather than a risk-to-benefit comparison against the traditional forms of drug trafficking, Darknet Markets are more commonly evaluated in terms of how they facilitate illicit activity in violation of the laws and regulations of the physical realm. For example, the illicit drug supply chain for Darknet Markets may directly or indirectly fund U.S. and foreign violent criminal and

terrorist organizations. This is because, regardless of where or how they are ultimately sold, illicit drugs are often mass-cultivated in countries where there is a permissive environment for drug production, as well as other criminal and terrorist activities, for both financial and ideological purposes.[16] As such, both the U.S. National Drug Strategy and the United Nations Office on Drugs and Crime posit that there is an inevitable nexus among all types of drug trafficking, transnational organized crime, and terrorism, which poses a serious threat to national security.[17]

THEORETICAL FRAMEWORK

The three theories that were used to support this research were the Space Transition Theory, Crime Opportunity Theory, and Rational Choice Theory.

Space Transition Theory

The overarching theory for this research is Space Transition Theory, which attempts to explain the differences in human propensity to commit criminal behaviors in physical space and cyberspace.[18] For example, one of the postulates of Space Transition Theory is that persons with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which otherwise they would not commit in physical space due to their status and position.[19] This theory is applicable to Darknet drug trafficking because the creation of Darknet Markets in "cyberspace" provided a permissive environment for individual drug users, who were previously unaffiliated with traditional drug trafficking organizations, to engage in illicit behavior which they may not have otherwise.

Crime Opportunity Theory

Crime Opportunity Theory explores the motivations behind committing crimes with a specific concentration on the propensity to commit crime based on opportunistic conditions. One of the most relevant principles of the Crime Opportunity Theory for this study states, "Social and technological changes produce new crime opportunities."[20] This principle is especially applicable to Darknet Markets, because these markets are inherently opportunistic creations that take advantage of the anonymous networks originally developed by the U.S. government to provide an outlet for persecuted and repressed segments of society in other nation-states.[21]

Rational Choice Theory

Rational Choice Theory states that most people make a rational calculation of the costs and benefits of any action they perform. This theory applies to the process of decision-making that occurs when individuals on Darknet Markets decide to engage in criminal drug trafficking, in which they weigh the risks of conducting the illicit activities versus the monetary profits. There are few examples of Rational Choice Theory being used as a theoretical framework for cybercrime, as it is generally used for traditional criminal, sociological, or economic models. As such, this model will be a tertiary point of reference for this study.[22]

RESEARCH FINDINGS

The following research questions guided this study:

1. What are Darknet Markets, and how are they used in the drug trafficking industry?

Darknet Markets are hidden services on the Darknet where users may purchase and sell illicit paraphernalia or services in exchange for cryptocurrency.[23] These Markets, which are available only by accessing the Darknet, vary from accessible open forum to invitation-only and password-protected online environments. Similar in infrastructure to online shopping marketplaces like Amazon and eBay, Darknet Markets are simply an obfuscated platform for multiple vendors to sell their wares, and for users to make concealed purchases. Transactions on Darknet Markets are facilitated through virtual or cryptocurrencies, such as Bitcoin, and conversations between vendors and consumers are generally encrypted via Pretty Good Privacy (PGP) protection measures. Once completed, the vendor employs a variety of operational security measures to package the illicit goods for shipment via traditional air and ground shipping companies, such as the U.S. Postal Service, UPS, and FedEx.[24]

Darknets are revolutionizing the drug trafficking industry in a similar manner to how online shopping at Amazon revolutionized the shopping industry, because they provide convenience, competitive markets, a variety of goods, and global reach.

Darknet Markets are the ideal location for drug trafficking primarily because they assuage the risk of law enforcement discovery and prosecution, one of the biggest job hazards for drug dealers and consumers. However, there are multiple other aspects of Darknet Markets, beyond anonymity, that contribute to their booming success in the drug trafficking industry. Darknets are revolutionizing the drug trafficking industry

in a similar manner to how online shopping at Amazon revolutionized the shopping industry, because they provide convenience, competitive markets, a variety of goods, and global reach. In 2012 approximately 243 million people worldwide reported using illicit drugs; 23.9 million of the reported users were Americans. By 2013, the number of American illicit drug users increased to 24.6 million, which continues an upward trend.[25] The world population in 2013 was 7.1 billion people, indicating that almost 3.5 percent of the world's population uses illicit drugs.[26]

Limited studies indicate that only three to ten percent of global drug users purchase illicit drugs on the Internet or Darknet.[27] This is possibly due to the complex technical requirements necessary to access, and make illicit purchases on, the Darknet. Additionally, the small population of Darknet consumers could be due to the composition of the Darknet Market consumer base; limited research indicates
this consumer base is comprised of individuals who buy in bulk, such as professionals or scholars who conduct planned and systematic drug use, as well as street-drug dealers themselves.[28] Current research indicates the number of Darknet Market users is no longer increasing at the rapid rate it did in the initial stages of Darknet Market existence; rather, sales indicate a stable economic environment.[29] According to a well-known researcher in the field, in 2015 there were an estimated 9,300 vendors selling illicit goods on Darknet Markets. Limited research indicates the Darknet's best-selling narcotics include marijuana, ecstasy, cocaine, and prescription drugs like Viagra and OxyContin.[30]

2. What is the IC/LE strategy to combat Darknet Markets?

IC/LE entities recognize there are unique challenges posed by Darknet Markets when it comes to identifying and prosecuting criminals. These challenges include the technologies that enable the anonymity of illicit drug vendors and consumers, such as TOR and strong encryption algorithms; jurisdictional limitations on transnational crime; a lack of international cooperation; a concern for private citizen rights on the Internet; outdated legislation; and technological tools that cannot keep pace with Darknet Marketplace mobility.[31]

Since the successful takedown of the "Silk Road," International and IC/LE entities have experienced limited success in discovering, indicting, and convicting online drug vendors. However, the rate at which these individuals are arrested is still marginal compared to the overall number of illicit drug traffickers on the Darknet. In 2014 Operation ONYMOUS, a joint operation among Europol, the FBI, and Homeland Security Investigations (HSI), resulted in the seizure of a total of 414 Darknet hidden services and led to the arrest of 17 people, to include Blake Benthall, who was the new administrator of Silk Road 2.0.[32] In 2015 an FBI-led international investigation, Operation SHROUDED HORIZON, resulted in the charging or arrest of nearly 70 people worldwide. These individuals were suspected of being hackers from the Darknet site "Darkode" and allegedly conducted illicit money laundering, wire fraud, and computer fraud. In 2015 the German Leipzig Authorities experienced a rare success in which online undercover operations, and poor operational security practices on the part of cyber criminals, enabled them to arrest seven individuals and issue warrants for 38 more individuals associated with a vendor known as "Shiny-Flakes" on the Darknet Market "Evolution." The authorities reportedly seized over 700 pounds of illegal drugs, worth nearly $4.25 million, from these individuals. In 2016 IC/LE entities arrested 11 individuals in New Orleans, LA, who were charged with possession, distribution, and conspiracy to distribute over 200,000 manufactured narcotics pills, worth nearly $1.1 million, on the Darknet.[33] Despite these successful operations, as of 2015 expert research indicates at least 28 Darknet Markets still exist and generate approximately $300,000-500,000 in sales per day, indicating little to no disruption of the Darknet Market economy or infrastructure.[34]

IMPLICATIONS OF THE STUDY

The resources expended against the small and resilient population of Darknet users appear to have a minimal impact on the overall Darknet drug trafficking trade. Intrinsically, the U.S. government overall must consider if the significant resource expenditures targeting Darknet Markets are justified or are a prudent use of resources, compared to other drug trafficking priority targets in the physical realm. This is an especially important consideration since the fiscal environment of the U.S. government has been strained since at least 2013, to include continuous budget cuts. An overemphasized IC/LE focus on Darknet Markets may cause a reduction in investigations and operations targeting dangerous drug traffickers in the physical realm, which could potentially result in an increase of violence in U.S. communities. The question that remains to be answered from the IC/LE counternarcotics community is whether the resources spent targeting elusive, low-risk Darknet Market targets, against which IC/LE operations have had a limited impact, would be better expended targeting the Pablo Escobars and El Chapos of the drug trafficking trade.[35]

CONCLUSION

Darknet drug trafficking and Darknet Markets will likely remain a challenge for IC/LE counternarcotics entities as long as technology continues to increase in sophistication and the global demand for illicit drugs remains. IC/LE counternarcotics entities have done an admirable job in applying innovation, creativity, and determination to identify new investigative tools, legal procedures, and operational plans to interdict this new method of drug trafficking and its facilitators. However, the U.S. War on Drugs overall remains a costly endeavor for the U.S. government, and Darknet Markets complicate the intensive resource demand that is necessary to identify, arrest, and prosecute illicit Darknet Market drug vendors and consumers.

NOTES

[1] *United States of America v. Ross William Ulbricht, a/k/a/ "Dread Pirate Roberts," a/k/a/ "DPR," a/k/a "Silk Road," Defendant.* P.B., 14 CRIM 068, (US District Court Southern District of New York 2014); *United States v. Curtis Clark Green*. M.C. and S.W. (US Attorney's Office District of Maryland Northern Division 2013); Joshua Bearman et al., *The Rise & Fall of Silk Road, Part 1*, The Untold Story of Silk Road (New York: Wired, 2015), accessed November 15, 2015, http://www.wired.com/2015/04/silk-road-1/; Joshua Bearman et al., *The Rise & Fall of Silk Road, Part 2*, The Untold Story of Silk Road (New York: Wired, 2015), accessed November 15, 2015, http://www.wired.com/2015/05/silk-road-2/.

[2] Nicolas Christin, "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace," in *22Nd International World Wide Web Conference* (Carnegie Mellon University, 2015), accessed January 5, 2015, https://www.andrew.cmu.edu/user/nicolasc/publications/Christin-WWW13.pdf; Marie Claire Van Hout and Tim Bingham, "Silk Road, the Virtual Drug Marketplace: A Single Case Study of User Experiences," *International Journal of Drug Policy* 24, no. 5 (2013): 385-391.

[3] "ODNI FAQ," dni.gov, last modified 2014, accessed December 16, 2014, http://www.dni.gov/index.php/about/faq?start=2; Phil Williams and Vanda Felbab-Brown, *Drug Trafficking, Violence, And Instability* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2012); Chau Ngo, *United Nations Office on Drugs and Crime Report: Illicit Drug Deals Multiply on the "Dark Net"* (New York: Global Information Network, 2014), accessed January 4, 2015, http://search.proquest.com/docview/1542481592?accountid=10504; Executive Office of the President of the United States, *National Drug Control Budget: FY 2014 Funding Highlights* (Washington, DC: The White House, 2013). Accessed February 3, 2014, http://www.whitehouse.gov/sites/default/files/ondcp/policy-and-research/fy_2014_drug_control_budget_highlights_3.pdf. Executive Office of the President of the United States, *National Drug Control Strategy 2014* (Washington, DC: The White House, 2014). Accessed February 3, 2015, http://www.whitehouse.gov/sites/default/files/ndcs_2014.pdf; Drug Enforcement Administration, *2013 National Drug Threat Assessment Summary* (Department of Justice, 2013). Accessed February 1, 2015, http://www.dea.gov/resource-center/DIR-017-13 percent20NDTA percent20Summary percent20final.pdf.

[4] United States Senator Charles E. Schumer, *SCHUMER: IN RESPONSE TO NEW INVESTIGATION THAT FINDS ILLEGAL, ONLINE DRUG MARKET IS THRIVING & INFILTRATING LONG ISLAND, SCHUMER CALLS FOR TOP TO BOTTOM DEPT. OF JUSTICE REVIEW OF HOW "DARK WEB" DRUG SALES CONTINUE TO GROW – ALSO VOWS INCREASED FUNDING TO BETTER TARGET CYBER DRUG DEALERS*, 2014, accessed December 4, 2015, http://www.schumer.senate.gov/newsroom/press-releases/schumer-in-response-to-new-investigation-that-finds-illegal-online-drug-market-is-thriving-and-infiltrating-long-island-schumer-calls-for-top-to-bottom-dept-of-justice-review-of-how-dark-web-drug-sales-continue-to-grow_also-vows-increased-funding-to-better-target-cyber-drug-dealers.

[5] Ty McCormick, "The Darknet: A Short History," *Foreign Policy* January/February, no. 204 (2014): 5-6, accessed December 22, 2015, http://web.b.ebscohost.com/ehost/detail/detail?vid=3&sid=e5b97c8a-78f2-4fda-89ec-af64d49635da percent40sessionmgr111&hid=102&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ percent3d percent3d#AN=93911125&db=rgm.

[6] Chris La Morte, "Pirates or Patriots?" *Poptronics* 2, no. 5 (2001): 17-18, http://web.b.ebscohost.com/ehost/detail/detail?vid=7&sid=e5b97c8a-78f2-4fda-89ec-af64d49635da percent40sessionmgr111&hid=102&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ percent3d percent3d#AN=500739107&db=rgm; Ian Clarke et al., *Freenet: Retrieval System* (Santa Monica, CA: National Science Foundation, 2000), accessed December 23, 2015, http://snap.stanford.edu/class/cs224w-readings/clarke00freenet.pdf.

[7] Marie Claire Van Hout and Tim Bingham, "Responsible Vendors, Intelligent Consumers: Silk Road, The Online Revolution in Drug Trading," *International Journal of Drug Policy* 25, no. 2 (2014): 183-189, accessed January 1, 2015, http://dx.doi.org/10.1016/j.drugpo.2013.10.009.

[8] John W. Creswell, *Research Design*, 4th ed. (London: SAGE Publications, Ltd., 2014), 4, 17, and 183.

[9] Ibid., 185.

[10] Creswell, *Research Design*, 29, 66, and 187. Solveig Brownfeld, PhD, *How to Research and Write a Thesis* (Washington, DC: National Defense Intelligence College, n.d.), accessed April 9, 2016, https://niu.blackboard.com/@@/2458A3FF55CF7F9F4CABDF671422F6B5/courses/1/2015_22_MCR_701_QAC/ content/_258376_1/SKIM-pp57-89-Brownfeld-How percent20to percent20Research percent20and percent20Write percent20a percent20Thesis percent2C percent20May percent202010.pdf, 59-68; Robert K Yin, *Case Study Research* (Los Angeles: SAGE Publications, 2009), 19-20.

[11] Brooke Wells, Luther Elliott, and Bruce Johnson, "Internet Marketing of Illegal Drugs: Growing Evasions of International Drug Controls," in *International Society for the Study of Drug Policy* (New York: National Development and Research Institutes, Inc., 2015), accessed January 3, 2015, http://www.issdp.org/conferences/2009/papers/Wells_Elliott percent26Johnson_Internetmarketingofillegal; Van Hout and Bingham, "Silk Road, the Virtual Drug Marketplace," 385-391; Lillian Ablon, Martin C. Libicki, and Andrea A. Golay, *Markets*

for Cybercrime Tools and Stolen Data: Hackers' Bazaar, eBook, 1st ed. (RAND Corporation, 2015), accessed January 2, 2016, http://site.ebrary.com/lib/dialibrary/detail.action?docID=10858286; Anonymous, "The Amazons of the Dark Net; Illicit E-Commerce," *The Economist* 413, no. 8911 (2014), accessed January 4, 2015, http://search.proquest.com/docview/1619356697?accountid=10504; Ngo, *United Nations Office on Drugs and Crime Report*. Monica J. Barratt, "SILK ROAD: EBAY FOR DRUGS," *Addiction* 107, no. 3 (2012): 683-683, accessed January 2, 2015, http://onlinelibrary.wiley.com/doi/10.1111/add.12470/abstract; "Law Enforcement Struggles to Control Darknet," *The OSINT Journal Review*, last modified 2014, accessed March 10, 2016, https://osintjournal.wordpress.com/2014/12/31/law-enforcement-struggles-to-control-Darknet/; Kate Conger, "Have We Seen the Last of the All Writs Act in the Encryption Fight?" *Techcrunch.Com*, 2016, accessed May 14, 2016, http://techcrunch.com/2016/04/25/have-we-seen-the-last-of-the-all-writs-act-in-the-encryption-fight/; Ladar Levison, "Secrets, Lies, and Snowden's Email: Why I Was Forced to Shut Down Lavabit," *The Guardian*, 2014, accessed May 14, 2016, http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email; Mark Scott, "Data Transfer Pact Between U.S. and Europe Is Ruled Invalid," *The New York Times*, 2015, accessed May 30, 2016, http://www.nytimes.com/2015/10/07/technology/european-union-us-data-collection.html.

[12] Andy Greenberg, "Global Web Crackdown Arrests 17, Seizes Hundreds of Dark Net Domains," *WIRED*, 2014, accessed May 30, 2016, https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/; Kushner, "The Darknet"; Andy Greenberg, "German Police Just Made a Gigantic Dark-Web Drug Bust," *WIRED*, last modified 2016, accessed March 10, 2016, http://www.wired.com/2015/03/evolution-shiny-flakes-bust-heroin-cocaine-silk-road/; "Shiny Flakes Bust: 38 Houses Raided," Deep Dot Web, last modified 2015, accessed March 10, 2016, https://www.deepdotweb.com/2015/03/12/shiny-flakes-bust-38-houses-raided/; Littice Bacon-Blood, "Laplace 'Dark Net' Drug Ring Suspect on Probation When Arrested," *NOLA.com*, last modified 2016, accessed March 12, 2016, http://www.nola.com/crime/index.ssf/2016/01/laplace_Darknet_suspected_drug.html; Littice Bacon-Blood, "11 Jailed After $1 Million Xanax Pill Bust in Laplace," *NOLA.com*, last modified 2016, accessed March 12, 2016, http://www.nola.com/crime/index.ssf/2016/01/11_jailed_after_1m_xanax_pill.html#incart_river_index; Lauren McCauley, "'The Dream of Internet Freedom Is Dying,' Warns Top Civil Liberties Attorney," *Common Dreams*, last modified 2016, accessed March 14, 2016, http://www.commondreams.org/news/2015/08/06/dream-Internet-freedom-dying-warns-top-civil-liberties-attorney.

[13] *United States of America v. Blake Benthall, a/k/a "Defcon," Defendant*. T.H. 14 MAG 2427 (Southern District of New York 2014); Andy Greenberg, "Silk Road Creator Ross Ulbricht Sentenced to Life in Prison," *WIRED*, last modified 2015, accessed November 15, 2015, http://www.wired.com/2015/05/silk-road-creator-ross-ulbricht-sentenced-life-prison/; Marie-Helen Maras, "Inside Darknet: The Takedown of Silk Road," *Criminal Justice Matters* 98, no. 1 (2014): 22-23, accessed January 3, 2015, http://www.tandfonline.com.bia.idm.oclc.org/doi/pdf/10.1080/09627251.2014.984541; Brian Doherty, "How Buying Drugs Online Became Safe, Easy, and Boring: Silk Road Is Dead, but Anonymous Internet Sales of Illegal Substances Are Here to Stay," *Reason* 46, no. 8 (2015), http://go.galegroup.com/ps/i.do?id=GALEpercent7CA389798345&v=2.1&u=fbiacad_main&it=r&p=GPS&sw=w&asid=e3523927b6df54912039094512725f9b.

[14] Dr. Adam R. Winstock, *An Overview of Key Findings from Global Drug Survey 2015* (London: Global Drug Survey, 2016), accessed May 14, 2016, http://www.globaldrugsurvey.com/the-global-drug-survey-2015-findings; Christopher Ingraham, "Why Buying Drugs Online Is Safer than Buying Them on the Street," *The Washington Post*, 2015, accessed May 14, 2016, http://www.washingtonpost.com/news/wonk/wp/2015/06/15/why-buying-drugs-online-is-safer-than-buying-them-on-the-street/.

[15] Kari Paul, "Ross Ulbricht Sentenced to Life in Prison for Running Silk Road," *Motherboard*, last modified 2015, accessed May 14, 2016, https://motherboard.vice.com/read/ross-ulbricht-sentenced-to-life-in-prison-for-running-silk-road.

[16] Drug Enforcement Administration, "2013 National Drug Threat Assessment Summary"; Tony Payan, Kathleen A. Staudt, and Z. Anthony Kruszewski, *A War That Can't Be Won* (Tucson: University of Arizona Press, 2013); Philip Keefer and Norman Loayza, *Innocent Bystanders: Developing Countries and the War on Drugs* (Washington, DC: World Bank, 2010); Philip B. Heymann and William N. Brownsberger, *Drug Addiction and Drug Policy* (Cambridge, MA: Harvard University Press, 2001), 51-81; Anita Kalunta-Crumpton, *Drugs, Victims and Race* (Winchester, UK: Waterside Press, 2006). Drugabuse.gov, "Health Effects | National Institute on Drug Abuse (NIDA)," last modified 2015, accessed February 1, 2015, http://www.drugabuse.gov/drugs-abuse/commonly-abused-drugs/health-effects; "ODNI FAQ", dni.gov, last modified 2014, accessed December 16, 2014, http://www.dni.gov/index.php/about/faq?start=2; Williams and Felbab-Brown, *Drug Trafficking, Violence, and Instability*; United Nations Office on Drugs and Crime, *World Drug Report, 2014* (New York: United Nations Office on Drugs and Crime, 2014), 7-12; Substance Abuse and Health Services Administration Center for Behavioral Health Statistics and Quality, Results from the 2013 National Survey on Drug Use and Health. Drugabuse.gov, "Drugfacts"; "DEA.Gov / Statistics & Facts," dea.gov, last modified 2015, accessed February 1, 2015, http://www.dea.gov/resource-center/statistics.shtml. Ngo, *United Nations Office on Drugs and Crime Report*. Ngo, *United Nations Office on Drugs and Crime Report*.

[17] United Nations Office on Drugs and Crime, *World Drug Report 2015* (Vienna: UNODC, 2015).

[18] K. Jaishankar, "Space Transition Theory of Cyber Crimes," in *Crimes of the Internet*, Schmallager F. and Pittaro Med., 1st ed. (Upper Saddle River, NJ: Prentice Hall, 2009), 283-301, accessed March 14, 2016, http://www.sascv.org/drjaishankar/theory.html.

19. Ibid.

[20] Marcus Felson and Ronald V. Clarke, *Opportunity Makes the Thief: Practical Theory for Crime Prevention*, Police Research Series, Paper 98 (London: Policing and Reducing Crime Unit; Research, Development, and Statistics Directorate of the Home Office, 1998), accessed December 14, 2015, http://webarchive.nationalarchives.gov.uk/20110218135832/rds.homeoffice.gov.uk/rds/prgpdfs/fprs98.pdf.

[21] Ibid.

[22] George E. Higgins, "Digital Piracy, Self-Control Theory, and Rational Choice: An Examination of the Role of Value," *International Journal of Cyber Criminology* 1, no. 1 (2007): 33-55, accessed December 22, 2015, http://www.cybercrimejournal.com/georgeijcc.pdf.

[23] "Updated: List of Dark Net Markets (Tor & I2P)," Deep Dot Web, last modified 2013, accessed February 8, 2015, http://www.deepdotweb.com/2013/10/28/updated-llist-of-hidden-marketplaces-TOR-i2p/.
[24] European Monitoring Centre for Drugs and Drug Addiction, *The Internet and Drug Markets* (Luxembourg: Publications Office of the European Union, 2016), 35; Ryan Mac, "Who Is Ross Ulbricht? Piecing Together the Life of the Alleged Libertarian Mastermind behind Silk Road," *Forbes*, 2013, accessed December 14, 2015, http://www.forbes.com/sites/ryanmac/2013/10/02/who-is-ross-ulbricht-piecing-together-the-life-of-the-alleged-libertarian-mastermind-behind-silk-road/.
[25] United Nations Office on Drugs and Crime, "World Drug Report, 2014," 7-12; Substance Abuse and Mental Health Services Administration Center for Behavioral Health Statistics and Quality, *Results from the 2013 National Survey on Drug Use and Health*. Drugabuse.gov, "Drugfacts: Nationwide Trends | National Institute on Drug Abuse (NIDA)," last modified 2015, accessed February 4, 2015, http://www.drugabuse.gov/publications/drugfacts/nationwide-trends. "DEA.Gov / Statistics & Facts," dea.gov, last modified 2015, accessed February 1, 2015, http://www.dea.gov/resource-center/statistics.shtml.
[26] Population Reference Bureau, *2013 World Population Data Sheet* (Washington, DC: Population Reference Bureau, 2016).
[27] European Monitoring Centre for Drugs and Drug Addiction, *the Internet and Drug Markets*, 16.
[28] Ibid., 16.
[29] United Nations Office on Drugs and Crime, "World Drug Report, 2014"; Drugabuse.gov, "Drugfacts: Nationwide Trends | National Institute on Drug Abuse (NIDA)," last modified 2015, accessed February 4, 2015, http://www.drugabuse.gov/publications/drugfacts/nationwide-trends. "DEA.Gov / Statistics & Facts," dea.gov, last modified 2015, accessed February 1, 2015, http://www.dea.gov/resource-center/statistics.shtml. Ngo, *United Nations Office on Drugs and Crime Report;* Williams and Felbab-Brown, *Drug Trafficking, Violence, and Instability*; Andy Greenberg, "Feds and Scandals Can't Stop the Dark Web," *Slate Magazine*, last modified 2016, accessed March 13, 2016, http://www.slate.com/blogs/future_tense/2015/08/13/carnegie_mellon_study_dark_web_pushes_more_than_100_million_yearly_despite.html.
[30] Kyle Soska and Nicolas Christin, *Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem* (Pittsburgh, PA: Carnegie Mellon University, 2015) 44, https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf; Allison Schrager, "Economic Secrets of the Dark Web," *Quartz*, last modified 2015, accessed March 13, 2016, http://qz.com/481037/dark-web/; Andy Greenberg, "Feds and Scandals Can't Stop the Dark Web."
[31] Wells, Elliott, and Johnson, "Internet Marketing of Illegal Drugs." Van Hout and Bingham, "Silk Road, the Virtual Drug Marketplace," 385-391; Ablon, Libicki, and Golay, *Markets for Cybercrime Tools and Stolen Data.* Anonymous, *The Amazons of the Dark Net.* Ngo, *United Nations Office on Drugs and Crime Report.* Barratt, "SILK ROAD: EBAY FOR DRUGS," 683-683; *The OSINT Journal*, "Law Enforcement Struggles to Control Darknet."
[32] Greenberg, "Global Web Crackdown Arrests 17, Seizes Hundreds of Dark Net Domains."
[33] David Kushner, "The Darknet: Is the Government Destroying the Wild West of the Internet?" *Rolling Stone*, 2015, accessed March 12, 2016, http://www.rollingstone.com/politics/news/the-battle-for-the-dark-net-20151022; Greenberg, "German Police Just Made a Gigantic Dark-Web Drug Bust"; Deep Dot Web, "Shiny Flakes Bust: 38 Houses Raided"; Littice Bacon-Blood, "Laplace 'Dark Net' Drug Ring Suspect on Probation When Arrested," *NOLA.com*, last modified 2016, accessed March 12, 2016, http://www.nola.com/crime/index.ssf/2016/01/laplace_Darknet_suspected_drug.html; Bacon-Blood, "11 Jailed After $1 Million Xanax Pill Bust in Laplace"; Bacon-Blood, "'Dark Net' Drug Ring Suspects Indicted in St. John Parish"; McCauley, "The Dream of Internet Freedom Is Dying."
[34] Soska and Christin, *Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem*, 44.
[35] Operation ONYMOUS was a joint operation among Europol, the U.S. FBI, and U.S. Homeland Security Investigations that closed a total of 414 Darknet Marketplaces selling illicit goods, and led to the arrest of 17 people. Anna Sergi, "Social Science Helps to Tackle Organised Crime," *Jane's Intelligence Review* 27, no. 1 (2015), http://search.proquest.com/docview/1634993161?accountid=10504; Van Hout and Bingham, "'Silk Road,' the Virtual Drug Marketplace"; Van Hout and Bingham, "Responsible Vendors, Intelligent Consumers"; Will Martin, *Black Market Cryptocurrencies: The Rise of Bitcoin Alternatives that Offer True Anonymity*, eBook, 1st ed., 2014, accessed January 3, 2016, http://books.google.com/books?id=CRYCBAAAQBAJ&printsec=frontcover#v=onepage&q&f=false; James Dean, ''Dark Net' Drug Market Doubles in Size in a Year', *The Times* (London, England), 2015, accessed January 1, 2015, http://go.galegroup.com.

Sarah R. Heidenreich is currently an analyst with the Air Force Office of Special Investigations, where she specializes in cyber investigations and operations. She obtained a BA in International Studies and Spanish from Allegheny College in Meadville, PA, in 2009 and graduated with a Master of Science of Strategic Intelligence from National Intelligence University in 2016. Sarah was recently selected as the award recipient for the 2017 Women in Federal Law Enforcement's Elizebeth S. Friedman Intelligence Award of Excellence, and continues to pursue research interests regarding the evolution of the Darknet.

Dr. Dennis A. "Wes" Westbrooks II is the Director of Undergraduate Studies at the National Intelligence University. His writing and presentations primarily focus on intelligence studies but he has researched and written on numerous other topics relevant to the Intelligence Community. Dr. Westbrooks (SMSgt, USAF, Ret) served 26 years as an intelligence professional deploying three times on combat intelligence, surveillance, and reconnaissance missions over Afghanistan and Iraq on board the RC-135. Wes is a graduate of the National Defense University's Joint Professional Military Education program and holds a BS from Hampton University, an MS from George Washington University, and a PhD from Hampton University.

NANOKRIEG:
Attaining Global Net Superiority

by James Carlini

"Hit the Beach!" has been replaced by "Hit the Grid!" when it comes to charging fortified electronic defenses today. Does everyone really understand the difference?"

– James Carlini

It is time to put the von Clausewitz book, *Vom Kriege* (*On War*), down and realize the 21st century battleground has taken on very different dynamics as well as a change in the dimension of time related to attacks, counterattacks, and intervals between them. Cloud computing, the Internet of Things (IoT), the Internet of Everything (IoE), 5G Networks, FirstNet (the First Responders' Network), and other cutting-edge concepts will not materialize successfully in the future if their supporting intelligent infrastructure is not solid and resilient against attacks. Gaping holes, ineffective threat intelligence tools, lack of adherence to security policies, and hidden vulnerabilities in defensive, architectural frameworks against cyberattacks and EMP bombs will guarantee failure.

Compared to the *Blitzkrieg* (the Nazi Lightning War strategy) of the Second World War, the invention of new software-based weapons (e.g., Stuxnet, Flame, Nimda, Satan) has made many traditional weapons systems, defense platforms, and war strategies obsolete. The ability to have total synchronicity of multiple attacks on thousands of locations and precision timing down to the microsecond are just two key parameters providing a totally different definition of what a focused attack can accomplish in a targeted, asymmetrical war.

In the asymmetrical warfare approach of the Electronic Age, D-Day has become D-Microsecond. With new hardware platforms like HFT (High-Frequency Transaction) servers, the speed of war has accelerated to the microsecond, if not nanosecond. Welcome to the accelerated pace of "Electronic Jihad."

A question to ask all military services, government agencies, and civilian corporate data centers and server farms is: "Are your electronic assets fully protected?" They are not, according to the latest security studies.

NANOKRIEG: A CYBER WAR WON AND LOST IN MICROSECONDS

NANOKRIEG [a term copyrighted by the author], the "under a second" war, will be the next big conflict. Are we thoroughly prepared, militarily, politically, and from a national homeland security defense perspective, to meet this real threat and defeat it? HFT servers can send out a transaction to multiple locations every two to three microseconds. In less than a second, over 100,000 pinpoint cyberattacks on different targets can be executed by these high-speed transaction processors. Stocks could plummet. Exchanges could be totally manipulated and institutional accounts could be totally wiped out—or transferred.

Certain controls in power grids and other utilities, like maximum temperature levels or power load levels, could be overridden. All of this can be done without regiments of trained soldiers or tons of supporting equipment landing on some remote beachhead.

In some cases, the supporting equipment creating the attacks could be embedded and activated in the actual organization which is being attacked and not by equipment owned by the attackers themselves. Some major attacks could happen and no one would even know about them. Most are not reported, and you can understand why. Current "Threat Intelligence" tools do not capture and analyze all the information of a sophisticated attack.

Logistics also takes on an entirely different dynamic. Weapons do not have to be flown into a battle zone or brought in by carriers and big transport ships. The cyber weapons of today—malware and ransomware—are carried in electronically on the network. The burden of heavily coordinated logistics is lifted and strategy can be focused directly on the impact, scope, and intensity of the attack itself.

Trojan horses, worms, viruses, denial-of-service (DOS) attacks, destruction of service (DeOS), ransomware, RaaS (Ransomware as a Service), and other destructive malware weapons do not need huge supporting logistics or long time frames in order to coordinate and assemble to "Hit the Beach!" They can be sent off in a microsecond on an

electronic pathway to selected, multiple targets to "Hit the Grid!" the new war zone of the Digital Age. Moreover, they can be set up to hit several hundred times a minute.

> *Attack him where he is unprepared, appear where you are not expected.*
>
> - Sun Tzu, *The Art of War*

Cyberwarfare is the perfect tool for those engaged in asymmetrical warfare in which their traditional resources are inferior to those of their enemies. All they need is a small cadre of software experts, not a multi-billion-dollar arsenal of planes, ships, and tanks as well as all the trained personnel who go along supporting them. They do not even need a sophisticated data center with millions of dollars of high-speed servers and broadband connectivity linking them to the network. They can use their targeted victims' own computer installations, if they can get access to them.

When it comes to spending a significant amount of money on defending "intelligent infrastructure" (cyberinfrastructure), many military people and politicians already have an idea of where funding should go and what priorities it should have. The trouble is, many who talk about cyberattacks, cyberwarfare, and defensive strategies do not have a comprehensive or uniform view of what "intelligent infrastructure" is.

Intelligent infrastructure consists of the individual infrastructure layers of **Power** and **Broadband Connectivity** within the **Platform for Commerce** (see Chart 1). Both need to be resilient and redundant for mission-critical applications.

When it comes to cyberattacks, some who are pessimists would say it is not a matter of "if" the military or an organization will get hacked, it is more a matter of "when" it will get hacked. These pessimists may be considered realists as we see more significant cyber events unfolding.

Chart 1:
THE PLATFORM FOR COMMERCE
(5,000 years in the making)

LAYER	LEVEL	DOMINANT INITIAL DRIVER OF IMPLEMENTATION IMPORTANCE
SPACE (INTERPLANETARY) (FUTURE)	8	JUST BEGINNING TO BE BUILT ((Space shuttles, space station, satellite networks) Future: mid-21st century, 22nd century? U.S., RUSSIA, JAPAN, CHINA?)
BROADBAND CONNECTIVITY NETWORK (CYBERINFRASTRUCTURE)	7B (wireless) 7A (wired)	CHINA, JAPAN, S. KOREA, NETHERLANDS, U.S. (beginning 21st century, IBCs, IIPs & IRECs)
AIRPORTS	6	EUROPE, UNITED STATES (mid-20th century)
POWER (GRIDS, NUCLEAR POWER, OIL)	5B (nuclear) 5A (everything else)	UNITED STATES (beginning/mid-20th century)
TELEPHONE NETWORK (ANALOG VOICE ONLY)	4	UNITED STATES (beginning/mid-20th century)
RAILROADS	3	UNITED STATES (mid-1800s)
ROADS/BRIDGES	2	ROMAN EMPIRE (500 BC- 476 AD)
PORTS/ DOCKS/ WATER	1	PHOENICIANS (1200 BC-900 BC) EGYPTIANS (3000 BC-1400 BC)

KEY: INTELLIGENT INFRASTRUCTURE

As I stated in another white paper:

> Cyberwarfare is not a futuristic theory being discussed on one of the military channels by some obscure, software architect anymore. It is a common occurrence in today's global economy and it appears some are trying to test the electronic defenses we have set up on the Internet.

NANOKRIEG attacks are not measured in days or hours. An entire cyberattack may last only a couple of seconds—or less. A wave of attacks could come every couple of seconds. The battlefields are now in server farms, data centers, and across the network infrastructure.

FireEye, a global security company focused on providing comprehensive cyber-defensive platforms, released its annual Advanced Threat Report. Here is one part of its findings: Cyberattacks are hitting organizations once every 1.5 seconds on average, which is up 200% from the year before. The intensity of attacks is increasing as well as the frequency of launching them, which is also being accelerated.

According to the Ponemon Institute, cited in a recent Forbes Report titled "Enterprises Re-Engineer Security in the Age of Digital Transformation," a typical data breach in the private sector costs $4,000,000. What is the value of a data breach in a military or government application? Is it more than just a monetary figure? What other value is lost?

FROM PLATFORM FOR COMMERCE TO FRAMEWORK FOR WAR

The U.S. Army Corps of Engineers recently referenced my concept on infrastructure, the **"Platform for Commerce,"** as the "business definition of infrastructure and economic growth" in its handbook "Infrastructure and the Operational Art." The concept defines traditional infrastructure and its 5,000 years in the making from Level 1 – Ports/docks/water to Level 8 – Space (interplanetary).

When it comes to traditional infrastructure, physical assets are clearly understood and protected in all organizations. Digital assets, or virtual "electronic assets," and intelligent infrastructure in a power grid, a third-party cloud network, or in a data center, are sometimes overlooked, undervalued, and not looked at from a uniform perspective as to their critical value to the organization and, collectively, the nation. Hardening an organization's networks (and clouds) as well as its data centers is a critical step in ensuring its business continuity is impervious to cyberattacks and terrorism.

There is no Geneva Convention when it comes to cyberattacks. Every installation is fair game. The only limitations are the creativity of the attackers and the power of the malware they have created. Preparing for NANOKRIEG, the virtual cyber-*Blitzkrieg* of the 21st century, must be planned and designed into all intelligent infrastructure.

Now, especially with cyberwarfare becoming more prevalent, there needs to be a uniform framework defining the military infrastructure, its current strategies and tactics, and how they combine to successfully defend against all types of threats and potential conflicts in the layers defined in **MINDSET. MINDSET** stands for ***Military Infrastructure, Natural Destructive Strategies, Energy, & Tactics*** (see Chart 2). Part of the **MINDSET** framework focuses on **Cyberwarfare** and **EMP** (Electro-Magnetic Pulse) bombs. These are the two layers we will discuss.

Today's anti-virus and cyber defense tools are not fully matured, nor comprehensive enough, to cover all detection of breaching scenarios. All cyber tools need to improve and broaden their effectiveness as nothing has attained a full capability to block—let alone uncover—all attacks. Today, they leave much to be desired. Following a simple policy for digital asset protection can greatly improve overall security and add some extra protection.

Chart 2:
FRAMEWORK FOR MINDSET© (*MILITARY INFRASTRUCTURE, NATURAL DESTRUCTIVE STRATEGIES, ENERGY, & TACTICS – DEFENSE*)

TYPE OF WARFARE & WEAPONS	EFFECTIVE COVERAGE AREA	DEFENSES
Traditional	**Local, Regional, Continental, and Intercontinental**	*
Atomic	**Intercontinental**	*
Drone	**Local, Regional**	*
Bio	**Regional, Continental, and Intercontinental**	*
Entomological (Insects) (Potential delivery system for Bio)	**Local, Regional, and Continental**	*
Seismic (Tectonic)	**Regional, Continental, and Intercontinental**	*
Weather	**Local, Regional, and Continental**	*
Soundwave (Audio)	**Local (Future: Regional?)**	*
Lightwave (Laser)	**Local (Line-of-sight)**	*
EMP (Electro-Magnetic Pulse)	**Regional, Continental, and Intercontinental**	*
CYBER (Internet & Smartphones)	**Global**	*
Space	**Planetary & Interplanetary**	*

Source: James Carlini, 2017. All Rights Reserved. * Not disclosed at this time.

KEY: EMP & CYBER Layers – Areas of concern in this white paper for cyberattacks to Intelligent Infrastructure.

A recent article (http://www.defenseone.com/ideas/2016/06/no-more-cyber-maginot-lines-we-need-hunt-down-hackers-they-strike/128823/) suggested:

> We need to flip the script on traditional cybersecurity. US Air Force strategist Colonel John Boyd imprinted his mantra on a whole generation of military thinkers: "People, ideas, hardware—in that order!" Applying Boyd's dictum to cybersecurity suggests several potential changes in our approach to attracting and maximizing talent, in how we articulate the ideas undergirding government policy, and in how we use our technology.

Building upon Colonel Boyd's observation, let us discuss what ideas are in place.

"Air Superiority" is a well-established concept and totally accepted as a critical strategy in the overall military foundation of the Department of Defense (DoD). For decades, Air Superiority has painted a clear picture of squadrons of B-52s carpet-bombing an area or flights of A-10s wiping out tank divisions in the open desert. Everyone understands that intense umbrella of attack (and defense). We need to be as comfortable with talking about cyberwarfare and protecting intelligent infrastructure with the same type of phrases and applied superiority capabilities.

"Global Net Superiority" and its implications of having a resilient, intelligent infrastructure impervious to cyberattacks must have that same amount of "clarity of understanding" and broad executive acceptance by DoD, the National Security Agency (NSA), the Department of Homeland Security (DHS), and civilian corporate counterparts protecting electronic-based assets as well. Its definition and value to the organizations must be as clear as what "Air Superiority" is to all military units today, whose dependence on its strength and resilience is key to survival.

"Global Net Superiority" was defined in 2015 (http://iot.sys-con.com/node/3371377) by this author in this way:

> The United States has had Air Superiority since 1947. Its military has shown dominance on the land, sea and in the air for decades, but what about having Global Net Superiority today – and tomorrow?

DEFINING, AND DEFENDING AGAINST, SECURITY THREATS: THE LAST 9%

"Our analysis shows that upwards of 90% of all real world incidents fall into just 9 basic patterns when you slice through all the fear, uncertainty and doubt that's so common in the cybersecurity narrative." So

observes Bryan Sartin, Executive Director, Global Security Services, at Verizon on a 2017 podcast discussing the outcome and summary of its annual (2017) Data Breach Investigations Report.

In one respect, that sounds like a great starting point to build rigorous cyber defenses. You could cover 90% of all the different approaches following that research and those conclusions, but what about the other 10% that is left? 10% is a huge gap—huge enough to drive past all the other established cyber defenses and create a virtual avoidance of the digital Maginot Line created by those who think it is impenetrable.

When you are looking at cybersecurity, a 10% gap in security is totally unacceptable. One percent would probably be considered too large a gap but, if you can cover 90% of that final 10%, you would be well above anything that is currently in place.

No system is 100% secure. "Always-on resiliency" is not attainable. The goal should be to add that last 9% (the 90% of the final 10%) of cyber defenses that would block attacks. That is attaining Global Net Superiority.

When looking at a threat, we need to understand how motivated the attackers are. In many cases, if the attackers are amateurs they are going to go after the "low-hanging fruit" of applied security measures. (Often these amateur-level people are called "script kiddies.") In many organizations, those safeguards are disregarded by some of the system's users. Non-compliance to an organization's safeguards will definitely weaken the actual level of security and make it susceptible to amateur hackers.

Password protection and following security protocols are only as good as the percentage of users who adhere to them. If passwords are to be changed every 30 to 60 days, there should be strict administrative enforcement of that requirement. In the military, that means everyone from the private to the general, from the seaman to the admiral. No exceptions.

The same goes for every other designated protection and safeguard policy which is put in place for all system users to adhere to. Security policy and procedures need to be reinforced to users who will be looking for some easy shortcuts to employ on an everyday basis. 100% adherence to security policies and protocols in an organization provides a much higher level of security than one where only 70-80% of the organization's system users follow policy, but the other 20-30% of the users disregard the established procedures they should be following. Strict adherence applies to all third-party contractors as well.

There also needs to be a clear and uniform sense of urgency when it comes to adding updates and applying software patches to system software. If a patch for a certain vulnerability comes out on Tuesday morning, it should be applied later that day or, by the latest, the next day, Wednesday, because by the following Tuesday cyberattacks may start launching to try to take advantage of that known vulnerability.

This sounds so simple to follow and yet many large organizations do not have this sense of urgency in their systems area. They are the first ones to succumb to a major cyberattack. Their systems are brought down by this lack of urgency when it comes to applying security measures and/or software patches and upgrades. Some devastating attacks could have been totally avoided.

If the attackers are more sophisticated, or bent on an electronic *Jihad*, cyber defenses need to be thought out and implemented to a higher degree of sophistication, resistance, and impenetrability.

If you have amateur attackers with an urge to "break into something," they are going to try and, if they have no immediate success, they will move on to something easier to break into. On the other hand, if the attacker is bent on breaking into a particular agency or enterprise system, he/she will work much harder in trying to defeat its defenses or find its vulnerability.

In any military application, the security measures should match, or preferably exceed, the latter situation, where the attacker's tenacity (and sophistication) will be much greater. Nothing is at Global Net Superiority at this point. A higher level of defense is what we should be setting as a goal and striving for. There should also be a clear uniformity in the approach so we avoid the all-too-common excuse, "Well, that's the way we do it in the Navy," or the Army equivalent, "That's the Army way."

We do not need traditional "branch rivalries" in this area of concern. They cannot be tolerated in this mission-critical area. All that does is slow down the process of putting up real defenses and offenses. Everyone needs to work together—quickly.

A joint-service approach to security should be instituted, not just for developing a uniformity across all systems, but also in creating a good mix of perspectives, experience, and joint creativity in developing new security innovations. We need to pool all resources together to get to a stronger, uniform solution, rather than reinvent the wheel five times, waste time, and have all the resources not working together as a solid team.

Currently, the U.S. Navy's ONE-NET is the wrong approach. (ONE-NET is a Navy-wide initiative to install a common and secure IT infrastructure at OCONUS Navy locations; see article at http://www.public.navy.mil/fcc-c10f/nctsguam/Pages/ONE-NET.aspx). The Navy should be combining all its resources with other services to get the best capabilities in a uniform package that can be used across ALL services/branches. Think ALL-NET, not ONE-NET.

GETTING EVERYONE ON THE SAME PAGE FOR GLOBAL NET SUPERIORITY

As in understanding traditional infrastructure, everyone needs to adopt the same comprehensive view of the complete definition of intelligent infrastructure, especially before a huge initiative to develop all-inclusive safeguards and defenses is approved.

Too often the people around the table discussing issues and elements of what intelligent infrastructure consists of will not have the same perspective, experiences, and level of familiarity about the framework they are talking about. They all need to adopt and use a uniform set of terminology, descriptions, and visual framework for the elements they are discussing. This holds true especially when they start focusing on restricting access and/or increasing performance of the electronic infrastructure and its safeguards.

In light of the recent discussions about Russians hacking into the U.S. election process, the question becomes, "Are we susceptible to a broader cyberattack on intelligent infrastructure?" How much would we lose in a real cyberattack? Would the damages and "time to return to normalcy" be even greater than in a war waged with conventional weapons and/or atomic weapons?

That would be a great set of questions to discuss. Furthermore, it should be one with the President as well as other key Cabinet members present (to include NSA, DHS, and the Pentagon). That discussion should be forthcoming soon and arranged to be on an ongoing basis.

No one has an exact handle on what the Russians did from a cyberattack standpoint in the last couple of years. Any intelligence agency saying it has "everything covered (or uncovered)" is reaching for straws.

The agencies should go back and realize that some intrusions might not be uncovered for a year—or more. Read the security studies by some of the industry leaders (Verizon, CISCO, FireEye, Flashpoint, etc.). If they are saying their surveys of over 1,000 or more sophisticated enterprise centers worldwide are revealing breaches not found for over a year, do you really think some of the antiquated election systems of the states run more by patronage workers than by real cybersecurity engineers are going to be that infallible to conclude they have found everything?

CARLINI-ISM: ***NANOKRIEG is war in a new dimension beyond Blitzkrieg and Maskirovka.***

CYBER THREATS AND THEIR RESOLUTIONS: KEEP IT SIMPLE

Those discussions should be focused on bringing the threats and their solutions into a conversation which everyone can understand. Rather than trying to impress someone with obscure technical terms, the "apples and oranges" approach to discussing complex technology issues brings forth a quicker, more agreed-upon resolution and comprehensive, uniform action plans across diverse leaders and technical engineers.

As to "Best Practices" in defenses for asymmetrical warfare and cybersecurity, it is such an ever-changing area that "Best Practices" are a fast-moving target when it comes to available technologies as well as cybersecurity. We must remember, "Building for the future means advancing from the past."

Do not get hung up on long discussions of "Best Practices" when it comes to cyber and asymmetrical warfare. Let the pseudo-experts tackle that. Cybersecurity is always adapting as cyberattacks are always transforming and morphing into different approaches. It is more a matter of focusing on a quality methodology of Total Continual Improvement (TCI) or establishing "Leading Practices" that constantly adapt because everything is moving and transforming at a fast pace. (Think "Kaizen" – methodology for continuous improvement.) What was considered a "Best Practice" last year could be totally obsolete this year. Those who point backward to what they accomplished or established in security policies are usually pointing at something already considered obsolete by those looking and aiming forward.

"Leading Practices" is a better operational policy to adhere to. "Leading Practices" means you are constantly reviewing and updating your "Best Practices" rather than sitting back and pointing to what you put in place three years ago expecting accolades from your peers. (Three years is more than a lifetime for cybersecurity issues.)

There are some basic "dos and don'ts" of system security which would have prevented the broad impact of the WannaCry Attack of over 150 countries at once on May 12, 2017 (see Chart 3).

Chart 3
BASIC DOs AND DON'Ts OF SYSTEM SECURITY

DO FOLLOW	DO NOT
All system security procedures (follow ALL policies).	Pick and choose security procedures that fit your own approach to security.
Password change schedules.	Keep the same password or use something easy to break, like your name, dog's name, car model, etc.
A clear sense of urgency when updating systems and software versions.	Lag behind in updating hardware and/or system/app software.
Applying the latest system changes, software patches, and password update (an automated process is preferable).	Disregard or wait when applying updates, patches, or other software on ALL programs.
Avoidance of posting security items or bragging about the system components you use at work on LINKEDIN, Facebook, or other social media tools.	Give out your UserID or password to anyone of whom you are unsure. Or add system configuration description or other information to any LINKEDIN or Facebook page.
Whatever enterprise restrictions there are on working outside of the organization's facilities.	Work on planes, trains, or in other areas where someone can read over your shoulder.

We Need to Protect Cyberinfrastructure Today – If We Want to Use It Tomorrow

Besides a totally different type of platform in which to wage war, it is virtual in its form, not a physical landscape or territory which we are protecting and defending. We must change our vision of conflict and attack vectors as well as developing a comprehensive perception of strategic defenses. All must understand what is needed for combat and reflect the necessary changes in their offensive and defensive arsenals as well as their related policies and procedures (see Chart 4).

CARLINI-ISM: ***There are no Frontlines any more, only virtual lines within electronic borders in NANOKRIEG.***

Chart 4:
COMPARISON OF BLITZKRIEG TO NANOKRIEG

	BLITZKRIEG	NANOKRIEG
TYPE OF ATTACK	Physical	Virtual
WEAPONS	Planes, tanks, artillery, and mechanized cavalry	Software bugs, worms, DoS attacks, Ransomware, and Malware
PERSONNEL	10,000s, if not more	1, 2, or 3
TIME TO EXECUTE	Days	One second (the time it takes to depress the Enter key)
BATTLEGROUND, BATTLEFIELD	Geographic region (one or two countries, limited by resources on hand)	Global impact (the WannaCry Friday attack immediately infected 1000s of computers across 150+ countries)
COST TO WAGE	Significant	Comparatively insignificant
TIME TO LAUNCH SECOND WAVE/SECOND FRONT	Days, if not weeks, to organize the logistics	Seconds, if not less

We need to get away from prescribing and funding the last war's solution for strategies and resources to fight the next war. Think of evolution.

Cavalry → Armored Cavalry → Air Cavalry → Cyber Cavalry

We have already seen this in multiple instances in the retail industry, where customers' credit card and personal information are stolen. Where were the safeguards? Where were the defenses against these types of attacks? If they were in place, were they fully utilized or overlooked by the systems administrators and system users?

According to IBM, almost one out of every four financial institutions (23.8%) is still exposed. For all the talk about instituting network safeguards, many major organizations and their mission critical applications are still vulnerable.

Sometimes, the attack itself has taken months to be detected in organizations. How can we defend against attacks and be aware of the immediacy of a problem, if we cannot detect some intrusions for months?

We are far from having *Global Net Superiority* across our data centers, server farms, power grids, networks, and the rest of the Intelligent Infrastructure in the United States. Full database and applications security is a must have, not a hoped for. In some cases, Chief Information Security Officers (CISOs) at some organizations have not been earning the checks they have been cashing.

FIGHTING AN ASYMMETRICAL WAR

The United States, as well as other nations, continues to spend hundreds of billions of dollars on physical weapon systems for traditional land, air, and sea battles, but how much are we spending on electronic warfare and cyber infrastructure defenses? Is that federal funding adequate? Are we spending enough?

CARLINI-ISM: ***Death by 1,000 cuts has been replaced with death by 1,000 bytes.***

The question becomes: Are we going to fight the next war on land, sea and in the air? Or is it going to be fought electronically between data centers or data centers and rogue server farms running viruses and destructive software? We clearly have *Air Superiority*, but do we have anything even close to *Global Net Superiority*?

New skills are needed to solve new challenges and we should not be relying on the "traditional approaches" to conventional warfare. We have "Top Gun" schools to improve skills and techniques for *Air Superiority*, but yet we have nothing comparable for improving cyber skills for *Global Net Superiority*.

CARLINI-ISM: ***Building for the future is a very hollow statement, when funding and resources are aimed toward maintaining the past.***

Battle scenarios are going to be something totally different compared to what traditional "military experts" are thinking. Asymmetrical wars are fought differently. Should we be spending our money and resources in a different direction? The short answer is "yes."

Terrorist countries do not have the resources to build multi-billion-dollar ships and billion-dollar air superiority fighters. They do not have the skill sets to develop and build an equivalent to the F-35 fighter, nor the money and trained personnel to sustain a full carrier battlegroup consisting of carriers and heavy cruisers.

What they do have is the talent to build powerful and elusive software viruses, Trojan horses, Denial of Service (DoS) Attacks, ransomware, and other types of destructive malware needed to bring down systems, infrastructure, power grids, and total economies in an asymmetrical war. Moreover, these types of weapon systems can act in a fraction of a second to take hold.

Quickness is the essence of the war.

– Sun Tzu**,** *The Art of War*

Launching an "attack" requires a lot less time in coordinating logistics and resources. Hence, the new term, NANOKRIEG: War in less than microseconds. We need to build electronic defenses against NANOKRIEG as well as offensive weapons.

CARLINI-ISM: ***Speed of "attack denial" response equals victory or, at least, survival in NANOKRIEG.***

If we look at the **EMP** and **CYBER** layers of the **MINDSET** framework, it is critical to adopt uniform standards in order to move forward in building critical elements of intelligent infrastructure and be able to communicate with those personnel in different agencies as well as different disciplines to develop and insure a solid, resilient defense. When it comes to education of our military forces involved in cyberwarfare, we need to ensure they are coming in with the right educational foundation to assimilate into jobs requiring skill sets not necessarily taught in the public school systems.

THE MILITARY NEEDS TO RE-THINK EDUCATION

When it comes to education, we need to get out of the old, Industrial Age mindset of **"The Three Rs**" and get into **FACT**-based skill sets in education. **The Three Rs** are Rote, Repetition, and Routine (see Chart 5).

These were the skill sets taught in public schools to assimilate a workforce to move into Industrial Age factory jobs. Unfortunately, we are well beyond the Industrial Age. We are well beyond the Information Age.

Chart 5: THE THREE Rs of INDUSTRIAL AGE SKILL SETS

SKILL SET	REASON
ROTE	In factory jobs, there were some job functions that had to be memorized by the worker.
REPETITION	Many jobs had repetitive tasks associated with them, especially assembly line jobs.
ROUTINE	Assembly line jobs were compartmentalized and once you learned your 3-5 job functions it became a very routine job for the 8-hour shift.

Source: James Carlini, *Location, Location, Connectivity*, 2014.

We are at the mobile Internet age where we have to understand and apply new concepts for applications that focus on anything, anywhere, at any time for anybody, as the working framework. Unfortunately, some of our educational processes are still hung up on ***The Three Rs***.

CARLINI-ISM: ***Creating new conceptual frameworks for military strategies means tearing down obsolete education and curricula.***

What is needed today is a different set of skills for young people to adopt and apply. **FACT**-based education focuses on ***Flexibility, Adaptability, Creativity, and Technology*** skill sets (see Chart 6). These are the skill sets necessary for next-generation workers as well as military personnel working on cyber-defense and electronic weapons platforms.

Chart 6: FACT-BASED SKILL SETS

SKILL SET	REASON
FLEXIBILITY	Learning a couple of skills today does not set you up for a lifelong career. Lifelong learning and learning how to be flexible are critical.
ADAPTABILITY	Jobs are not that "routine" anymore. Things change and the worker needs to adapt to sometimes constantly changing conditions.
CREATIVITY	How do you attack a problem? Solutions evolve as challenges change. Creative people are needed for innovation as well as defining alternatives for dynamically changing environments.
TECHNOLOGY	Every industry has been touched by computerization. Computer skills have become "basic skills" you must have in order to be viable in the workforce.

Source: James Carlini, *Location, Location, Connectivity*, 2014.

Advancing from Clausewitz's observations (see Chart 7), which are cut-and-dried and do not reflect the new framework of war in a cyber world, we need to go beyond his perspective. From Clausewitz's *On War*:

If we take a general view of the four elements composing the atmosphere in which war moves, of *danger*, *physical efforts*, *uncertainty*, and *chance*, it is easy to conceive that a great force of mind and understanding is requisite for being able to make way with safety and success among such opposing elements, a force which, according to the different modifications arising out of circumstances, we find termed by military writers and analysts as *energy*, *firmness*, *staunchness*, *strength of mind, and character*.

All these manifestations of the heroic nature might be regarded as one and the same power of volition, modified according to circumstances; but nearly related as these things are to each other, still they are not one and the same, and it is desirable for us to distinguish here a little more closely at least the action of the powers of the soul in relation to them.

In the first place, to make the conception clear, it is essential to observe that the weight, burden, resistance, or whatever it may be called, by which that force of the soul in the general is brought to light, is only in a very small measure the enemy's activity, the enemy's resistance, the enemy's action directly. The enemy's activity only affects the general directly in the first place in relation to his person, without disturbing his action as commander. If the enemy, instead of two hours, resists for four, the commander instead of two hours is four hours in danger; this is a quantity which plainly diminishes the higher the rank of the commander. What is it for one in the post of commander-in-chief? It is nothing.

Chart 7 – von CLAUSEWITZ, PRUSSIAN MAJOR GENERAL, LEVELS OF WAR

THE LEVELS OF WAR
POLICIES
STRATEGIES
TACTICS

Carl von Clausewitz, Prussian Major General (1780-1831, wrote *On War – Vom Kriege*) – The Levels of War – Time, Space, and Mass.

In comparison to Clausewitz's observations, "physical efforts" are replaced today with electronic or "virtual efforts." There have also been some new variables added. One is velocity of attack.

How long would it take to mount a planned second wave attack? Several days, maybe the next day at best? What about an unplanned second wave? Weeks, if not months? The velocity in NANOKRIEG can be several seconds—or at the most, for a second wave.

Attacks are coming in on a whole different virtual plane which has very different dimensions of time and space. Our strategies and tactics must adjust for this new warfare (see Chart 8).

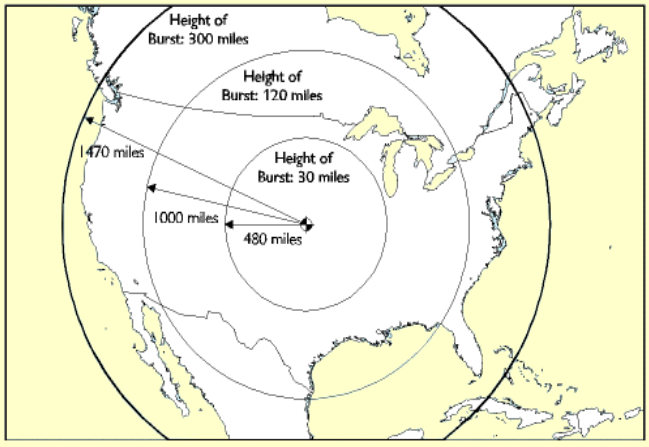
Chart 8 - NEW FRAMEWORK FOR WAR IN NANOKRIEGIAN WARFARE

LAYER OF INFRASTRUCTURE	ATTACK LOCATIONS	VELOCITY of ATTACK	RESIDUAL DAMAGES
NETWORKS	LOCAL REGIONAL NATIONAL CONTINENTAL GLOBAL	(Days, Hours, Minutes, Milliseconds, Microseconds)	MORALE (PSYCHOLOGICAL), SERVICE OUTAGE, ECONOMIC IMPACT, DIMINISHED PRODUCTIVITY
POWER GRIDS	LOCAL REGIONAL NATIONAL CONTINENTAL GLOBAL	(Days, Hours, Minutes, Milliseconds, Microseconds)	MORALE (PSYCHOLOGICAL), SERVICE OUTAGE, ECONOMIC IMPACT, DIMINISHED PRODUCTIVITY
OTHER INFRASTRUCTURE GRIDS (Gas, Pipelines, Transportation)	LOCAL REGIONAL NATIONAL CONTINENTAL GLOBAL	(Days, Hours, Minutes, Milliseconds, Microseconds)	MORALE (PSYCHOLOGICAL), SERVICE OUTAGE, ECONOMIC IMPACT, DIMINISHED PRODUCTIVITY
MILITARY GRID	LOCAL REGIONAL NATIONAL CONTINENTAL GLOBAL	(Days, Hours, Minutes, Milliseconds, Microseconds)	MORALE (PSYCHOLOGICAL), SERVICE OUTAGE, DIMINISHED OFFENSIVE & DEFENSE CAPABILITIES

EMP (ELECTRO-MAGNETIC PULSE) BOMBS

Instead of going through a long definition of all the concepts relating to EMP bombs, let me summarize by saying you do not want any EMP explosion overhead of your data center, electronics, or any personal communications devices. Once the pulse is triggered, the pulse will devastate all electronic devices which do not have any shielding. The direct coverage area of the EMP's effect is shown in Diagram 1.

DIAGRAM 1 – EMP COVERAGE



Area Affected by an Electromagnetic Pulse, by Height of Burst

Source: Gary Smith, "Electromagnetic Pulse Threats," testimony before the House National Security Committee, July 16, 1997.

We are at a point where a rogue nation has the delivery system to deliver an EMP bomb 100 to 150 miles above the continental United States. It does not need pinpoint accuracy to deliver a warhead to a specific city when just getting it 100 to 150 miles

overhead can deliver a much more devastating blow across a larger geographic area. 300 miles overhead takes out most of the continent.

An EMP bomb would do a lot more permanent damage across a region than several bombs targeted on one city. No working electronics equal going back into the early 1800s. This is why every data center and critical network hub should be EMP-proof. This was something discussed back in the Cold War and should be at the top of the list today.

Too many organizations—government, military, and civilian—depend on mission-critical applications and communications-based information systems. They cannot afford unshielded data centers and networks. This includes FirstNet, the first responders' communications network being designed today. Is it EMP-proof? I do not think so.

CREATING AN IMPERMEABLE DEFENSE

This is what the goal should be for all organizations concerned about improving cyber-defenses:

First, to ensure all critical electronics are covered with some type of defensive shielding, like a Faraday cage in order to negate the effects of an EMP explosion.

Second, to create the Global Net Superiority capability within all their networked computer installations. Impermeable defenses would negate most rogue attacks. Remember, nothing is 100% secure or totally reliable. We can only strive to get close to that 100% goal (99% is not as good as 99.9% and that is not has good as 99.99%).

Third, to know the basics, practice the basics, and make sure you have 100% participation and adherence to security policies (see Chart 9).

Chart 9: BASIC POLICIES TO ADOPT

KNOW YOUR SYSTEM(s)	Know the exact software you have. Know the exact versions of software you are running. Have an up-to-date inventory. Practice the Do & Don'ts in CHART 3.
KNOW YOUR CONFIGURATION	Have a Network Configuration Map. EVERY exact device should be listed on it. You would be surprised at how many organizations cannot produce an 8 ½ x11 piece of paper that shows their total installation or network configuration.
KNOW YOUR LIMITATIONS	Know what your limitations are as to software, systems, and personnel.
KNOW YOUR TRAFFIC & APPS	What analysis tools do you have? Are they helping you understand the flow of transactions and traffic? If not, get rid of them and start over. Do NOT maintain obsolete software or old, legacy systems that cannot be fully protected.

Fourth, which will be discussed in a future article, to create an offense to cyberwarfare. Besides Stuxnet and Flame, what else is being developed? Can we build something to send directly back to the source of the malware? It is easier said than done because you can use a third party's host computer/server to launch the attack. You need to be able to find the true originator of the attack and not the host server he/she has commandeered as the backup rogue server. That takes some sophisticated intelligence, but it does not rule it out.

Fifth, if you decide to use a third party, to ensure he/she institutes a quality program to support your applications (see Chart 10).

Chart 10: DEFINING ROLES AND RESPONSIBILITIES WHEN THIRD PARTIES ARE USED

FACILITY OWNERSHIP	SET OF POLICIES & PROCEDURES	INVENTORY	RESILIENCY FACTOR?
Your Organization	**Yes**	**Accurate accounting**	**Yes**
Outside Third-Party	**Yes/****	**Accurate accounting**	**Yes*****
Network Carrier/ Other Vendors	**Yes/****	**Accurate accounting**	**Yes*****

KEY:

** Your organization must have oversight for others (third-party outsourcers and any vendors) in place (and followed). Why? You are the one in charge of all decisions.

*** Organization should check the actual infrastructure to ensure there are no single points of failure and "Recovery Plans" should be tested annually, at a minimum. Recovery plans should be re-engineered and thought through to be more focused on "business continuity" rather than the approach of a systematic shutdown and then a systematic re-boot of the hardware and applications (the traditional Disaster Recovery approach for systems).

CONCLUSION

We need to move forward rapidly in these areas because other nations are moving forward in cyberwarfare as well. We have yet to establish Global Net Superiority and that should be the primary mission across all military, government, and civilian organizations for intelligent infrastructure.

[Author's Note: More details will be discussed in my upcoming book, *NANOKRIEG: Beyond Blitzkrieg*. My earlier book, *Location Location Connectivity: Next-Generation Real Estate, Intelligence Infrastructure, Technology, and the Global Platform for Commerce,* published in 2014, is also recommended.]

James Carlini is a visionary and strategist for mission-critical networks, technology, and intelligent infrastructure. He has been president of his own consulting firm since 1986. Holder of the MBA degree, he is a former award-winning adjunct faculty member at Northwestern University in both its executive master's and undergraduate programs (1986-2006), developing and teaching courses in technology management, team dynamics, Six Sigma, network security, and international applications of technology. His original "Platform for Commerce" definition of infrastructure and its impact on economic growth is referred to in the U.S. Army Corps of Engineers' handbook, Infrastructure and the Operational Art *(2014). Jim served in the Air National Guard and the U.S. Army Reserves from 1972 to 1985.*

The Specter of Cyber in the Service of the Islamic State: The Zeros and Ones of Modern Warfare

by Troy E. Smith

Rouse him, and learn the principle of his activity or inactivity. Force him to reveal himself, so as to find out his vulnerable spots.

- Sun Tzu

SUMMARY

There is a cyber-electromagnetic contest between nation-states and the Islamic State, which involves gaining, maintaining, and exploiting technological advantage. The expansion of the Islamic State (ISIS) over the last two years has included capabilities to inflict damage over the Internet and manipulate the resources of cyberspace for recruitment and the spread of propaganda. ISIS has employed a cyber-strategy that utilizes asymmetric warfare and adaptive tactics based on the Fourth Generation Warfare (4GW) model. In this article the overarching strategy proposed by the author is analysed by comparing it to the tenets of Social Learning Theory and terrorist strategies presented by Kidd and Walter (2006): intimidation strategy, provocation strategy, and outbidding strategy. To effectively challenge ISIS in the cyber-electromagnetic contest requires analysis of its strategies and tactics to determine effective ways to mitigate the threat and to develop a base for anticipatory intelligence.

INTRODUCTION

The reach of terrorism has become increasingly pervasive in what David Rapoport has coined the "Fourth Wave of Terrorism." The Islamic State of Iraq and Syria (ISIS) is the quintessence of this evolved form of terrorist, which has emerged with its own unique strategy. One key strategic change is the expansion of attacks from conventional forms on land and air to the digital realm of cyberspace. Over the years, ISIS activities have demonstrated the inclusion of cyber into its strategy. Rather than shunning Western technology, ISIS is leveraging society's addiction to this realm of human interaction and has evolved into a hybrid threat actor launching attacks that are innovative, networked, and technologically savvy. The Islamic State's approach to the use of the Internet is highly advanced and versatile compared to that previously observed with other terrorist groups. The group has proven its ability to capitalize on emerging technologies in order to establish and maintain cultural and social advantage, leveraging these new capabilities for command and control, recruiting, coordinating logistics, raising funds, mobilization, and propagandizing its message.[1, 2] Its effective manipulation of cyberspace has contributed to transforming this organization into a jihadist global movement and brand.[3]

Attacks on U.S. information infrastructure from malicious sources is an eventuality rather than a possibility. In 2008 the Department of Defense (DoD) reported that U.S. military systems were scanned or attacked more than 300 million times per day.[4] To date, ISIS activists have taken advantage of the approach by security agencies, which are oriented to target conventional methods of attack. This has allowed ISIS and its activists to outpace national security efforts.[5] There exists a cyber-electromagnetic contest, which involves gaining, maintaining, and exploiting technological advantage between nation-states and ISIS. To effectively challenge ISIS in this contest there must be analysis of its strategies and tactics with a view to determining effective ways to mitigate these threats and developing a base for anticipatory intelligence. This article looks at various interrelated strategies that leverage cyberspace to achieve the goals of ISIS, which may be extrapolated from its past and current activities.

CYBERSPACE: THE UNIQUE FOURTH THEATER OF INTERACTION

The cyber domain is distinct from the conventional theaters of military and intelligence interaction, i.e., land, sea, air, and space. What differentiates cyber from these other domains are four attributes inherent to the cybersphere. First, the cyber domain is a man-made domain. Second, military capabilities across the other domains are managed through the cyber domain. Third, military and civilian aspects of the cyber domain are often

intertwined and difficult to differentiate. Fourth, attribution within the cyber domain is difficult to assign, i.e., the anonymity that is intrinsically possible in the cyber domain makes identifying the source of cyber actions extremely difficult.[6] These attributes combine to create an entirely novel domain of interaction necessitating a different decision-making model.[7]

The cyber domain supports instantaneous action from a distance, e.g., one can be anywhere in the world and launch an attack which occurs almost immediately.

While these are the primary attributes, there are also additional factors that make cyber unique and further justify the need for a proactive and targeted strategy for cyber defense. For instance, the cyber domain supports instantaneous action from a distance, e.g., one can be anywhere in the world and launch an attack which occurs almost immediately. This means that the activities of ISIS can transcend borders, making the entire world a potential target or victim. Anyone may become a victim of a cyberattack or a target for radicalization and recruitment through the dissemination of propaganda. Additionally, the attacks are asymmetric as there can be a one-to-many mapping of attacks; furthermore, a small nation-state or even a lone actor can cause major damage in cyberspace with the right skills and tools.[8] As a result of these attributes, terrorist groups with gang-like networks and technically proficient members, such as Junaid Hussain aka Abu Hussain Al Britani, aka Trick, the former head of the Cyber Caliphate, have developed tactics that confound nation-states.[9] Rabitat al-Ansar released a video in May 2015 titled "Message to America: From the Earth to the Digital World," vowing persistent hacking attacks on U.S. and European electronic targets.[10]

ISIS CYBER STRATEGY

The overarching strategic plan of action for ISIS's efforts in cyberspace is the creation and exploitation of cyber tactics, which can be easily adopted and adapted by ISIS supporters remotely. These nullify the greater resources and conventional methods of prevention used by the West, to establish and solidify ISIS as a brand. This strategy has a central influence in the establishment of ISIS's image and its unprecedented ability to recruit individuals to its cause. The enduring goal of these strategies is to achieve change at the level of regime, territory, and policy so as to seize social control and status quo maintenance.[11] This strategy is targeted at two unique but related groups, namely governments and individuals—government policies and actions it wishes to influence, and the support of individuals whom it seeks to entice through fear.[12] Powerful countries such as the United States prefer combat where only the strong wins.[13] However, ISIS's use of cyberspace has enabled it to circumvent the conventional forms of engagement used in the past. This circumvention allows it to effectively disseminate a message rallying Muslims to engage in violent struggle against oppressive Western nations and the "infidel" Arab regimes.[14] Global interconnectedness brought about through linked digital information networks brings immense benefits, but it also places a new set of offensive weapons in the hands of states and non-state actors, including terrorist groups. Military defense networks can be remotely disabled or damaged. Private sector networks can be infiltrated, disrupted, or destroyed.[15] The attributes of cyberspace align well with this strategy as it facilitates remote actions, asymmetric attacks, and access. ISIS has made no effort to hide its intent to use cyberspace in its jihad. In 2003 it published a manual which emphasized the power of an "electronic jihad," which included participation in forums and hacking.[16]

Well before the 9/11 attacks, Al-Qaeda recognized the power of asymmetric warfare and adaptive tactics for its jihad struggle.

Well before the 9/11 attacks, Al-Qaeda recognized the power of asymmetric warfare and adaptive tactics for its jihad struggle.[17] This came from the terrorist group's understanding of the power which could be derived from Fourth Generation Warfare (4GW). 4GW strategy is based on redefining or bypassing what could be defined as traditional strengths; conflict shifts focus from destroying military targets and conventional forces to targeting social order. Threat actors target a societal framework, laws, technology, and ideologies.[18] ISIS has followed this strategic model of turning technology into a quantum force multiplier. This form of attack also poses a unique problem as not only is it asymmetric but it also has the ability to retaliate by kinetic means unhindered by the definition of force in international law. Michael Schmitt, an international legal scholar on "use of force" issues, after carefully considering Article 2(4) of the United Nations Charter and its application, holds that cyberattacks must fit into a traditional, consequence-based frame of reference to qualify as armed force. Schmitt's criteria have generally been accepted in recent years.[19] This empowers ISIS as it forces nation-states into a mostly defensive position. Therefore, the tactical use of this method is disproportionately advantageous to ISIS.

The 4GW strategy provides a framework for the development of other more specific strategies which allow for tailored use of the cyber resource to derive specific desired outcomes. These strategies are intimidation strategy and provocation strategy.

INTIMIDATION AND PROVOCATION STRATEGIES

The intimidation strategy is based on deterrence; it creates a scenario wherein the enemy determines action as not cost-effective. Thereby, the terror group can influence political action or the action of individuals by means of threats and actions that demonstrate the resolve to do actual damage. Execution of this strategy demonstrates the reach and power of the terrorist group. It has a secondary objective of demonstrating, enticing, and encouraging supporters who see this as an irrefutable sign of power on the part of the terrorist groups and powerlessness on the part of the state. This strategy not only engages the country/ countries of interest but also their supporters with the goal of making defense undesirable due to the possibility of retaliation.

The provocation strategy aims to goad the target nation into a military response which will harm civilians in the terrorist group's home territory.

The provocation strategy aims to goad the target nation into a military response which will harm civilians in the terrorist group's home territory. This will fortify the propaganda that the nation is oppressive, evil, and unsympathetic and must be vigorously resisted and replaced. This strategy can shift support away from the nation's government by its own citizens as was seen in the 2003 invasion of Iraq. After September 11, 2001, the United States invaded Iraq, claiming links between Al Qaeda and the Ba'athist regime. This activity resulted in opposition external and internal to the U.S. It also distracted attention from the activities of Al Qaeda and allowed the U.S. to be villainized.[20] Opportunistically, Saddam Hussein began to convey a more Islamic, religious appearance in Iraqi media, showing himself praying at mosques and supporting the Palestinian cause, possibly hoping to reframe the war as a struggle against Western imperialism and Israeli scheming. This provocation strategy as used by ISIS in cyberspace has not been tremendously successful thus far, as the damage done by cyberattacks has not been sufficient to warrant a kinetic reply. However, due to the potential threat of cyberwarfare, the U.S. continues to examine how a kinetic reply can qualify as *jus ad bellum* after a cyberattack in relation to Article 2(4) of the United Nations Charter.

The strategies of intimidation and provocation are executed as attacks on websites and social network accounts, and as data theft, which forms part of ISIS's offensive activity referred to as *ghazwa* (raid/attack in Arabic).[21] Prominent examples of this type of cyberattack are evident in ISIS's takeover of U.S. Central Command social media accounts and attacks on more than 19,000 French websites in the week following the attack on the *Charlie Hebdo* office in Paris. Further, Kurdish Peshmerga forces have attested to ISIS's use of social media as part of an intimidation strategy.[22] Almost a year before the conquest of Sinjar and Makhmour, ISIS used social media to show its willingness to brutally kill its enemies, even children.[23] This use of the cyberspace allows ISIS to portray itself as an unstoppable behemoth with a willingness to kill in the most sadistic ways. This can be seen as an effective use of psychological warfare.

OUTBIDDING STRATEGY

Technology also facilitates another strategy that focuses on people rather than the enemy at large, i.e., a people-centric strategy (hearts and minds). The strategy identifies that people and ideas are the essence of conflict and determine rhythm and duration of battle. Therefore, the strategy employs tactics (cyber) which utilize a resource through which most of the world's population can be reached for radicalization, propaganda, or the exhibition of power. This people-centric strategy can be compared to the traditional outbidding strategy described by Kydd and Walter (2006).[24] It is the mechanism which can turn a passive supporter into an active member. In early 2016, then-U.S. President Barack Obama stated that ISIS uses the Internet and social media to recruit young Muslims to the group by radicalizing their views.[25]

The outbidding strategy is employed when two parties are competing for support of undecided individuals, or even decided ones. Parties try to present cases that show they best represent the individual's interests. Foreign Terrorist Fighters (FTF) and "Lone Wolf" terrorists can be considered a product of an outbidding strategy employed by ISIS against target nation-states. This strategy representing oneself as a zealot actually enhances the attractiveness of the group.[26] The terrorists demonstrate this by assuring their willingness to continue armed struggle despite its cost. They achieve this by publicizing their activities as widely as possible.

In general, this approach gratifies sympathizers and captures the imagination of potential recruits. The outbidding strategy utilizes six non-discrete narratives—brutality, mercy, victimhood, war, belonging, and utopianism. The Internet creates an environment in which these narratives are almost self-perpetuating, being quickly reworked and redistributed to increase the potential audience exponentially. This aids in creating spoken propaganda from afar without direct involvement. This propaganda engine takes many forms, including online magazines such as *Dabiq*, movies on YouTube, and mobile applications. The mobile application "Dawn of Glad Tidings" allowed ISIS to take control of the users of Twitter accounts to generate a high volume of Twitter activity in a coordinated manner and thus raise the online profile of the organization.[27] This not only attracts new supporters and solidifies ties with old ones but also sustains the group's global relevance.

Social media and other similar web services have emerged as the 21st century's "radical mosque."

The Internet brings people together based on personal interests and values. This benefits terrorists who have ideology and experiences that are generally viewed negatively by the majority. The Internet provides a medium where interested persons can engage and initiate contact or just gather information. For those already recruited or sympathetic to the ideology of ISIS, the Internet offers a source of support. Like-minded individuals can connect and encourage each other. The curious can have direct contact with former and current terror fighters where they can be encouraged by them and learn from them.[28] Social media and other similar web services have emerged as the 21st century's "radical mosque." The Internet provides access to a worldwide audience where information can be exchanged quickly and at low cost, while maintaining the anonymity of the user.[29] Through the use of web media and social media, ISIS can reshape the thinking of potential threat actors, i.e., radicalization.

CONCLUSION

Through its websites, newsletter, e-books, and social media, ISIS can with little effort increase its contact with potential recruits and maintain that contact over long periods of time, increasing the impact on individuals. It also presents persons who can be copied and idealized. These models can be tailored to suit various target groups. The main impact is augmenting the meanings individuals assign to specific actions and behavior. This can be applied specifically to the perception of what is right and wrong, which is heavily dependent on the individual's cognitive model. Additionally, social media and other online groups provide a support mechanism, which supplies positive reinforcement for terrorist behavior (deviant), i.e., differential reinforcement. It presents a message of immediate change, religious duty, self-assertiveness, and transformation. This increases the likelihood of initial and continued deviant behavior.[30]

To counter ISIS's cyber-based strategies effectively, these facets must be understood. Key components must be disassembled and a nuanced analysis applied to gain an in-depth understanding of the aims and objectives of its activities. Understanding the strategy behind ISIS actions will prevent misconceptions which can lead to flawed decision-making, which in turn stymie efforts to counteract its advances on the cyber battlefield. Today, counterterrorism strategies must consider the platforms employed by ISIS to leverage cyberspace and the effectiveness of its tactics. National security must use its own outbidding strategy to decrease the occurrence of FTF. Officials must create an online presence which is enticing to at-risk individuals and counter the trend of misinformation. This counter-strategy must embrace cyberspace to dismantle the rhetoric of the terrorist groups so that the flawed logic can be highlighted and its Faustian underpinnings exposed. This may call for a revaluation of current information architecture and cyber strategies.

In the war on terror, the information war that wages between ISIS and the free world is no less important than the aspect of physical engagement conducted in geographic space.

Terrorists are using cyberattacks and social media operations to influence the beliefs of their enemies and the population they control. It is another way to effectively signal their reach/access, strength/capability, and resolve to use all available means to defeat their enemy. This exhibition of soft power, which is applied as part of 4GW, has proven quite effective in making ISIS a household name and allowing it to recruit an unprecedented number of international citizens. To defeat this threat vector which cyberspace represents, the strategies must be systematic and sustained. In the war on terror, the information war that wages between ISIS and the free world is no less important than the aspect of physical engagement conducted in geographic space.

[Editor's Note: This manuscript was submitted prior to recent dramatic successes on the battlefield that Western forces have experienced against the ISIS "caliphate." Nevertheless, despite the loss of huge expanses of physical territory by the group, its actions elsewhere in the world, and in particular in cyberspace, still pose a tremendous threat.]

NOTES

[1] Davis, Jeremy. "ISIS Cyber Caliphate Migrating to New Communications Platform." *SC Magazine*. Last modified 2016. http://www.scmagazine.com/isis-cyber-caliphate-migrating-to-new-communications-platform/printarticle/469537/.

[2] Platov, Vladimir. "ISIS Cyber-Caliphate." *New Eastern Outlook*. Last modified 2016. http://journal-neo.org/2016/02/10/isis-cyber-caliphate/.

[3] Sweet, Julia. "Online Trolling as a Strategy for Terrorists." *Modern Diplomacy*. Last modified 2016. http://moderndiplomacy.eu/index.php?option=com_k2&view=item&id=1487:online-trolling-as-a-strategy-for-terrorists&Itemid=487.

[4] Rosenbach, Eric. *Confrontation or Collaboration? Congress and the Intelligence Community*, 2009.

[5] Sweet, Julia. "Online Trolling as a Strategy for Terrorists." *Modern Diplomacy*. Last modified 2016. http://moderndiplomacy.eu/index.php?option=com_k2&view=item&id=1487:online-trolling-as-a-strategy-for-terrorists&Itemid=487.

[6] Brantly, Aaron Frnaklin. "The Decision to Attack: Military and Intelligence Cyber Decision-Making." University of Georgia, 2012.

[7] Payments Council. "Cyber Threat Intelligence: Criminological Review," 2014.

[8] Rosenzweig, Paul. "Thinking About Cybersecurity: From Cyber Crime to Cyber Warfare." The Great Courses, 2013.

[9] Wilson, G.I., John Sullivan, and Hal Kempfer. "Fourth Generation Warfare (4GW): Tactics of the Weak Confound the Strong," 2003. http://www.academia.edu/6797297/Fourth_Generation_Warfare_4GW_Tactics_of_the_Weak_Confound_the_Strong.

[10] Davis, Jeremy. "ISIS Cyber Caliphate Migrating to New Communications Platform." *SC Magazine*. Last modified 2016. http://www.scmagazine.com/isis-cyber-caliphate-migrating-to-new-communications-platform/printarticle/469537/.

[11] Kydd, Andrew, and Barbara Walter. "The Strategies of Terrorism." *International Security* 31, no. 1 (2006): 49-80.

[12] Ibid.

[13] Wilson, G.I., John Sullivan, and Hal Kempfer. "Fourth Generation Warfare (4GW): Tactics of the Weak Confound the Strong," 2003. http://www.academia.edu/6797297/Fourth_Generation_Warfare_4GW_Tactics_of_the_Weak_Confound_the_Strong.

[14] Hoffman, Adam, and Yoram Schweitzer. "Cyber Jihad in the Service of the Islamic State (ISIS)." *Strategic Assessment* 18, no. 1 (2015): 71-81.

[15] Waxman, Matthew. "Cyber Attacks as 'Force' under UN Charter Article 2(4)." *International Law Studies* 87 (2011).

[16] Hoffman, Adam, and Yoram Schweitzer. "Cyber Jihad in the Service of the Islamic State (ISIS)." *Strategic Assessment* 18, no. 1 (2015): 71–81.

[17] Wilson, G.I., John Sullivan, and Hal Kempfer. "Fourth Generation Warfare (4GW): Tactics of the Weak Confound the Strong," 2003. http://www.academia.edu/6797297/Fourth_Generation_Warfare_4GW_Tactics_of_the_Weak_Confound_the_Strong.

[18] Ibid.

[19] Waxman, Matthew. "Cyber Attacks as 'Force' under UN Charter Article 2(4)." *International Law Studies* 87 (2011).

[20] Chomsky, Noam. "Invasion as Marketing Problem: The Iraq War and Contempt for Democracy." *Mississippi Review* 32, no. 3 (2004): 88-93.

[21] Hoffman, Adam, and Yoram Schweitzer. "Cyber Jihad in the Service of the Islamic State (ISIS)." *Strategic Assessment* 18, no. 1 (2015): 71-81.

[22] Ibid.

[23] Filkins, Dexter. "The Fight of Their Lives." *The New Yorker*. Last modified 2014. http://www.newyorker.com/magazine/2014/09/29/fight-lives.

[24] Kydd, Andrew, and Barbara Walter. "The Strategies of Terrorism." *International Security* 31, no. 1 (2006): 49-80.

[25] Hoffman, Adam, and Yoram Schweitzer. "Cyber Jihad in the Service of the Islamic State (ISIS)." *Strategic Assessment* 18, no. 1 (2015): 71-81.

[26] Winter, Charlie. "The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy," 2015. http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/the-virtual-caliphate-understanding-islamic-states-propaganda-strategy.pdf.

[27] Hoffman, Adam, and Yoram Schweitzer. "Cyber Jihad in the Service of the Islamic State (ISIS)." *Strategic Assessment* 18, no. 1 (2015): 71-81.

[28] Winter, Charlie. "The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy," 2015. http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/the-virtual-caliphate-understanding-islamic-states-propaganda-strategy.pdf.

[29] Freiburger, Tina, and Jeffrey S Crane. "The Internet as a Terrorist's Tool: A Social Learning Perspective." Cyber Criminology: Exploring Internet Crimes and Criminal Behavior" (2011): 127-138.

[30] Ibid.

Troy E. Smith, a citizen of the Caribbean nation of Trinidad and Tobago, entered the field of intelligence in 2008 upon joining the Security Intelligence Agency of that country. His initial position was as an intelligence officer. Subsequently, he embarked upon several training endeavors, both regionally and internationally. As an analyst he has written a number of papers on the intelligence activities of the Chinese, on cybercrimes, and on the insider threat. After beginning work on an MA in Intelligence Studies degree at American Military University in the U.S., he chose to focus on the area of intelligence collection. Troy represents his agency on several committees and has served in various command centers over the last seven years. He is a frequent and valued contributor to AIJ.

Persistent Operational Intelligence: An Intelligence Strategy for Joint Force 2020

by COL (USAR) Reid W. Webber

OVERVIEW

This article develops a new intelligence strategy for Joint Force 2020 called Persistent Operational Intelligence. It analyzes the security environment, future Joint Force missions, and current intelligence doctrine to support theater security and combat operations. The project identifies the lack of a strategy to maintain continuous operational intelligence regarding key regional security environments and to understand the conditions where threats to the homeland originate. The article proposes a new strategy to create six geographic Joint Intelligence Task Forces staffed by assigned and aligned Joint Force intelligence units to support future operations. The Mission Commander for each Joint Intelligence Task Force will create unity of effort in order to synchronize intelligence plans, analysis, and operations through a network environment with new workflow and three-dimensional software to continuously apply intelligence resources of the Total Force. It concludes that the Persistent Operational Intelligence strategy will effectively synchronize military intelligence forces and improve America's ability to employ the Joint Force effectively to accomplish national objectives in complex security environments.

DISCUSSION

The global security situation has changed continually since the end of the Cold War. Before 1989 the United States faced a single strategic competitor, the Soviet Union. The U.S. currently faces multiple challenges from emerging competitors, terrorist networks, and regional instability that pose strategic threats to the homeland. The nation must transform the military that deterred nuclear war for over 50 years to meet these new challenges. Joint Force 2020 is America's military of the future. The new force synchronizes with diplomatic, economic, and information instruments of national power to create "whole of government" efforts for conducting theater security operations, deterring adversaries, supporting civilian authorities, and conducting combat operations to win the nation's wars.[1] Joint Force 2020 provides the nation a tremendous military capability, but does the nation have the ability to understand where and when to deploy the force in light of recent intelligence failures?

In September 2014 General (USA) Martin Dempsey, then-Chairman of the Joint Chiefs of Staff, outlined his vision for Intelligence, Surveillance, and Reconnaissance (ISR) for Joint Force 2020 and identified four main challenges given current processes: lack of common data standards, disjointed management of the ISR force, parochial ISR architectures, and increasing threat to systems and communications.[2] This article examines the conditions that create disjointed intelligence processes and operations in order to understand the root causes of GEN Dempsey's assessment. The analysis begins with the strategic security environment, Joint Force 2020, and the national intelligence structure. Furthermore, it describes current military doctrine and joint intelligence functions within the geographic combatant commands for theater security and combat operations, including lessons learned from recent operations. The goal is to determine if Joint Force 2020 has the appropriate intelligence structure and doctrine to meet future missions. The conclusion of the article proposes a new strategy, Persistent Operational Intelligence, to create the Intelligence Joint Force 2020 and support the nation's ability to effectively deter threats and defend the homeland.

The strategic security environment continues to change due to globalization and the end of the Cold War. The most challenging environments originate from regions of instability, such as failing states and emerging competitors which challenge peace and access to the global commons. Nations and terrorist groups that own, or seek to acquire, weapons of mass destruction pose the highest threat to the homeland and regional peace.[3] U.S. decision-makers require detailed knowledge and deep regional expertise to build a common strategy with like-minded nations and multinational institutions[4] to confront nuclear weapons proliferation by North Korea and Iran, while deterring military expansion by Russia and China.

Many of these regional hotspots are home to terrorist networks and illicit organizations that pose threats to the homeland, U.S. citizens, diplomatic facilities, and allied

nations. The deteriorating conditions in Syria, Iraq, and Libya exemplify these situations. As stated by Hillary R. Clinton, "Internal violent conflict, weak or failed governance, and humanitarian emergencies in numerous states around the world have become a central security challenge for the United States."[5] Joint Force 2020 will conduct "missions in a security environment characterized by several persistent trends such as proliferation of weapons of mass destruction, the rise of modern competitor states, violent extremism, regional instability, transnational criminal activity, and competition for resources."[6] Ten primary missions exist: Conduct Counterterrorism, Deter/Defeat Aggression, Project Power, Counter Weapons of Mass Destruction, Operate in Cyberspace/Space, Maintain Nuclear Deterrent, Defend the Homeland/Support Civil Authorities, Provide Stabilizing Presence, Conduct Stability, and Conduct Humanitarian Operations.[7] The clarity of the missions belies the uncertainty of the locations that will be determined by rapidly evolving situations.

The concept that every deployed leader is a Mission Commander is a dramatic shift in intelligence priorities and processes.

The military will develop a Mission Command philosophy to adapt to changing conditions through operational design and decentralized execution.[8] Mission Command will "empower leaders at the lowest level to carry out assigned tasks"[9] by linking deployed forces to fully integrate and synchronize operations.[10] It supports decision-making at the local level among the military, civilian agencies, and allies, where decisions achieve success and save lives. The concept that every deployed leader is a Mission Commander is a dramatic shift in intelligence priorities and processes.

Senior U.S. civilian and military decision-makers rely on the national Intelligence Community (IC) to provide intelligence on national security. The IC comprises sixteen intelligence organizations, including nine that operate under the Department of Defense.[11] The primary flow of intelligence is from the ground up, ending in Washington, DC. This process developed during the Cold War to contain the strategic threat posed by the Soviet Union. However, the strategy failed to protect the homeland from terrorists and did not identify the lack of Iraq's weapons of mass destruction in 2003.[12] The IC focused on protecting the nation and not on understanding emerging threats and regional conditions. The 9/11 Commission's investigation exposed gaps and stovepipes between multiple, and often within, organizations.[13] Congress reacted by passing the Homeland Security Act of 2002[14] and the Intelligence Reform and Terrorism Prevention Act of 2004.[15] These acts created the Department of Homeland Security and the Director of National Intelligence to coordinate federal agencies in order to address the intelligence gaps and protect the homeland from terrorists. Subsequently, 105 Joint Terrorism Task Forces and 72 Fusion Centers were established throughout the United States where federal, state, and local authorities coordinate efforts to investigate terrorism-related leads.[16] The focus of these reforms is to improve defense inside the homeland, not in the regions where threats originate.

The IC's mission is to "provide timely, insightful, objective, and relevant intelligence to inform decisions on national security issues and events."[17] It is not responsible for monitoring regional environments. Russia's ability to quickly annex the Crimea is one example where the situation escalated faster than the ability to understand and enable the U.S. to deter aggression.[18] In 2014 President Obama decided to deploy troops to battle the Ebola virus nine months after the initial outbreak and after over 3,000 people died. The decision was too late to stop the first Ebola death in America.[19] The U.S. followed the European Union's lead in supporting the rebels after Libyan security forces cracked down on demonstrators in early 2011.[20] Libya remains a failed state and terrorist safe haven where terrorists killed U.S. Ambassador Stevens and three others in 2012. The confusing reports from the Department of State prompted Congress to initiate an investigation to determine what the White House, the Department of State, and the Intelligence Community knew about the events.[21] The investigation continues five years later. The rise of the Islamic State of Iraq and Syria (ISIS) in Syria, Iraq, Libya, Afghanistan, and Nigeria[22] indicated a continuous threat by terrorist groups that current strategies did not prevent. These examples illustrate the rapidly changing regional conditions and the complex issues facing the nation's senior leaders and Joint Force Mission Commanders to develop effective plans.

The current intelligence gaps "are not 'intelligence failures' but major challenges and problems that need to be solved."[23] The current efforts concentrate intelligence resources to protect the homeland, but fall short of developing a holistic understanding of the complex security environments where threats originate. President Obama identified the value of intelligence support to the troops to be equally as important as the strategic intelligence that informs executive decisions.[24] Then-Secretary of Defense Chuck Hagel highlighted the requirement to synchronize operational intelligence efforts with improved analysis and dissemination at the operational and tactical levels.[25] The nation's senior leaders recognized the value of regional intelligence for deployed forces and the limitations of current doctrine.

The Department of Defense employs six geographic combatant commands and subordinate Service component commands to conduct a variety of operations to strengthen regional security, build partner nation capacity, deter emerging threats, support international initiatives, and improve cooperative security operations.[26] The combatant commands synchronize six core joint functions: command and control, intelligence, fires, movement and maneuver, protection, and sustainment[27] in order to apply the appropriate military forces. The strategic- and theater-level intelligence products support senior decision-makers in approving forces and resources to accomplish these missions.

The geographic combatant command Intelligence Director is responsible for the theater intelligence process: analysis, identification of gaps, intelligence requirements, and advising the commander on the appropriate ISR assets to provide early warning of threats and surveillance operations to monitor locations of interest.[28] Each geographic combatant command has collection management authority which it manages through the Joint Intelligence Operations Center based on the combatant commander's highest-priority missions.[29] The term ISR has become synonymous with Air Force Unmanned Aerial Vehicle (UAV) operations as the U.S. Strategic Command synchronizes "collection, processing, exploitation, and dissemination staffed through the Global Force Management process to the Joint Staff and Secretary of Defense."[30] The Air Force's aerial ISR platforms are managed at the strategic level while ground and naval ISR platforms are employed at the operational or tactical level. The separated management functions ensure that synchronization is accidental and rarely support the forward units, thus creating disjointed intelligence efforts over critical regions.

U.S.-based conventional and special operations commands deploy small units to conduct theater operations and exercises through the Service component commands.[31] Figure 1 illustrates the basic command and control relationships.

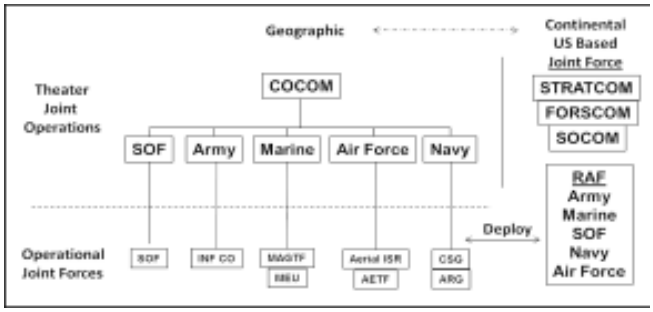


Figure 1. Geographic combatant command and control structure relationships for deployed forces under each Service component.[32]

As of June 2014, there were over 149,000 deployed forces to over 185 nations and islands; 150 of the locations had fewer than 100 personnel.[33] These small units lack dedicated intelligence support and usually monitor the local news or look to U.S.-based unit intelligence analysts who lack detailed understanding of complex conditions and are usually focused on the next training event.

Joint Force Mission Commanders require operational intelligence, which doctrine defines as "intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or operational areas."[34] Operational intelligence focuses on terrorist groups, political instability, and key factors that are driven by the population or "Human Domain" which the Joint Force must influence to accomplish national objectives.[35] Figure 2 illustrates the intelligence architecture and priority of efforts within the combatant command. The current doctrine creates multiplication and redundancy of intelligence efforts by each Service component and every military unit, often deployed to the same country. The limited ISR resources and constant competition among national, theater, and operational requirements ensure there are never enough to support every unit.

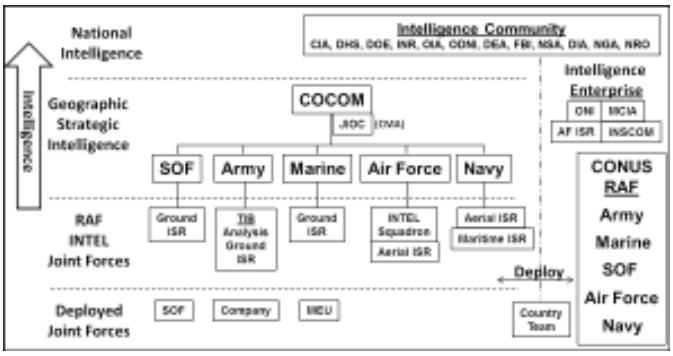


Figure 2. Geographic combatant command and control structure relationships for deployed forces under each Service component and intelligence architecture.[36]

The Army developed the Regionally Aligned Force (RAF) concept to rotate divisions and brigades to each geographic combatant command and to build culturally aware conventional forces and conduct security operations.[37] The 2nd Brigade of the 1st Infantry Division conducted security operations and exercises as the RAF for Africa Command from 2013 to 2014.[38] After al-Qaeda in the Islamic Maghreb (AQIM) operatives conducted terrorist attacks on two northern Niger towns,[39] it highlighted the force protection threats to RAF personnel and the inability of the current doctrine to maintain persistent operational intelligence for deployed forces.

The U.S. Army Intelligence and Security Command (INSCOM) recognized the gap in intelligence efforts and developed the Theater Intelligence Brigade (TIB) Anchor Point Concept. The concept aligns an intelligence brigade to each geographic Army Service component command supported by Functional Intelligence Brigades to provide counterintelligence, human intelligence, signals intelligence, aerial ISR, and the National Ground Intelligence Center.[40] The vision creates a federated Intelligence Enterprise of Army intelligence units to support the RAF units as they rotate between different geographic commands.

In August 2013, the 66th Military Intelligence Brigade tasked C Company (Regional Operations Company II), 24th Military Intelligence Battalion, to form the TIB Anchor Point for U.S. Army Africa (USARAF). The unit created intelligence fusion teams synchronized with 1st Infantry Division G2 Staff, and the 323rd Military Intelligence Battalion (Reserve) to monitor six priority operational environments. The TIB Anchor Point developed an informal network of analysts among USARAF, Special Operations Command Africa, 1st Information Operations Command, II Marine Expeditionary Force, 10th Special Forces Group (Airborne), Special Purpose Marine Air Ground Task Force, 704th Military Intelligence Brigade, Asymmetric Warfare Group, and other units. The soldiers, sailors, airmen, Marines, and civilians developed a tremendous intelligence network that benefited all commands.

The fusion teams used Google Earth to display the Common Operating Picture (COP) and Current Intelligence Picture (CIP), then transitioned to the Distributed Common Ground System-Army (DCGS-A), the Army's Intelligence computer system designed to create a common analytical platform for all echelons.[41] The RAF, deployed units, and diplomats experienced dedicated persistent operational intelligence while teamwork reduced duplication of effort throughout the enterprise and across eight time zones. The concept developed deep regional understanding, dramatically reduced the analyst's daily database searches, created daily collection requirements to focus ISR operations, and built holistic understanding of assigned operational environments. The coordinated efforts created over 500 intelligence products to deployed forces, U.S. diplomats, and partner nations.

As a situation deteriorates, the Department of Defense often establishes a Joint Task Force (JTF) to command and control military operations.[42] The new JTF staff and combatant command staff must adapt processes as the new Mission Commander develops the operational design to integrate the primary joint operational functions: command and control, intelligence, fires, movement and maneuver, protection, and sustainment.[43] The newly created JTFs face multiple challenges to man, equip, build staff procedures, and gain understanding of the situation, usually taking weeks to months to begin operations.[44] Commanders usually form a Joint Intelligence Support Element (JISE) to synchronize intelligence analysis and operations, often augmented by a National Intelligence Support Team of interagency liaison officers.[45] The newly appointed Senior Intelligence Officer faces a challenge to build the JISE; plan and deploy personnel and computer systems; develop operational intelligence; and develop intelligence processes to synchronize collection with combatant command Joint Intelligence Operations Centers (JIOCs).

U.S. Central Command identified many problems with intelligence during the build-up to Operation IRAQI FREEDOM and adapted to the system known as C4I: Command, Control, Communications, Computers, and Intelligence.[46] Once past the border, the combat maneuver units were inundated by reports, encumbered by the collections bureaucracy, and lacked human intelligence at the tactical level and sufficient linguists to understand the local population.[47] By 2004 each U.S. division changed its JISE to create "fusion centers" for both conventional and special operations forces to flatten the intelligence networks and drive intelligence operations.[48] Special Operations Task Force 714 created the Joint Inter-Agency Task Force (JIATF) as a fusion team that focused analysis by connecting contributing organizations into a network of diverse elements in a unified effort to support operations.[49] By 2006 the CIA's Baghdad Station Chief noted, "The close and growing collaboration, in fact, was bringing about a revolution in the real-time integrations of intelligence and military operations."[50] Intelligence agencies increased cooperation with the military when they shared common danger from terrorists, far from Washington, DC. The synchronization of analysis and ISR operations developed operational intelligence and the Task Force increased counterterrorist raids from 18 per month in 2004 to over 300 per month in 2006 using the Find, Fix, Finish, Exploit, and Analyze (F3EA) targeting process.[51]

The Air Force sponsored a Rand Corporation project to analyze ISR operations in Iraq and Afghanistan in 2008. It found that strategic Priority Intelligence Requirements (PIR) are usually broad and tactical PIRs are too narrowly defined.[52] Operational-level ISR provides the intelligence to drive operations, where "one good high priority collection is better than 99.9 percent wrong targets."[53] The key recommendation of the study to improve ISR operations is to align all aerial ISR under the Air Force Service component; unfortunately, the study does not address synchronizing ground, maritime, space, and cyber with aerial ISR operations.[54] GEN Dempsey recognized the challenge of the growing diverse ISR fleet: "ISR Joint Force 2020 is the panoramic grouping of personnel, processes, equipment, and other resources under DOD."[55]

The Joint Force will continue to face challenges employing the most advanced ISR assets and talented analysts without an effective intelligence strategy.

Military intelligence professionals work on a wide variety of computer systems, which creates challenges. The Army DCGS-A is an analytical software toolkit with over 70 programs for Army soldiers, but like other service-specific computers lacks joint interoperability. This weakness could be solved by developing joint workflow software throughout the geographic combatant commands, the Army, Navy, Air Force, Marines, and Special Operations. One successful example was the Access database designed and built by the soldiers of the Florida Army National Guard Special Operations Detachment-Central. The software streamlined the daily workflow for the intelligence analysts, collection managers, and planners during deployments to Joint Special Operations Task Force – Horn of Africa and Joint Special Operations Task Force – Trans-Sahara.[56] The five-man fusion team monitored six operational environments and supported counterterrorist operations, a dramatic ten-fold time saver over current processes.

GEN Tommy Franks transformed Central Command to synchronize intelligence functions before Operation IRAQI FREEDOM in approximately 18 months. Combat divisions deployed to Iraq took another year to adapt to intelligence fusion center concepts. Two years after the fall of Saddam, Special Operations Task Force 714 created the Joint Inter-Agency Task Force to synchronize intelligence functions and dramatically increase counterterrorist operations. Using these examples, it will take the Joint Force 2020 approximately 18 to 24 months to relearn lessons from 2006 and adapt intelligence structures and processes to meet combat operations.

The Theater Intelligence Brigade Anchor Point concept designed by the 66th Military Intelligence Brigade and the computer intelligence workflow software designed by the Special Operations Detachment-Central provide examples to meet the goal. Since 9/11, Congress has sponsored dramatic changes to domestic law enforcement agencies to protect the homeland. The Washington Post estimates that 854,000 people hold Top Secret security clearances and work in about 10,000 locations across the United States[57] connected by the Joint Worldwide Intelligence Communications System.[58] The nation has the resources but lacks the strategy to monitor regional security challenges. Now is the time to develop a strategy to effectively direct, organize, and employ the Joint Force military intelligence capability.

The strategy must synchronize the core joint function—intelligence—at the operational level. It must focus on regional environments in order to synchronize, not duplicate, the national-level IC efforts. It must function within the geographic combatant commands as a Joint Force rather than a single service to develop joint intelligence processes. The strategy should use the advantage of the nation's Total Force (Active, Guard, and Reserve) to synchronize global operations linked by secure networks to maintain current budget levels. The strategy should develop Mission Command philosophy for military intelligence soldiers, sailors, airmen, Marines, and civilians to synchronize plans, analysis, and ISR operations with common work flow and data standards. The strategy will create the most effective and efficient Joint Intelligence Force to support daily theater security operations and enable the Joint Force to adapt quickly to contingency and combat operations.

The Persistent Operational Intelligence strategy combines new doctrine, organization, Mission Command, and software to prepare the Joint Force to operate beyond the borders with the full capacity of the undisputed world leader in military intelligence analysis, surveillance, and reconnaissance capabilities. The concept creates six geographically aligned Joint Intelligence Task Forces (JITFs) with Mission Command responsibilities.

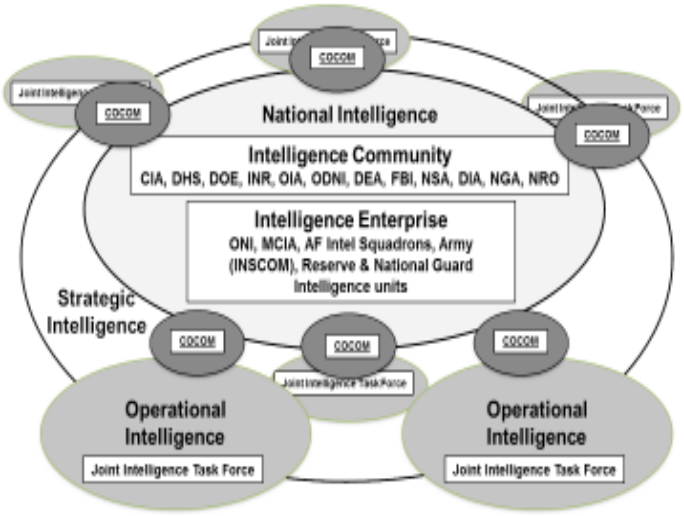


Figure 3. Joint Intelligence Task Force geographically synchronized with the Intelligence Community and Intelligence Enterprise.[59]

Figure 3 depicts the relationship and responsibility between the JITFs and the Intelligence Community. The design increases unity of effort, reduces redundancy, and improves the nation's ability to monitor regional security environments. The JITFs will be dynamic, agile organizations to focus efforts on the priority operational environments while the Joint Intelligence Operations Centers focus on the strategic picture and seams between the commands. The JITF primary mission is the dedicated operational intelligence synchronization for the Joint Forces

to accomplish the ten primary missions. Figure 4 depicts the JITF position within the combatant command and depicts the changes in collection management processes and priority of intelligence operations.

JITF Mission Command is a combination of collection management authority, operational control, and tactical control of assigned and aligned Joint Force intelligence units adapted to the specific conditions of each geographic combatant command. Mission Command is the appropriate command relationship to maintain unity of effort across each JITF global network.[61] "Leadership is critical. Rank doesn't matter in intelligence. A junior analyst inside an organization may have the most knowledge on a critical subject debated at the senior staff level."[62] The JITF creates the network to identify, train, advance, and promote the most knowledgeable and professional intelligence personnel. The result creates deep regional understanding, continuous career progression, and information superiority for the Joint Force.

JITF planners will use the Adaptive Planning and Execution System and Dynamic Threat Assessment in order to support the flexible planning environment envisioned by the Secretary of Defense.[63] Planners create and sustain operations of the JITF and adapt to changing military conditions. They will network and synchronize Active, Guard, and Reserve intelligence forces in a five-dimensional effort across land, sea, air, space, and cyber domains to create persistent intelligence operations.[64] They will identify new opportunities with partner nation military intelligence organizations to increase intelligence-sharing relationships. The result will be a dynamic and interactive intelligence task force.

The vision is a federated intelligence network of fusion teams across multiple locations and time zones comprised of all-source, geospatial, signal, linguistic, and human intelligence analysts. They combine open-source news reports, social media, liaison reports, and reports from every deployed ISR platform to maintain operational intelligence of complex political environments, track terrorist networks, and provide force protection and early warning of deteriorating conditions. "In the interpretation of fusion, everyone associated with the intelligence cycle would work from the proposition that collection feeds the development of a holistic analytic picture."[65] The network includes experts in counterintelligence, social science, computer forensics, biometrics, and other unique skills to eliminate the current, stove-piped request process. The fusion teams will push intelligence to deployed units, ISR forces, RAF, allies, United Nations peacekeepers, and U.S. diplomats. The result is Persistent Operational Intelligence for the Joint Force and the nation's senior leaders.

The JITF will synchronize ISR operations: "Effective synchronization results in the maximum use of every intelligence asset where and when it will make the greatest contribution to success."[66] The JITF Mission Commander provides the expertise to employ Joint Force ISR assets to

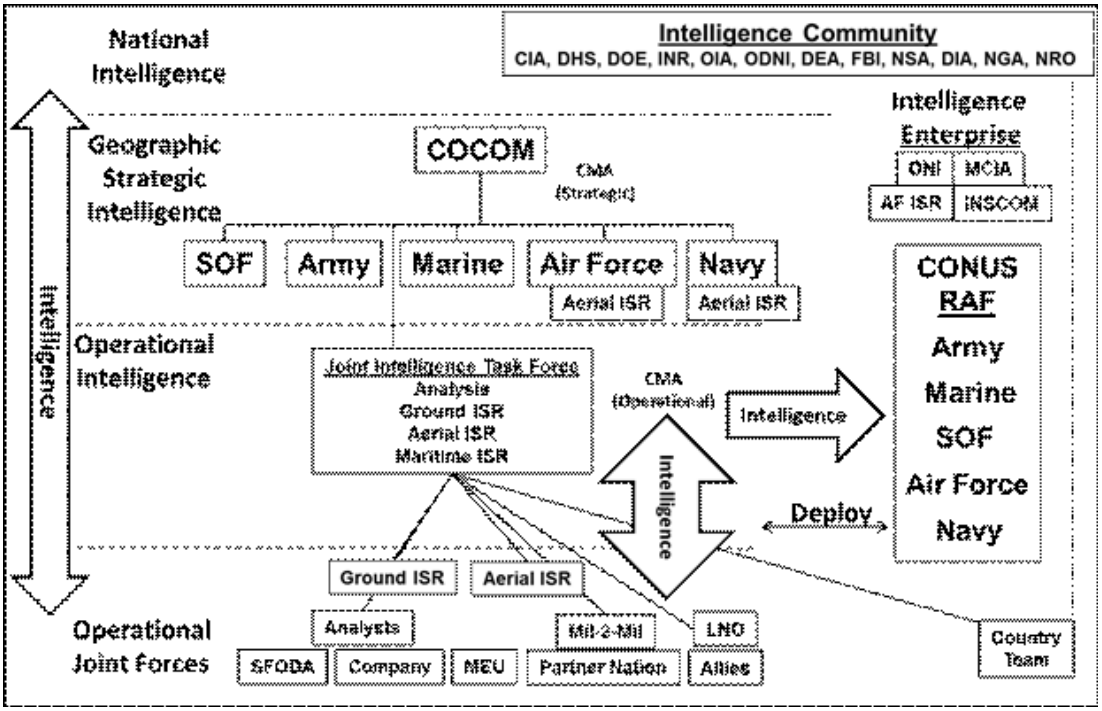


Figure 4. The geographic combatant command structure changes with the Joint Intelligence Task Force.[60]

maintain a holistic and continuous collection plan at the operational level, "a task that most do not understand well."[67] The change shifts the current collection management from the strategic to the operational level where TF 714 produced the most dramatic effects.

GEN Dempsey established his vision for Joint Force ISR capabilities: "To create a force that enhances jointness, incorporates multi-intelligence technology, is interoperable and survivable, and relies on integrated PED of collected data we must share a common vision and sacrifice proprietary systems for a more powerful collective capability."[68] The JITF will drive technological advances to link ISR sensors to analysts with common data standards, effectively moving data across the commands at the appropriate classifications for U.S. and coalition operations.[69] Improved workflow will dramatically reduce duplication, increase the time available for analytical efforts, and logically streamline large volumes of data that can overwhelm new analysts.[70] The goal is to use the computer technology to link the entire JITF network among analysts, collection managers, planners, processing and exploitation teams, and Mission Commanders. The Persistent Operational Intelligence strategy reduces competition between the services and builds teamwork and common software to benefit the Joint Force. A single organization with a common strategy can eliminate the current Word, Adobe, Excel, JPG and PowerPoint files and replace them with three-dimensional intelligence similar to computer video games with which all young analysts are familiar. Figure 5 represents a new, virtual Current Intelligence and Common Operations Picture with the workflow software to synchronize the intelligence process: plans, collection, processing & exploitation, analysis & production, dissemination & integration, and evaluation & feedback.[71] This concept links sensors to analysts to accelerate intelligence processes and maintain information superiority to support the Joint Force.

The new organization will be virtually organized, in order to use the nation's advantages of time zones, facilities, and secure communications. The concept will require changes within combatant commands to establish appropriate command relationships and intelligence processes. The JITF concept uses Mission Command philosophy to coordinate and streamline the Department of Defense Global Force Management Process, "which starts and ends with the Secretary of Defense,"[72] to maintain Persistent Operational Intelligence. One of the most important assets of an Army RAF division might be a counterintelligence team with a native linguist. The JITF agility will enable the Joint Force to recognize quickly these unique opportunities, a rare opportunity under the current Service culture.

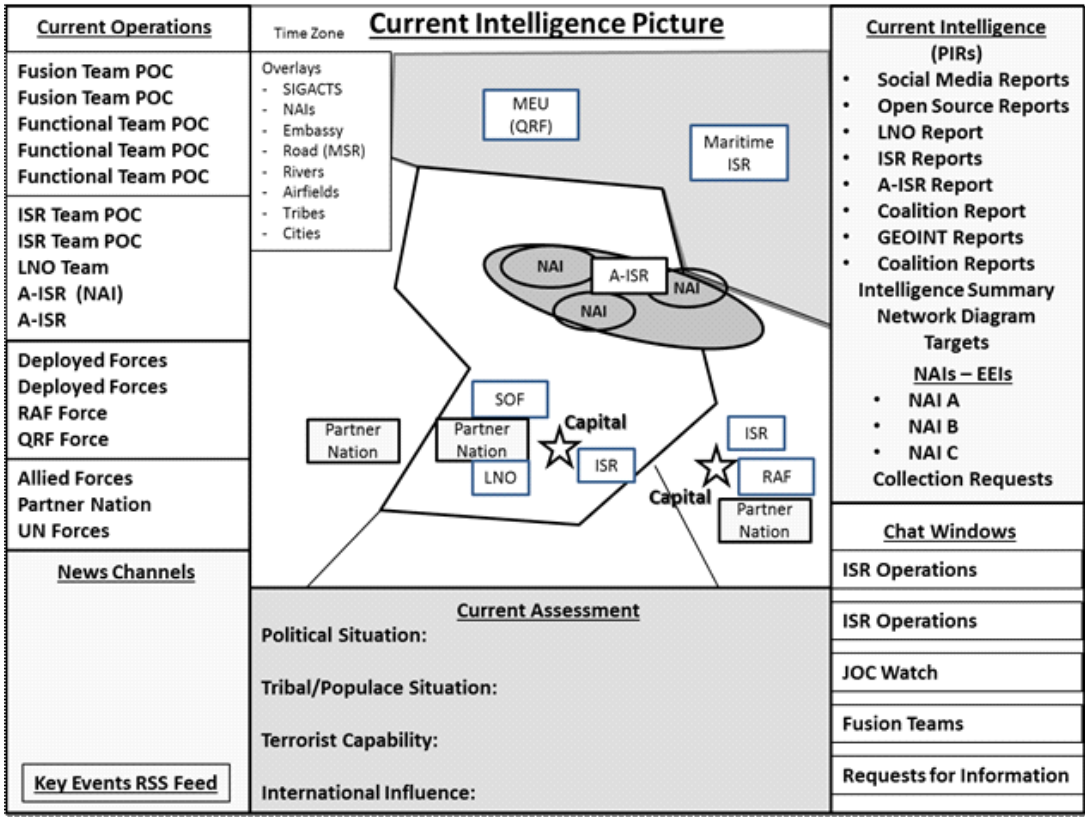


Figure 5. Notional Current Intelligence Picture showing workflow and JITF contacts to maintain Persistent Operational Intelligence operations.

The nature of the JITF mission will require the majority of the personnel to conduct their work on classified systems in sensitive compartmented information facilities. Senior leaders will never see the JITF in a single formation, but will conduct Mission Command using video teleconferences, chat, and email. The military must develop leaders who can visualize that "The World Is Flat" to develop global synchronization with operational precision like large multinational companies.[73] The education process must extend to the rest of the Joint Force in order to teach how to maintain the JITF network and prevent gaps caused by local unit events and administrative requirements.

The plan must develop business rules between the military and the Intelligence Community to synchronize intelligence processes. The IC took over three weeks to produce a 92-page National Intelligence Estimate for Iraq in 2002.[74] This is one type of national intelligence product for informing senior civilians and general officers. These products do not support Joint Force Mission Commanders such as colonels, lieutenant colonels, and captains who use PowerPoint, Google Earth, and DCGS-A tools. The product was ultimately proven false and did not prepare any brigade, battalion, or company commander for Operation IRAQI FREEDOM. The JITF and IC leaders must develop a good working relationship to support the "whole of government" approach for intelligence at the operational level, where a soldier's act of kindness will make allies and mistakes are international headlines.

The Persistent Operational Intelligence strategy synchronizes Joint Force military intelligence, surveillance, and reconnaissance resources to monitor critical operational environments continuously and to prepare the Joint Force to accomplish national objectives. The strategy synchronizes Active, Guard, and Reserve intelligence personnel to create deep, holistic regional expertise. The layered operations between the Intelligence Community and the Joint Force will improve the nation's ability to understand emerging threats to the homeland. The strategy will support theater security operations and effectively employ advanced ISR assets. The Joint Force will improve the ability to work more effectively with allies, respond to contingencies, and quickly transition to combat operations to defeat the nation's enemies.

NOTES

1 U.S. Joint Chiefs of Staff, "Concepts," linked from *Joint Staff Library Home Page*, http://www.dtic.mil/doctrine/concepts/concepts.htm (accessed September 24, 2014).

2 Martin E. Dempsey, *Joint ISR Whitepaper* (Washington, DC: U.S. Joint Chiefs of Staff, June 2014), 2-4, http://www.dtic.mil/doctrine/concepts/white_papers/cjcs_wp_isr.pdf (accessed November 24, 2014).

3 Charles T. Hagel, *Quadrennial Defense Review 2014* (Washington, DC: U.S. Department of Defense, March 4, 2014), IV, http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf (accessed September 24, 2014).

4 Barack H. Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed September 24, 2014).

5 Hillary R. Clinton, *Quadrennial Diplomacy and Development Review: Leading Through Civilian Power* (Washington, DC: U.S. Department of State, 2010), 121, http://www.state.gov/documents/organization/153108.pdf (accessed September 24, 2014).

6 Martin E. Dempsey, *Capstone for Joint Operations: Joint Force 2020* (Washington, DC: U.S. Joint Chiefs of Staff, 2012), 2, http://www.defenseinnovationmarketplace.mil/resources/JV2020_Capstone.pdf (accessed September 12, 2014).

7 James F. Amos, William H. McRaven, and Raymond T. Odierno, *Strategic Landpower: Winning the Clash of Wills* (Fort Eustis, VA: TRADOC, May 2013), 2, http://www.tradoc.army.mil/FrontPageContent/Docs/Strategi%20Landpower%20White%20Paper.pdf (accessed September 24, 2014).

8 Martin E. Dempsey, *Mission Command White Paper* (Washington, DC: U.S. Joint Chiefs of Staff, April 3, 2012), 3, http://www.dtic.mil/doctrine/concepts/white_papers/cjcs_wp_missioncommand.pdf (accessed September 12, 2014).

9 Dempsey, *Capstone for Joint Operations*, 5.

10 Dempsey, *Joint ISR Whitepaper*, 2.

11 "Members of the Intelligence Community," linked from *U.S. Department of National Intelligence Home Page*, http://dni.gov/index.php/intelligence-community/members-of-the-ic (accessed September 25, 2014).

12 Bob Woodward, *Plan of Attack* (New York, NY: Simon and Schuster Publisher, 2004), 197.

13 Thomas Kean and Lee Hamilton, *The 9/11 Commission Report* (Washington, DC: National Commission on Terrorist Attacks Upon the United States, July 22, 2004), 425-426, http://www.9-11commission.gov/report/911Report.pdf (accessed September 19, 2014).

14 "U.S. Department of Homeland Security Creation," linked from *U.S. Department of Homeland Security Home Page*, www.dhs.gov/creation-department-homeland-security, (accessed March 10, 2015).

15 "9/11 Commission," linked from *U.S. Senate Committee on Homeland Security & Government Affairs*, http://www.hsgac.senate.gov/issues/9-11-commission (accessed September 18, 2014).

16 Lee Hamilton and Thomas Kean, *Tenth Anniversary Report Card: The Status of the 9/11 Commission Recommendations* (Washington, DC: National Security Preparedness Group, September 2011), 11, http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/CommissionRecommendations.pdf (accessed September 17, 2014).

17 James R. Clapper, *The 2014 National Intelligence Strategy of the United States of America*, (Washington, DC: Office of the Director of National Intelligence, September 18, 2014), 2, http://www.dni.gov/files/documents/2014_NIS_Publication.pdf (accessed August 15, 2015).

18 Nile Gardiner, Jack Spencer, Luke Coffey, and Nicolas Loris, "Beyond the Crimea Crisis: Comprehensive Next Steps in U.S.-Russian Relations," March 24, 2014, linked from The Heritage Foundation, http://www.heritage.org/research/reports/2014/03/beyond-the-crimea-crisis-comprehensive-next-steps-in-usrussian-relations (accessed June 3, 2015).

19 Rebecca Davis, "Ebola Epidemic 2014: Timeline," October 15, 2014, *The Guardian*, http://www.theguardian.com/world/2014/oct/15/ebola-epidemic-2014-timeline (accessed June 3, 2015).

[20] Lisa Daniel, "Initial Libya Mission Complete, Successful, Gates Says," April 1, 2011, *American Forces Press Service*, linked from *U.S. Department of Defense Home Page*, http://www.defense.gov/news/newsarticle.aspx?id=63392 (accessed June 2, 2015).
[21] "Benghazi Timeline: How the Probe Unfolded," *CBS News*, http://www.cbsnews.com/news/benghazi-timeline-how-the-probe-unfolded (accessed June 6, 2015).
[22] Oren Dorrell, "ISIL takes body blows in Iraq while affiliates grow elsewhere," April 22, 2015, *USA Today*, http://www.usatoday.com/story/news/world/2015/04/21/isil-isis-taking-body-blows-while-arms-grow-elswhere/26134545/ (accessed May 9, 2015).
[23] Anthony H. Cordesman, *The Iraq War: Strategy, Tactics, and Military Lessons* (Washington, DC: The Pentagon Press, 2003), 195.
[24] Obama, *National Security Strategy*, 8.
[25] Hagel, *Quadrennial Defense Review*, 38.
[26] U.S. Joint Chiefs of Staff, *Military Contribution to Cooperative Security (CS) Joint Operating Concept, Version 1.0* (Washington, DC: U.S. Joint Chiefs of Staff, September 19, 2008), 10, http://www.dtic.mil/doctrine/concepts/joint_concepts/joc_cooperativesecurity.pdf (accessed September 24, 2014).
[27] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, Joint Publication 1 (Washington, DC: U.S. Joint Chiefs of Staff, March 25, 2013), V-19, http://www.dtic.mil/doctrine/new_pubs/jp1.pdf (accessed September 5, 2014).
[28] U.S. Joint Chiefs of Staff, *Joint Intelligence*, Joint Publication 2-0 (Washington, DC: U.S. Joint Chiefs of Staff, October 22, 2013), I-11, http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf (accessed September 24, 2014).
[29] Stanley McChrystal, Tantum Collins, David Silverman, and Chris Fussell, *Team of Teams: New Rules of Engagement for a Complex World* (New York, NY: Penguin Publishing Group, 2015), 182, Kindle e-book.
[30] Ibid., III-9.
[31] U.S. Joint Chiefs of Staff, *Joint Security Operations in Theater*, Joint Publication 3-10 (Washington, DC: U.S. Joint Chiefs of Staff, November 13, 2014), II-8, http://www.dtic.mil/doctrine/new_pubs/jp3_10.pdf (accessed June 8, 2015).
[32] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Force*, Joint Publication 1-0, II-10, II-11; U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011), IV-6 – IV-9, http://dtic.mil/doctrine/new_pubs/jp3_0.pdf (accessed September 24, 2014).
[33] *Defense Manpower Data Center*, "Total Military Personnel and Dependent End Strength," July 2014, https://www.dmdc.osd.mil/app/dwp/rest/download?fileName=SIAD_309_ReportP1406.xlsx&groupName=milRegionCountry (accessed October 22, 2014).
[34] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010, as amended through July 16, 2014), 191-192, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed September 24, 2014).
[35] Amos, *Strategic Landpower*, 3.
[36] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces*, Joint Publication 1-0, II-10-11; U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0, IV-6-9; U.S. Joint Chiefs of Staff, *Command and Control of Joint Air Operations*, Joint Publication 3-30 (Washington, DC: U.S. Joint Chiefs of Staff, February 10, 2014), III-29, http://www.dtic.mil/doctrine/new_pubs/jp3_30.pdf (accessed August 1, 2014); U.S. Joint Chiefs of Staff, *Command and Control for Joint Land Operations*, Joint Publication 3-31 (Washington, DC: U.S. Joint Chiefs of Staff, February 24, 2014), I-8, http://www.dtic.mil/doctrine/new_pubs/jp3_31.pdf (accessed August 1, 2014); U.S. Joint Chiefs of Staff, *Command and Control for Joint Maritime Operations*, Joint Publication 3-32 (Washington, DC: U.S. Joint Chiefs of Staff, August 7, 2013), IV-2, http://www.dtic.mil/doctrine/new_pubs/jp3_32.pdf (accessed August 1, 2014); U.S. Joint Chiefs of Staff, *Joint Task Force Headquarters*, Joint Publication 3-33 (Washington, DC: U.S. Joint Chiefs of Staff, July 30, 2012), III-2, http://www.dtic.mil/doctrine/new_pubs/jp3_33.pdf (accessed August 1, 2014); U.S. Joint Chiefs of Staff, *Special Operations*, Joint Publication 3-05 (Washington, DC: U.S. Joint Chiefs of Staff, July 16, 2014), III-6, http://www.dtic.mil/doctrine/new_pubs/jp3_05.pdf (accessed August 1, 2014); U.S. Joint Chiefs of Staff, *Joint and National Intelligence Support to Military Operations*, Joint Publication 2-01 (Washington, DC: U.S. Joint Chiefs of Staff, January 5, 2012), III-10, http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf (accessed September 24, 2014).
[37] Kimberly Field, James Learmont, and Jason Charland, "Regionally Aligned Forces: Business Not as Usual," *Parameters* 43, no. 3 (Autumn 2013), 56, http://strategicstudiesinstitute.army.mil/pubs/Parameters/issues/Autumn_2013/5_Field.pdf (accessed October 24, 2014).
[38] *U.S. Army G-3/5/7*, "Regional Alignment of Forces," briefing (Washington, DC: U.S. Department of the Army, September 10, 2013), 7, https//usawc.blackboard.com/bbcswebdav/pid-42701-dt-content-rid-44507_1/courses/15DE2308999D1/READINGS/088L1S3L3 (accessed October 14, 2014).
[39] Leela Jacinto, "Niger's Attacks May be a Collaborative Jihadist Effort," July 23, 2013, *France 24*, http://france24.com/en/20130524-niger-attacks-may-be-a-collaborative-jihadist-effort-analysis-aqim-mujao/#./?&_suid=142283070862901606831812601089 (accessed November 18, 2014).
[40] U.S. Department of the Army, *Intelligence*, Army Doctrine Publication (ADP) 2-0 (Washington, DC: U.S. Department of the Army, August 31, 2012), I-6, http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/adp2_0.pdf (accessed September 24, 2014).
[41] *The Distributed Common Ground System – Army Home Page*, http://dcgsa.apg.army.mil/about_dcgsa/ (accessed August 25, 2014).
[42] U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0, IV-7.
[43] Ibid., II-4, III-1.
[44] Timothy M. Bonds, Myron Hura, and Thomas-Durell Young, *Enhancing Army Joint Force Headquarters Capabilities* (Santa Monica, CA: Rand Arroyo Center, 2010), 7, http://www.rand.org/content/dam/rand/pubs/monographs/MG600/MG675-1/RAND_MG675-1.pdf (accessed April 30, 2015).
[45] U.S. Joint Chiefs of Staff, *Joint Intelligence*, Joint Publication 2-0, III-6.
[46] Tommy R. Franks with Malcom McConnell, *American Soldier* (New York, NY: Harper-Collins Publishing, 2004), 175.
[47] Anthony H. Cordesman, *The Iraq War: Strategy, Tactics, and Military Lessons* (Westport, CT: Praeger Publishers, 2003), 184-188.
[48] George W. Casey, Jr., *Strategic Reflections: Operation Iraqi Freedom July 2004-February 2007* (Washington, DC: National Defense University Press, October 2012), 71, http://ndupress.ndu.edu/Portals/68/Documents/Books/Strategic-reflections.pdf (accessed September 19, 2014).
[49] Stanley McChrystal, *My Share of the Task: A Memoir* (New York: The Penguin Group, 2013), 119, Kindle e-book.
[50] Robert M. Gates, *Duty: Memoirs of a Secretary at War* (New York: Knopf Doubleday Publishing Group, January 2014), 33, Kindle e-book.
[51] McChrystal, *Team of Teams*, 135-137, 218.

[52] Sherill Lingel, Carl Rhodes, Amando Cordova, Jeff Hagen, Joel Kvitky, and Lance Menthe, *Methodology for Improving the Planning, Execution, and Assessment of Intelligence, Surveillance, and Reconnaissance Operations* (Santa Monica, CA: Rand Corporation, 2008), 35-37, http://www.rand.org/content/dam/rand/pubs/technical_reports/2008/RAND_TR459.pdf (accessed March 30, 2015).
[53] Ibid., 35.
[54] Ibid., 39.
[55] Dempsey, *Joint ISR Whitepaper,* 1-3.
[56] "Special Operations Detachment Ready for Upcoming Missions to Support U.S. Africa Command," September 15, 2009, linked from *Florida Guard Online*, http://www.fl.ng.mil/3740 (accessed June 12, 2015).
[57] Dana Priest and William M. Arkin, "A hidden world, growing beyond control: Top Secret America, a Washington Post Investigation," July 19, 2010, *The Washington Post*, http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/1, (accessed June 23, 2015).
[58] U.S. Joint Chiefs of Staff, *Joint Communications System*, Joint Publication 6-0 (Washington, DC: U.S. Joint Chiefs of Staff, June 10, 2015), V-3, http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf (accessed June 23, 2015).
[59] U.S. Joint Chiefs of Staff, *Joint Intelligence*, Joint Publication 2-0, III-4; "Organization," linked from *Office of the Director of National Intelligence home page*, www.dni.gov/index.php/about/organization (accessed January 14, 2015).
[60] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces,* Joint Publication 1-0, II-10-11; U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0, IV-6-9; U.S. Joint Chiefs of Staff, *Command and Control of Joint Air Operations*, Joint Publication 3-30, III-29; U.S. Joint Chiefs of Staff, *Command and Control for Joint Land Operations,* Joint Publication 3-31, I-8; U.S. Joint Chiefs of Staff, *Command and Control for Joint Maritime Operations,* Joint Publication 3-32, IV-2; U.S. Joint Chiefs of Staff, *Joint Task Force Headquarters,* Joint Publication 3-33, III-2; U.S. Joint Chiefs of Staff, *Special Operations,* Joint Publication 3-05, III-6, U.S. Joint Chiefs of Staff, *Joint and National Intelligence Support,* Joint Publication 2-01, II-2, II-3.
[61] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces,* Joint Publication 1-0, V-3.
[62] Michael T. Flynn and Charles A. Flynn, "Integrating Intelligence and Information: Ten Points for the Commander," *Military Review (January-February 2012),* 6, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20120229_art005.pdf (accessed September 24, 2014).
[63] Robert M. Gates, *Adaptive Planning Roadmap II* (Washington, DC: U.S. Department of Defense, March 2008), 8, https://usawc.blackboard.com/bbcswebdav/institution/DEP%20Content/DE2310/AY15/READINGS/Block1/B01U01_AP (accessed February 1, 2015).
[64] U. S. Joint Chiefs of Staff, *Joint Intelligence*, Joint Publication 2-0, I-11.
[65] Ben Connable, *Military Intelligence Fusion for Complex Operations: A New Paradigm* (Santa Monica, CA: Rand Corporation, 2012), 5, http://www.rand.org/content/dam/rand/pubs/occasional_papers/2012/RAND_OP377.pdf (accessed September 24, 2014).
[66] U.S. Joint Chiefs of Staff, *Joint and National Intelligence Support,* Joint Publication 2-01, II-2.
[67] Flynn, "Integrating Intelligence and Information," 5.
[68] Dempsey, *Joint ISR Whitepaper*, 9.
[69] Dempsey, *Joint ISR Whitepaper,* 3-4.
[70] Dempsey, *Capstone for Joint Operations,* 10.
[71] Ibid., III-1.
[72] Michael A. Santacroce, ""Planning for Planners" Joint Operation Planning Process (JOPP), Volume I," 2011, *U.S. Naval War College,* 92, https://www.usnwc.edu/getattachment/7d3f6744-b9c4-479b-9c8d-da2c132e368e/Planning-for-Planners_Jan_2012_new.aspx (accessed April 4, 2015).
[73] Thomas L. Friedman, *The World Is Flat: A Brief History of the Twenty-First Century* (New York: Farrar, Straus & Giroux, 2005), 11, Kindle e-book.
[74] Woodward, *Plan of Attack,* 197.

COL (USAR) Reid W. Webber is a Distinguished Military Graduate of Eastern Illinois University, where he received a BS degree and was commissioned a Quartermaster Corps officer in 1988. He is a graduate of the U.S. Army Command and General Staff College, Advanced Joint Professional Military Education, and the U.S. Army War College. He is a Department of the Army civilian where he serves as Director of the Army's Aerial-ISR Coordination Center at the 116th Military Intelligence Brigade, Ft Gordon, GA. COL Webber's command assignments include Commander of Detachment 4/9, CENTCOM J2 Army Reserve Element; Deputy Commander of the 66th Military Intelligence Brigade; Chief of AFRICOM J2 Sahel Intelligence Mission Operations Center; Military Intelligence Detachment Command of 3/20th SFG (A); and Rigger Platoon Leader of the 3/325th Airborne Battalion Combat Team. Key staff assignments include Assistant Chief of Staff, G2 for 7th Civil Support Command; ACE Chief, U.S. Army Africa Theater Intelligence Brigade Anchor Point at 66th MI Brigade; J2 Senior Intelligence Officer for Joint Special Operations Task Force – Trans-Sahel; J2 Senior Intelligence Officer for Joint Special Operations Task Force – Horn of Africa; J2 Senior Plans Officer for Special Operations Command-Central; J2 Special Operations Command and Control Element-Afghanistan; J2 Special Operations Detachment-Central; and S2, 3/265th ADA Battalion. Major overseas deployments include Operation PROVIDE COMFORT, 1991; Operation IRAQI FREEDOM, 2002-03; Operation ENDURING FREEDOM, 2005-06 and 2009-14; and the Global War on Terror, 2006-09.

Strategic Intelligence Officers at DIA's Integrated Intelligence Centers

by Maj (USA) Michael W. Hein

In my first two months at the Defense Intelligence Agency (DIA) as a Strategic Intelligence officer, I published a President's Daily Brief (PDB) article, and a year later I was responsible for analytic production on North and West Africa. When I first arrived in January 2014, however, I did not know I would be managing civilian analysts and writing PDB articles. Consequently, what should a field grade Army Strategic Intelligence officer (Functional Area 34) expect when assigned to DIA? What should that officer strive for over the course of a three-year assignment? Unlike officers in one of the Army's basic branches assigned as staff officers at the battalion, brigade, and division level in regular Army units, most officers who transfer to the Strategic Intelligence field have no idea what to expect from an assignment at DIA. Many report to one of the Agency's regional Integrated Intelligence Centers (commonly known as "Centers") where they are immediately expected to assume the duties of either an analyst or a manager responsible for supervising civilian analysts and reporting through a civilian chain of command. It takes many officers at least a year to begin to understand how the Agency works and how they must fit in so that they successfully perform their duties and continue their own professional development. This article is intended to equip Army field grade Strategic Intelligence officers with answers to those questions before they begin their first tour at DIA.

WHAT IS A STRATEGIC INTELLIGENCE OFFICER?

Army officers in the Strategic Intelligence specialty (FA 34) are trained to provide expertise on intelligence activities at the theater and strategic levels.[1] The Army looks to the Strategic Intelligence officer to lead analysis and intelligence programs that support key decision-makers, policymakers, and warfighters in the Department of Defense (DoD), interagency, joint, coalition, and combined communities.[2] Specifically, Strategic Intelligence officers are expected to conduct strategic intelligence analysis and planning, joint intelligence preparation of the operating environment (JIPOE), and campaign planning, as well as to develop collection requirements at the strategic level.[3]

Upon entering the Strategic Intelligence functional area, officers must complete the Master of Science of Strategic Intelligence (MSSI) program at DIA's National Intelligence University located in Bethesda, Maryland. Officers from Army branches other than Military Intelligence must also complete the Strategic Intelligence Officer Course (SIOC) at the U.S. Army Intelligence Center located at Fort Huachuca, Arizona. Upon completing the MSSI program and, if necessary, the SIOC, Strategic Intelligence officers are assigned to Army subordinate commands (primarily at echelons above corps), combatant commands, DoD, the Joint Staff, and national agencies to support the development of national security policy and theater strategic plans and operations.[4] Key developmental assignments for majors are team/branch chief, desk officer, senior analyst, or plans/operations/warning officer, and key developmental assignments for lieutenant colonels are branch chief/deputy division chief, deputy director of intelligence, and plans/operations officer.[5] Majors are expected to gain experience in leading and managing a team or branch conducting strategic intelligence analysis, planning, integration, and exchange/liaison with foreign intelligence services. Lieutenant colonels are expected to continue to develop these competencies, as well as serving as the DoD or Army representative at other national-level agencies.[6]

For many Strategic Intelligence officers, their first assignment after completing the MSSI degree is in one of DIA's four regional Centers. Many others are first assigned to one of the geographic combatant commands (AFRICOM, CENTCOM, EUCOM, PACOM, NORTHCOM, or SOUTHCOM) and then return to DIA for their next assignment.

WHAT IS AN INTEGRATED INTELLIGENCE CENTER?

DIA serves as the principal advisor on defense-related intelligence to the Secretary of Defense and the Chairman of the Joint Chiefs of Staff, although its customers range from forward-deployed warfighters to national policymakers.[7] DIA's mission is to provide its customers intelligence on foreign militaries and operating environments that helps policymakers prevent and win

wars.[8] DIA's Directorate of Intelligence conducts all-source analysis of foreign military capabilities and intentions, including both current and estimative intelligence production, while the Directorate of Operations conducts intelligence collection.[9] DIA's Defense Attaché System provides military attachés to serve in U.S. embassies around the world, representing DoD to host nations and advising U.S. ambassadors on military matters.[10]

The Directorate of Intelligence itself is organized into four regional Centers that LTG (USA) Michael Flynn established in 2012 during his tenure as the Agency's Director.[11] They are the Middle East Africa Regional Center (MARC), the Europe Eurasia Regional Center (EERC), the Asia Pacific Regional Center (APRC), and the Americas Regional Center (AMRC). The Central Intelligence Agency has since adopted a center-based model, as well.[12] Each center networks and integrates analysts from the Directorate of Intelligence and collectors from the Directorate of Operations and brings them together as one team to produce defense-related analysis and finished intelligence.[13] The regional Centers also collaborate closely with DIA's Defense Countering Terrorism Center, which produces integrated, all-source intelligence in support of the DoD campaign against terrorism.[14] Strategic Intelligence officers are assigned throughout DIA, but this article will focus on those assigned to Integrated Intelligence Centers (IICs).

IIC analysts support policymakers primarily through written products and briefings. The DIA's principal executive analytic product is the Defense Intelligence Digest article, typically less than three pages, setting forth the agency's assessment on a particular subject. The Defense Intelligence Digest (DID) is a compilation in magazine format of various articles and is distributed within the Defense Department and to military commands worldwide. Analysts also author other finished intelligence products, including PDB articles, graphics, tabloids, and longer papers, as well as less formal written products such as response memoranda and even email answers to short-suspense questions from Pentagon customers. Briefings are typically given to Pentagon deputies, assistant deputies, and their staffs, as well as to U.S. ambassadors and other diplomats.

WHAT SHOULD A STRATEGIC INTELLIGENCE OFFICER STRIVE FOR AT AN IIC?

Majors account for about half of the Army officers assigned to the Centers, with lieutenant colonels accounting for most of the other half, along with a few senior captains. An Army lieutenant colonel in the Strategic Intelligence functional area assigned to one of the Centers will frequently be tapped to serve as a deputy division chief responsible for a geographic region within one of the Centers for part of a three-year tour, with the remaining time in a staff position—frequently operations. A captain or major should strive to serve at least one year as a branch chief. It is a very challenging, educational, and rewarding assignment through which officers learn more about DIA than through any other job in a Center.

WHAT SHOULD A STRATEGIC INTELLIGENCE OFFICER EXPECT?

A major in the Strategic Intelligence functional area assigned to a Center should expect to serve first as a line analyst for up to a year before having the opportunity to be a branch chief. Due to the limited number of branch chief positions, Strategic Intelligence officers are in competition with three distinct groups for such an assignment: other Strategic Intelligence officers, Foreign Area Officers, and civilian DIA analysts for whom a branch chief position is a core developmental assignment at the GG-14 level.[15] Only about half of the Army officers assigned to the Centers are Strategic Intelligence officers. Most of the others are Foreign Area Officers who are serving as Army attachés in U.S. embassies abroad under the DIA's Defense Attaché System. Whether the Foreign Area Officers have already served as attachés or are preparing for their first official posting as an attaché, they typically know more about the region than their Strategic Intelligence counterparts due to their regional specialization and graduate study. In addition, each branch chief position that is held by a military officer means one less billet for GG-14s seeking core developmental assignments. As a result, there are not enough branch chief positions for all Strategic Intelligence officers to spend their entire tour in a Center as a branch chief.

As an analyst, a captain or major should expect to be assigned to an account, such as covering several small nations or focusing on the security forces of a high-priority country. Officers assigned to accounts that match a recent deployment—such as to Iraq or Afghanistan—may have significant subject matter expertise, but most will need to learn an entirely new account. Nevertheless, working as an analyst provides the Strategic Intelligence officer with the opportunity to research, write, and brief key strategic issues, and to learn both the foundational knowledge and day-to-day work of analysts before assuming the branch chief role and supervising civilian analysts.

Working as an analyst brings with it several unique challenges. Strategic Intelligence officers should then be prepared for several such challenges too. First, academic work in a master's program—including at the National Intelligence University—provides virtually no preparation for drafting DID articles or any other similar DIA product. A DID article is very different than the standard five-paragraph

argumentative essay that college and graduate students are expected to master; the five-paragraph essay is primarily devoted to providing a convincing argument on one side of an issue or another. DID articles, on the other hand, are short products that provide the policymaker with key strategic developments and their implications, supported by examples from classified reporting. The DID's short length allows only for assessments, rather than a step-by-step logical argument. It takes more than a little practice to distill a large amount of raw classified reporting into a short product that policymakers can quickly absorb and directly incorporate into policy deliberations.

Second, the Strategic Intelligence officer should be prepared for the challenge of becoming a subject matter expert. This is very different from the training Army officers receive, which is to lead sections, platoons, and companies. Moreover, it means that the officer will find himself or herself doing the job that junior enlisted soldiers typically perform in a battalion, brigade, or division intelligence section.

Not surprisingly, serving as a branch chief also brings a unique set of challenges. The most crucial is learning how a Center actually works. A branch is typically comprised of between 10 and 30 analysts who provide written intelligence products and briefings on their assigned countries. Analysts also participate in intelligence exchanges with military intelligence agencies of foreign nations, and a branch chief may be assigned to organize an exchange. Some of a branch's written products are written on initiative, based on indications of interest from Pentagon customers (provided daily by their assigned DIA liaison officers). Many products, however, as well as most briefings, are specifically tasked. While production of finished intelligence involves multiple levels of review by senior analysts at the branch, division, Center, and Directorate of Intelligence levels, the branch chief is ultimately responsible for all production. In addition to developing and executing a plan for initiative production, the branch chief must also ensure that all tasked products and briefings are completed on time. This activity consumes a significant amount of a branch chief's time.

The DIA has its own policies and procedures—not to mention culture—when it comes to such matters as human resources, finance, training, evaluations, ethics, and discipline. As a federal agency, DIA is an organization that is not operated as a military organization or a private sector enterprise. While discussion of all these policies and procedures is beyond the scope of this paper, suffice it to say that an Army officer must learn and master many of them in order to be successful. A closely related, but no less important challenge, is leading and managing civilians. While many leadership principles the Army teaches apply equally well to a civilian organization, an Army officer must function not as a leader of a military unit but as a civilian supervisor. How then does a field grade Army office who has never worked in a national agency, much less served as a civilian supervisor, learn how to avoid the many pitfalls this situation presents and succeed? The three best sources of guidance are the officer's civilian supervisor, the officer's civilian peers (other branch chiefs), and DIA training.

First and foremost, an officer serving as a branch chief should seek the counsel and guidance of the division chief. Ideally, the division chief will be a mentor. In addition to setting the division's priorities, though, the division chief will likely know the answer or how to find the answer to any question about DIA policies, procedures, and culture that the officer might have. Next, the officer should strive to develop a strong working relationship with the civilian branch chiefs in the division. Branch chiefs within the same division must cooperate in order to succeed when it comes to a wide range of decisions, such as determining which branch will provide an analyst for a rotational or joint assignment. Third, a Strategic Intelligence officer should take all the supervisor and leadership courses required for civilian mangers, as well as the advanced analysis course for senior intelligence analysts (typically GG-14 level, called SIAs at DIA). In addition, a course offered by the Office of the Director of National Intelligence, "Integrating the Intelligence Community," provides an excellent overview of how DIA is integrated into the broader Intelligence Community.

Finally, officers must pay particular attention to mentoring the few NCOs who are also assigned to IIC branches. NCOs are often assigned as line analysts and need analytic training every bit as much as the new civilians DIA hires.

OTHER OPPORTUNITIES

While Strategic Intelligence officers are generally better suited for branch chief than for any other role in an IIC, some have the requisite writing skills and, most importantly, knowledge of a given account to serve as a senior intelligence analyst. Some Strategic Intelligence officers will be reluctant to take on this role since it requires, above all, a mastery of the DID article. Even for accomplished writers with graduate degrees, it takes time, and most of all practice, to be proficient enough at writing a DID article and then to be able to critique and guide a team of half a dozen civilian analysts with up to 10 years of experience at DIA. Officers who have the ability to serve in this role typically have extensive experience at embassies or multinational organizations in the target country, have master's or doctoral degrees from highly-ranked civilian universities, and are proficient in the language of the target country or region.

Since DIA analysts produce daily current intelligence for the Chairman of the Joint Chiefs of Staff and the Secretary of Defense, there are also opportunities to serve in both the branch chief role and SIA role at the Pentagon.[16] There, Center analysts on a year-long rotation prepare the daily intelligence briefing for the Secretary and the Chairman. Since these briefings are prepared daily, covering the entire globe with a much smaller number of analysts than at the DIA's Centers, the analysts must by necessity operate as generalists and rely on the Centers' strategic and more in-depth analysis to support assessments of current intelligence.

Another highly beneficial duty for a Strategic Intelligence officer (usually a major) is as an executive officer in a Center's headquarters. This is a highly sought after position for government civilians as it provides a window into the workings of the Center and its role in the DIA hierarchy. A stint as an executive officer is an ideal follow-on assignment after a year as a line analyst and another as a branch chief. Strategic intelligence officers can also compete for assignments as aides in the DIA front office for the Director and Deputy Directors.

Finally, a Strategic Intelligence officer may be assigned as a Division executive officer, whose main job is to ensure that the Division completes all requisite products, briefings, and other tasks in a timely manner. It is an excellent way to learn how a division functions prior to an assignment as a branch chief.

CONCLUSION AND RECOMMENDATIONS

Strategic Intelligence officers should strive to serve as both analysts and branch chiefs at the DIA regional Centers. This is the best way to learn how the Agency executes its mission of providing the Secretary of Defense and the Chairman of the Joint Chiefs of Staff, as well as forward-deployed warfighters, with intelligence on foreign militaries and operating environments. Moreover, it teaches the officer how to integrate intelligence at the agency level and at any of the geographic or functional combatant commands (which are likely follow-on assignments). The Centers, for their part, should ensure that, soon after arriving, Strategic Intelligence officers enroll in the same courses on analysis and supervision that GG-14 civilians are required to complete. This will ensure that they are as well prepared as possible for any assignment they might be given.

[Author's Note: The views expressed do not reflect the official policy of the Department of Defense, the U.S. Army, the Intelligence Community, or any other element of the U.S. government.]

NOTES

[1] Department of the Army Pamphlet 600-3, *Commissioned Officer Professional Development and Career Management* (Washington, DC: Headquarters, Department of the Army, 2010), 252.
[2] Ibid., 253.
[3] FA 34 Strategic Intelligence Officer Critical Task List, approved October 2016.
[4] Ibid., 252.
[5] Ibid., 254.
[6] Ibid.
[7] John H. Hedley, "The Evolution of Intelligence Analysis," in *Analyzing Intelligence*, eds. Roger Z. George and James B. Bruce (Washington, DC: Georgetown University Press, 2008), 27; see also "Strategy," Defense Intelligence Agency website, accessed December 4, 2016, http://www.dia.mil/About/Strategy.
[8] "2016 Defense Intelligence Agency Strategy," Defense Intelligence Agency website, accessed December 4, 2016, www.dia.mil/Portals/27/Documents/About/2012-2017-DIA-DS-Strategic-Plan.pdf.
[9] Hedley, "The Evolution of Intelligence Analysis," 27; Defense Intelligence Agency, "Strategy"; "Mission Areas," Defense Intelligence Agency website, accessed December 4, 2016, http://www.dia.mil/Careers/Mission-Areas.
[10] "Joint Military Attaché School (JMAS)," Defense Intelligence Agency website, accessed December 4, 2016, http://www.dia.mil/Training/Joint-Military-Attache-School-JMAS; see also "Military," Defense Intelligence Agency website, accessed December 4, 2016, http://www.dia.mil/Careers/Military.aspx.
[11] Cheryl Pellerin, "Intelligence Agency Director Discusses Roadmap for Future," American Forces Press Service, September 16, 2013, accessed December 4, 2016, http://archive.defense.gov/news/newsarticle.aspx?id=120797.
[12] "Mission Centers," Central Intelligence Agency website, accessed December 4, 2016, https://www.cia.gov/offices-of-cia/mission-centers.
[13] Defense Intelligence Agency, "Mission Areas."
[14] "Attacks on USS Cole Spurred DIA's Intelligence Mission," DIA Office of Corporate Communications, October 12, 2014, accessed December 4, 2016, http://www.dia.mil/News/Articles/Article-View/Article/567026/attacks-on-uss-cole-spurred-dias-counterterrorism-mission.
[15] This is the equivalent of a key developmental job for Army officers.
[16] Hedley, "The Evolution of Intelligence Analysis," 150.

MAJ (USA) Michael W. Hein is currently assigned to the Defense Intelligence Agency. During 2010-11, he served as the intelligence officer for the 3rd Battalion, 7th Infantry, 4th Brigade, 3rd Infantry Division, which was responsible for western Anbar Province in Iraq from July 2010 to June 2011. Mike holds BA and BS degrees in History and Biology, respectively, from Stanford University, plus a JD from the Columbia Law School.

[Editor's Note: MAJ Hein was one of my more outstanding part-time students in the MSSI program at National Intelligence University.]

Renaissance Women: A Perfect Match for Science and Technology Intelligence Education

by Kimberly Reubush, Maria-Kristina Hayden, and Dr. Brian T. Holmes

[Authors' Note: The views expressed in this article are ours alone and do not imply endorsement by the Defense Intelligence Agency, the Federal Bureau of Investigation, the Department of Defense, or the U.S. government.]

INTRODUCTION

In March 2016, four female graduate students from the National Intelligence University (NIU) took on an impromptu challenge proposed by their instructor—enter and compete in the U.S. Cyber 9/12 Student Challenge. The Atlantic Council describes the event as "an annual cyber policy competition for students across the globe to compete in developing national security policy recommendations tackling a fictional cyber catastrophe."[1] Despite no institutional history in this competition, the team placed second out of 40 teams from 25 universities. Although it was not surprising to the NIU faculty that the team members performed well, their success prompted a more significant debate about the reasons why they did so well in not only the competition but also in the Anthony G. Oettinger School of Science and Technology Intelligence.[2] This debate sparked an informal research study into the backgrounds of successful female students like this team to better understand their experiences and viewpoints, in an effort to see if there were any key factors they shared in common. The research and observations focused primarily on female graduate students in the full-time program who earned a Master of Science and Technology Intelligence (MSTI) degree from the School of Science and Technology Intelligence at NIU.

The research and observations focused primarily on female graduate students in the full-time program who earned a Master of Science and Technology Intelligence (MSTI) degree from the School of Science and Technology Intelligence at NIU.

According to data obtained from NIU's Office of Institutional Effectiveness, since the MSTI degree's inception in 2012, women have performed exceedingly well in the School's full-time program, based on scientific and technical intelligence (S&TI)-aligned research awards won and overall GPAs. This is in spite of the fact that less than one quarter of the School's full-time graduate student population is female. In 2012 the female population represented only 7 percent of the total, whereas in subsequent academic years it ranged from 21 to 24 percent. According to an analysis of the 10 highest GPAs in the School since 2012, 6 were obtained by female students. Those women attended NIU with undergraduate degrees in biology, international affairs, political science, and marine environmental science, to name a few, and came from a variety of different government agencies and military services. There was no singular undergraduate educational degree or background that was reflected by this particular student sampling.

THE MODERN SCIENCE AND TECHNICAL INTELLIGENCE PROFESSIONAL

There is far more to spying than just spying.[3] Many of today's intelligence analysts and collectors play the role of the modern-day Renaissance man. Leonardo da Vinci, the Italian polymath, is considered the quintessential Renaissance man example because he excelled at several fields in science and the arts.[4] To say that today's S&TI professionals, or functional experts, have to succeed in this interdisciplinary manner would be an understatement.[5] "Scientific and technical intelligence" is based on a working knowledge of the underpinnings of the science and technology that enter into the intelligence realm.[6] Areas of focus often include the analysis of weapons of mass destruction, emerging technologies, and cyber issues among others. Within several years of hiring, these unique intelligence officers are expected to synergize a vast spectrum of organizational tradecraft manuals, foreign and domestic policies, laws, bureaucracies, terms of art, languages and, of course, geopolitical, military, diplomatic, economic, scientific, and technological subjects spanning many countries and actors, spliced together in a global context.[7] It is not enough to master a single discipline to do well and meet the mission requirements prescribed by Executive Order 12333, and driven by Intelligence Community Directive 204, which guides evolving national

intelligence priorities.[8] During the Cold War, many new intelligence hires had degrees related to Russian studies or were military weapons experts and focused on those areas for years.[9] While this type of experience is still valued and used today, this hiring and career paradigm is a distant relic. Most new employees now are required to broaden their expertise within a few years.

WHAT'S IN A GENDER OR DEGREE?

A recent study by the University of Washington described why some science, technology, engineering, and math (STEM) fields have fewer women than others.[10] Nowhere in the study was there evidence of a lack of ability as a primary factor. Instead, a lack of pre-college experience in STEM, gender gaps in belief in one's abilities, and a masculine culture that discourages women from participating were determined the factors most likely to explain gendered patterns in the six STEM fields evaluated. Jenny Anderson also wrote a story in *Quartz* describing gender trends within STEM, across multiple countries, that detailed why each gender is more inclined to pursue different jobs in science-related fields.[11]

A quick survey of the type of educational backgrounds represented by functional S&TI experts reveals that STEM and social science degrees are currently represented. Classic STEM disciplines might be in the majority depending on the agency and office, but that hiring trend is more mission-centric than the universal rule. Some analysts even have both on their resumes. Ultimately, regardless of their educational specialty, every S&TI officer has to learn aspects of the other. One is just as likely to find a technical collector who is a "jack-of-all-trades" as to find a "specialist." Each is needed. Interestingly, new articles communicate the idea that, in today's world, the barriers between the two discipline "groups" are dissolving.[12]

S&TI as an intelligence profession is far more inclusive than it is believed to be.

There are modern undergraduate programs that embody the best aspects of these blended ideals. For instance, Georgetown University created the Science, Technology, and International Affairs major in its Walsh School of Foreign Service.[13] Its website aptly notes that "now more than ever, science and technology are at the heart of international affairs." Regardless, the fact is that S&TI as an intelligence profession is far more inclusive than it is believed to be. The Anthony G. Oettinger School of Science and Technology Intelligence is similar in that regard to its students. A diverse set of experts who can multitask and can draw from a spectrum of educational backgrounds and experiences to fully integrate their knowledge base is needed in order to provide the best possible intelligence products to customers.[14]

RESEARCH FOR IMPACT

A common trait revealed through an interview process was the fact that many NIU female MSTI students were as proactive as they were open to structured guidance. They were also driven to seek creative solutions to unique S&TI problems that would be impactful for their customers. Rarely did they perform research for the sake of research, and few were risk-averse. The background work and outreach required to understand strategic intelligence and its national security relevance in context was just as important as the results many of these women achieved. This approach tended to integrate far more social science methodologies than scientific ones.[15] Ultimately, the female students creatively blended academic theory with intelligence practice in a transparent and synergistic fashion across fields.[16] A significant percentage of female students did this well and therefore won awards.

In 2016, all three of these thesis awards were won by female S&TI students, despite women representing only 21 percent of the School's full-time population that year. Overall, women have won 50 percent of all the S&T awards granted since 2012.

Of the numerous university thesis awards listed in the current NIU Academic Catalog, three are generally aligned to the Science and Technology Intelligence School's curriculum and themes. These include the Scientific and Technical Intelligence Committee Award (STIC), the National Intelligence S&T Award (S&T), and the National Intelligence Officer for Cyber Intelligence Research Award (NIO Cyber).[17] Since 2014, the first year the NIO Cyber award was introduced, female graduate students from the School have won 33 percent (1 out of 3) of the thesis awards granted. Since 2012, they have won 50 percent of the S&T awards (3 out of 6) granted (two students won the award in 2015 as a result of a tie), and 60 percent (3 out of 5) of the STIC awards. In 2016, all three of these thesis awards were won by female S&TI students, despite women representing only 21 percent of the School's full-time population that year. Overall, women have won 50 percent of all the S&T awards granted since 2012. Male students won the S&T and STIC awards in 2012 when the female student population was only 7 percent (or 2 students) of the total. The average full-time population of women and men in the School from 2012 to 2016 was 35 students per year.

WOMEN WEIGH IN

When asked directly, some female MSTI students attribute their success to personal pride. In the male-dominated fields of science, technology, intelligence, and the military, both servicewomen and civilians have a lot to prove—partly to themselves, and partly to the male-dominated battlefield and conference room. It is not about competition, necessarily, but rather preempting the gender stereotypes that never fit many of these high achievers.

Kimberly Reubush and Maria-Kristina Hayden are alumnae of the Science and Technology Intelligence School and co-authors of this article. They shared their personal perspectives of the program and their challenges. Reubush, a 2014 NIU alumna from the Federal Bureau of Investigation (FBI), was the first person from her organization to be nominated for the MSTI program. In order to attend, she had to convince not only her division's management of the positive benefits of the program but also her agency's executive management to modify its application policy. This required a significant amount of time and effort. She believed that it was critical to learn how to better explain the scientific and technical data produced in her job in order to contextualize it in a strategic way to meet the requirements of the Intelligence Community (IC) and better serve her customers. In this manner, NIU's S&TI program seemed like a perfect destination for her. Failure in the program was not an option for her, and could have negatively affected other personnel from her agency seeking these unique educational opportunities in the future.

Reubush, a bench scientist at the FBI accustomed to producing technical forensic evaluations, needed to learn how to think more like an all-source intelligence analyst upon arrival at NIU. She recognized and overcame this challenge by pairing up with a classmate who was a professional analyst but did not have a scientific background like hers. The two collaborated closely to complement their skills and strengthen their foundational knowledge in the effort to succeed. For her thesis research, rather than apply strictly qualitative-based research methods commonly used in social science, Reubush leveraged the capabilities of her home agency, FBI's Terrorist Explosive Device Analytical Center (TEDAC), to conduct a series of improvised explosive experiments to validate critical intelligence, and integrated her quantitative results with qualitative analysis. The execution of this type of mixed methodology was not representative of the majority of NIU theses. There was an inherent risk in the effort based on the limited time available in an 11-month degree program and the complex approval and material acquisition chain involved. She overcame these challenges, and her thesis stood out upon its successful completion. Reubush used the data collected to demonstrate a more definitive answer to address an explosive device's effectiveness, which built on the IC's initial hypothetical assessment.

After graduation, Reubush was assigned a project at the FBI to help determine better ways by which scientific results, originally generated for legal cases, could also be appropriately exploited in the IC. She routinely applies the skills her degree provided, including an ability to speak both scientific and intelligence terms of art, to improve her support to and integration with intelligence analysts. The result is a far better intelligence product.

...the four-woman team won second place at the Atlantic Council's U.S. Cyber 9/12 Student Challenge in 2016.

One year later, in 2015, Hayden received notification through the Defense Intelligence Agency that her third application to NIU's MSTI program had been accepted. Hayden had remained determined to attend because of the similarities between NIU's MSTI program and her multidisciplinary "Science, Technology, and International Affairs" undergraduate degree within Georgetown's School of Foreign Service. While at Georgetown, Hayden applied twice for the Department of Defense Science, Mathematics, and Technology Research for Transformation (SMART) scholarship, and as a senior became the first Georgetown student grantee. The award paid for her final year at Georgetown and paired her with a post-graduation analytic position at the Pentagon. A few years later, NIU became the logical continuation of an education that spanned both STEM topics and strategic issues.

During her time at NIU, Hayden sought to maximize the short 11-month program through extracurricular engagement and networking. She was determined to achieve in the classroom (she earned the second highest GPA in the University) and produce an impactful thesis. For an elective course deliverable in NIU's cyber concentration, she became a member of the four-woman team that won second place at the Atlantic Council's U.S. Cyber 9/12 Student Challenge in 2016. She proudly recalls her team staying up all weekend drafting and presenting U.S. policy response options based on a post-cyber attack scenario for the Challenge. Separately, she created a mixed method research design that entailed interviewing energy executives about their cybersecurity challenges and testing her qualitative conclusions with a quantitative analysis of their responses. Maria ultimately won the 2016 Elizebeth S. Friedman Award in recognition of the master's thesis that most significantly contributes to the U.S. homeland security intelligence mission.[18]

CONCLUSION

After interviewing several different alumni and current female graduate students in the Science and Technology Intelligence School, including Reubush and Hayden, a few final trends were observed. Every student emphasized the desire to learn how to more effectively "bridge the gap," or integrate technical analysis and strategic assessments. There are numerous articles describing the complexities and challenges S&TI analysts face when conveying information to policymakers.[19] NIU's graduate program became a destination for students desiring to learn how to perform this duty more effectively. Reubush and Hayden pursued this goal tirelessly.[20] Regardless of the service or agency the students represented, improvement in this area was a key component of their success.

The School's female students were driven to creatively plan and execute original thesis research that often bridged academic disciplines, methodologies, and intelligence practitioner norms. Incorporating the best aspects of quantitative and qualitative techniques and blending the research to support challenging intelligence mission areas resulted in a superior level of effort well received by senior intelligence officers and the broader national security community.

Similarly, the School's female students were driven to creatively plan and execute original thesis research that often bridged academic disciplines, methodologies, and intelligence practitioner norms. Incorporating the best aspects of quantitative and qualitative techniques and blending the research to support challenging intelligence mission areas resulted in a superior level of effort well received by senior intelligence officers and the broader national security community.[21]

Almost in unison, all of the female students interviewed communicated that they tended to more proactively seek professional guidance when they required assistance than their male peers. This tendency likely enabled a more effective pathway toward achieving success in the classroom and their research. Most tied this to a personal need to be more persistent in reaching their goals. Ultimately, it is clear that these female graduate students in the Science and Technology Intelligence School wanted to represent and prove themselves as top of their class. They certainly did, and the School certainly wants more Renaissance women like them.

[Comments by an expert reviewer, Dr. Arden L. Bement, Jr., former inaugural Director of the Global Policy Research Institute at Purdue University; he is also a former Director of the National Science Foundation, former Director of the National Institute of Standards and Technology, and former Deputy Undersecretary of Defense: "Thank you for this interesting and enlightening article. I found parallels at Purdue's Global Policy Research Institute with the performance of women students in developing policy briefs on global grand challenges that required analyzing the interrelationships among technical, social, and economic factors. Often women students were selected by their teammates as team leaders. Over the past six years, women students in the program have garnered prestigious scholarships for international study, such as the Fulbright, Truman, and U.S. Presidential programs. They had something to prove and they certainly did."]

[Editor's Comment: On August 24, 2017, in Arlington, VA, Dr. Brian Holmes was invited to summarize aspects of this article at the inaugural Science, Technology, and Innovation exchange (STIx). The STIx, an effort led by the Director for Basic Research in the Office of the Assistant Secretary of Defense for Research and Engineering, showcased a spectrum of science and technical investments, outcomes, and innovations from a Defense-wide perspective. Dr. Holmes' summary can be viewed at https://youtu.be/kQAsVqfv6Zg.]

NOTES

[1] The Atlantic Council, http://www.atlanticcouncil.org/programs/brent-scowcroft-center/cyber-statecraft/cyber-9-12 (accessed on January 24, 2017).

[2] The Anthony G. Oettinger School of Science and Technology Intelligence, http://ni-u.edu/wp/academics/schools/college-of-science-and-technology-intelligence/ (accessed on January 24, 2017).

[3] Why the Best Spies in Mossad and the CIA Are Women, https://www.forbes.com/sites/crossingborders/2012/09/30/why-the-best-spies-in-mossad-and-the-cia-are-women/#2bb853af2bb0 (accessed on January 23, 2017).

[4] Biography of Leonardo da Vinci, http://www.biography.com/people/leonardo-da-vinci-40396#synopsis (accessed on January 24, 2017).

[5] Scientific and Technical Intelligence Analysis, https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol19no1/html/v19i1a06p_0001.htm (accessed on January 23, 2017).

[6] Master of Science and Technology Intelligence, http://ni-u.edu/wp/academics/schools/college-of-science-and-technology-

intelligence/master-of-science-and-technology-intelligence/ (accessed on January 20, 2017).
[7] The Global Goals: Economic Transformation in an Interconnected World, http://blogs.worldbank.org/voices/global-goals-economic-transformation-in-an-interconnected-world (accessed on January 25, 2017).
[8] Intelligence Community Directives, https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/intelligence-community-directives (accessed on January 25, 2017).
[9] CIA Analysts Highlight Value of Declassified Cold War Intelligence Reporting on Warsaw Pact Military Forces, https://www.cia.gov/news-information/press-releases-statements/2014-press-releases-statements/cia-analysts-highlight-value-of-declassified-cold-war-intelligence-reporting-on-warsaw-pact-military-forces.html (accessed on February 15, 2017).
[10] Why Do Some STEM Fields Have Fewer Women than Others? UW Study May Have the Answer, http://www.sciencenewsline.com/news/2016101318330092.html (accessed on January 20, 2017).
[11] The origin of Silicon Valley's gender problem, https://qz.com/853435/the-origin-of-silicon-valleys-gender-problem/ (accessed on February 10, 2017).
[12] How Social Sciences Are Converging with STEM, http://www.socialsciencespace.com/2014/01/the-contemporary-social-sciences-are-now-converging-strongly-with-stem-disciplines-in-the-study-of-human-dominated-systems-and-human-influenced-systems/ (accessed on February 20, 2017).
[13] Science, Technology and International Affairs Major, https://sfs.georgetown.edu/stia/ (accessed on February 25, 2017).
[14] What Is Knowledge Integration? http://www.igi-global.com/dictionary/knowledge-integration/16357 (accessed March 15, 2017).
[15] Intelligence Careers, https://www.intelligencecareers.gov/ (accessed on March 1, 2017).
[16] Critical Thinking for Strategic Intelligence, https://www.amazon.com/Critical-Thinking-Strategic-Intelligence-Katherine/dp/1452226679/ref=pd_sim_14_2?_encoding=UTF8&pd_rd_i=1452226679&pd_rd_r=YMHYMNV7R15M30KHWT8Q&pd_rd_w=pJfp2&pd_rd_wg=DDJrU&psc=1&refRID=YMHYMNV7R15M30KHWT8Q (accessed on February 20, 2017).
[17] NIU Academic Catalog: The Scientific and Technical Intelligence Committee Award is presented in recognition of the master's thesis that most significantly contributes to the advancement of experimental science in an IC-related area. Submissions are evaluated for originality, experimentation, lab research, and overall contribution to the knowledge base in an S&T intelligence-related field. The National Intelligence S&T (Science and Technology) Award is presented by the National Intelligence Officer in recognition of the best master's thesis on an analytical science and technology intelligence topic. Submissions are evaluated for originality, methodology, and overall contribution to the knowledge base in an S&T intelligence-related field. The Cyber Intelligence Research Award is presented by the National Intelligence Officer for Cyber in recognition of the best master's thesis in the intelligence fields of cyber analysis, collection, operations, policy, or strategy. Submissions are evaluated based on originality, analytic methodology, technical acumen, and practical application; http://ni-u.edu/wp/niu-academic-catalog/ (accessed on March 1, 2017).
[18] NIU Academic Catalog: The Coast Guard Foundation presents the Elizebeth S. Friedman Award in recognition of the master's thesis that most significantly contributes to the U.S. homeland security intelligence mission. Submissions are evaluated for originality, thoroughness of research, and overall contribution to the nation's homeland security intelligence program. Dubbed "America's first female cryptanalyst," Ms. Friedman solved more than 12,000 coded messages during the Prohibition era, effectively putting rum-running syndicates out of business on the U.S. Pacific and Gulf Coasts; http://ni-u.edu/wp/niu-academic-catalog/ (accessed on March 1, 2017).
[19] More Art Than Science: Intelligence and Technical Topics, https://warontherocks.com/2016/04/more-art-than-science-intelligence-and-technical-topics/ (accessed on March 20, 2017).
[20] A Higher Standard: Communicating Technical Intelligence, https://warontherocks.com/2016/06/a-higher-standard-communicating-technical-intelligence/ (accessed on March 20, 2017).
[21] The Carrot or the Stick? Incentivizing Safe Cyber, https://warontherocks.com/2016/10/the-carrot-or-the-stick-incentivizing-safe-cyber/ (accessed on March 20, 2017).

Kimberly Reubush earned a Master of Science and Technology Intelligence degree from the Anthony G. Oettinger School of Science and Technology Intelligence at the National Intelligence University in 2014, and currently serves as a supervisory forensic examiner at the FBI's Terrorist Explosive Device Analytical Center in Huntsville, AL.

Maria-Kristina Hayden earned a Master of Science and Technology Intelligence degree from the Anthony G. Oettinger School of Science and Technology Intelligence at the National Intelligence University in 2016, and recently joined the Cyber Threat Intelligence Group of a global financial institution as Vice President and Senior Information Security Analyst after serving as an intelligence analyst at the Defense Intelligence Agency.

Dr. Brian T. Holmes is Dean of the Anthony G. Oettinger School of Science and Technology Intelligence at the National Intelligence University, which completed its move from Washington, DC, to the Intelligence Community Campus-Bethesda, MD, in February 2017. He is a former research scientist, U.S. Navy officer, and intelligence analyst.

Five Years Later:
Women, Combat Operations, and Revisiting "The Other Fifty Percent"

by WO1 (ARNG) Kailah M. Murry

Women have a much better time than men in this world; there are far more things forbidden to them.

-Oscar Wilde

INTRODUCTION

In December 2015, then-Secretary of Defense Ash Carter changed the cultural landscape of the military by stating the U.S. military will let women serve in all combat roles beginning in 2016.[1] Just three years prior to this announcement, the *American Intelligence Journal* published an article titled "The Other Fifty Percent: Psychological Operations and Women in Eastern Afghanistan," which discussed the importance of females working in combat operations as psychological operations (PSYOP) soldiers. The intent of the article was to force the discussion of how women can be a unique resource on the battlefield beyond merely manpower. The purpose of this follow-up article is two-fold: first, to review how the military has changed in reference to women participating in combat roles since 2012; and second, to discuss how the Intelligence Community (IC) has long utilized women in operations and leadership roles in a way of interest to the military.

"THE OTHER FIFTY PERCENT" AND REMARKABLE CHANGES IN THE DEPARTMENT OF DEFENSE

The basis for this article came from the original 2012 article that proposed the Department of Defense (DoD) needed to "augment the PSYOP effort [through female presence] or provide proof as to why a female PSYOP detachment or company may need to be created."[2] Beyond the facts that in 2012 women were not yet allowed in certain combat roles or roles at certain echelons, the article argued, "The largest threat and issue for female PSYOP surprisingly did not come from the country or the support unit; it came from within PSYOP itself."[3] Final recommendations included the continuance of utilizing female PSYOP soldiers on combat missions, adding additional female PSYOP soldiers to units deploying into combat environments, retooling the training that female engagement teams receive to mimic PSYOP training, publicizing female PSYOP and Female Engagement Team (FET) missions in order to gain acceptance, and continuing the use of female PSYOP soldiers beyond missions in Operation ENDURING FREEDOM.[4] The conclusions from 2012 are still valid; however, the decrease in forces overseas has since caused a large decrease in PSYOP missions that requires a shift in focus from solely PSYOP missions to all military missions, to include any combat or non-combat military missions.

This article will use the experiences and recommendations noted in 2012 and turn the discussion to how military forces could use females as has been done by the IC since the Revolutionary War.

This article will use the experiences and recommendations noted in 2012 and turn the discussion to how military forces could use females as has been done by the IC since the Revolutionary War. Laura Loftus, renowned writer on the female advantage in combat, states, "Accounting for gender is not easy, nor is it an area of expertise for the military. Each culture is markedly different so there cannot be a one-size-fits-all approach. At the same time, this is not an issue the military can afford to ignore, in light of the relative size of the women's population."[5] There is no doubt the military has had many women in multiple positions that have had an indelible effect on changes happening in the military up through today. Nevertheless, when compared to one another, the military has yet to give the same level of trust and access to women as the IC has over the same time span.

VARIOUS HISTORICAL ROLES OF WOMEN IN THE INTELLIGENCE COMMUNITY

There is a proud history of women serving in the IC long before the military intentionally endorsed females into the armed forces. The positions range from assignments in analysis to administrative processing; others have served in positions that routinely put them in danger in various spy networks, or as case managers, or sabotage operations specialists. Today, women have held leadership roles in intelligence operations and over entire agencies; these women have become involved as "respected and integral parts of the IC."[6] Beyond the agencies of which most are well aware, such as the Office of the Director of National Intelligence (ODNI), women are assuming greater roles in DoD at the executive level; this would include various high-level positions in the Office of the Under Secretary of Defense for Intelligence (USDI). The military needs to replicate this model of developing and utilizing women for the talents that they have or are able to acquire.

The official beginning of the IC came under General George Washington in the Revolutionary War. Women were immediately an integral part of information sharing, in some cases risking life to gather the data they could to pass to the army. "In the early years of the American Revolution (1775-1783), many Philadelphia women passed key information along to General George Washington at Valley Forge. Wives were used to pass secret notes along to help the Continental Army fight the British."[7] The famous Culper Ring utilized women as spies in New York during 1778. The code 355 signified a woman agent. These women "played an important role in the counterintelligence missions that caught Benedict Arnold for treason."[8] Men viewed women through the short lens of being wives, homemakers, cooks, and house cleaners, something the IC took advantage of in order to gather more information.

Nearly a century later, the IC continued to use women during the Civil War. Women gathered intelligence at a time "when the perception of gender roles began to change. Field agents would report to their designated handler, a military or civilian case officer responsible for an agent's activities."[9] At the same time, more than 400 women who desired to fight for the Union or the Confederacy disguised themselves as men to be able to serve in combat.[10] The wartime contributions of women positively expanded the notion of what women were capable of, but fell short of granting any further thought after the war to women serving permanently in the forces, let alone in combat.

Into the 20th century, the Office of Strategic Services (OSS), the precursor to the CIA and the U.S. Special Operations Command (SOCOM), permitted women to serve in clerical, as well as operational, roles. "Of the 13,000 employees at the OSS, approximately 4,500 women served, and continued to stay in the field after the war, providing breakthroughs and contributions throughout the Cold War."[11] Extraordinary women of this time included Virginia Hall. "Virginia Hall was one of the only American civilian women during WWII to receive the Distinguished Service Cross for heroism... Her sabotage operations against the Germans destroyed bridges and disrupted enemy communications. Hall organized three Free French battalions, distributed radios and weapons, aided downed airmen and worked with the French Resistance movement on many highly dangerous missions."[12] Again, much like in the wars prior to World War II, women were a part of lethal and non-lethal missions on the battlefield. Much like the other wars, too, this expanded the perception of women's capabilities. Yet again, the impact of women outside the IC was short-lived and mostly forgotten after the war as men and women returned to their customary roles. Only the IC continued to capitalize on the advantage women have provided throughout the past two centuries.

The IC has long sought out individuals of outstanding caliber to lead the Community without thought given to gender, race, color, or creed, something the military has struggled with in the past century but has recently made incredible strides to overcome.

The IC also has had many women in high-level leadership roles, at times as high as agency heads. Under President William Clinton, Barbara McNamara "was the deputy director of the National Security Agency (NSA), [which is] the highest civilian point under the military director."[13] The CIA has had several female deputy and assistant directors in the past decade, to include Avril Haines and Gina Haspel as previous deputy directors."[14] Letitia Long was the previous head of the National Geospatial-Intelligence Agency (NGA) from 2010 until 2014 and was the first female head of an agency in the IC.[15] Betty Sapp has been Director of the National Reconnaissance Office (NRO) since 2012.[16] All these excellent exemplars of intelligence leaders also held many other leadership positions prior to their stations at the highest levels in their respective agencies. The IC has long sought out

individuals of outstanding caliber to lead the Community without thought given to gender, race, color, or creed, something the military has struggled with in the past century but has recently made incredible strides to overcome.

WOMEN ON THE BATTLEFIELD AND USING THE IC AS A MODEL

Females are providing an edge on the battlefield in both lethal and non-lethal operations. The 2012 article concluded with a quote from Laura Loftus, who stated, "As the Army continues to operate in complex environments, involving extended kinetic and non-kinetic contact with indigenous populations, it is critical for the Army to understand and appreciate the capabilities and potential of indigenous women as peacemakers and peacekeepers."[17] The original article focused on how PSYOP utilizes woman-to-woman contact to gain information for use in combat planning or operations. Furthering this thought, one could say it is critical for the military to understand and appreciate the capabilities and potential of all women as lethal and non-lethal operators. The IC has understood, appreciated, and utilized women in roles that would augment operations beyond what was accepted of the traditional female role.

In traditional societies, women are hugely influential in forming the social networks that insurgents use for support. When women support COIN efforts, families support COIN efforts...

If one understands, appreciates, and desires to utilize women beyond the traditional role, then one cannot ignore the disarming nature of a woman. There are those who subscribe to the belief, "Men will tell women anything, because of their disarming, nurturing, and non-threatening nature. Men never suspect women are intelligence officers. Women can easily play 'dumb Dora'."[18] The same can be true of women. While working overseas, women intelligence collectors do not usually state their intentions outright; they may act as individuals interested in helping the other woman or simply wanting to form a friendship with another woman. Those things may in fact be true, but it is not far-fetched to mention a reliance on quid pro quo in some situations, for example, helping women set up a school in their village while at the same time asking for some information on movement of individuals through the village. Field Manual (FM) 3-24 states, "In traditional societies, women are hugely influential in forming the social networks that insurgents use for support. When women support COIN efforts, families support COIN efforts... Coopting neutral or friendly women through targeted social and economic programs builds networks of enlightened self-interest that eventually undermine insurgents."[19] Disarmament can lead to information for intelligence purposes and this role can become a combat multiplier.

After this discussion, the question remains: What does this mean for women in the combat environment? Why does anyone care if the IC employed women in roles that gained the military more intelligence or access to the enemy, when everyone is looking at the physical aspects of women in combat? The answer is the IC trusts women who are placed in compromising situations, ones that in fact are more intimate and can be considered more dangerous in some circumstances, and the military should follow suit in allowing females into all positions in which they show capability of performance. This is not a new prospect; it is the same fight happening for decades under equality. The articles are numerous about this subject. The IC, too, has rigorous standards for some "delicate" positions that all recruits must meet, something the military could point to as a proven method for selection. Rather than continue the long, drawn-out conversation on whether or not women are worthy of simply being allowed to compete, everyone must allow the transformation of the military to take place, albeit with standards in place that all must meet depending on the requirement of the position.

THE OTHER SIDE OF THE ARGUMENT

There are concerns that continue unabated about the use of females in combat, ranging from physical capabilities to emotional and mental characteristics. The article "Women Warriors: Female Accession to Ground Combat" notes, "Because of their inevitable physical inferiority to their male comrades, women cannot be regarded as fully equal in a Corps [or a military] that prioritizes physical strength."[20] Another article notes, "Female integration has been ferociously resisted through discrimination, harassment, and abuse; the 1991 Tailhook Convention and the 1996 Aberdeen Training Ground are only two of the most notorious of numerous other incidents. There is little doubt that female service personnel have faced very serious discrimination and often-outright harassment in the armed forces." [21] Finally, Brian Mitchell's "Women in the Military: Flirting with Disaster" concludes, "Women are no longer needed in the military [and] their expanding presence is destroying the military's body and soul."[22] The concerns are understandable, but far from being a decisive blow to women serving in an equal capacity to men. One article

even insists, "The number of women entering combat arms would be small, at least initially, and therefore there would be ample opportunity to sort out some quantifiable problems. If these are solved and this experiment proves successful, we should then move without trepidation toward full integration of women."[23] A simple search for articles or books on the subject reveals many that point to the undervalued capabilities of women physically and mentally who could be of great use to the force, as well as the programs in place to combat issues concerning harassment and discrimination.

In addition to the concerns noted above, there are many challenges to women in any workforce, but especially within the military. This would include "a lack of sponsors or advocates, bias and harassment, insufficient workplace flexibility, an increasing number of extreme jobs, outside responsibilities, health issues, voluntary time off… [all of] which affects women at a higher rate than their male counterparts."[24] However, these challenges no longer rest with women; men equally experience most of these trials. If one asks how the single father or husband of a sick partner feels in the same situation, the answer most assuredly matches that of any woman. These challenges are no longer faced by women alone, and should not keep women from being as much a part of the force as they want and prove to be.

CONCLUSION

It is interesting that DoD has long argued over something that already has been on the battlefield since the Revolutionary War. "Military units, not individual soldiers, win wars, and the military must diminish the rights of the individuals who serve in it in order to create effective units."[25] Diminishing the human being based upon gender is not within the bounds of how to operate a highly effective unit.

In order to create lasting change and acceptance, leadership below the highest levels of the executive staffs must move the military services forward. "While different studies of military change disagree whether military organizations can reform themselves or whether they require external leadership, most concur that officer leadership is essential for successful change. Where the officer corps goes, so goes the culture of the military."[26] The President and Secretary of Defense made their decision; women will contend for all military positions and will be included at all levels of military organization. Only leaders with great forethought and ability to see the value of women in all career lines will be able to bring the military force into the future.

As a final note, there needs to be a continuing discussion about mentorship. "Women need to pay it forward as "translators" or mentors to the younger women of today, recruiting and molding them to become successful... They need to leverage the talents, ambition, and drive of the junior members… to reap the full benefits in order to meet an increasingly complex and challenging mission."[27] The military needs leaders such as Letitia Long, previous NGA Director, who once said in an interview:

> I tend not to think about being a woman in a man's world. I really look at it as the challenges and rewards of being a leader in times like today. I cannot deny the fact that I am a woman. Women have made great strides in the intelligence and defense communities, and I think both communities clearly understand the business case for diversity. From an NGA perspective, we really focus on cognitive diversity, not diversity simply based on age, gender or ethnicity. Diversity is about your experience, your background and everything you bring to the table. The challenge is that we are leading during a challenging time, and the reward is being a part of an agency that delivers… products that make a difference.[28]

It is time for the military to move beyond the power of the pen and allow women to join their brothers with the power of the sword.

Countless women have stepped into the limelight to prove the value of women to the force. These women include retired Army General Ann Dunwoody, first female four-star general; Navy Admiral Michelle Howard, first female four-star admiral; and Air Force General Lori Robinson, Commander of U.S. Northern Command (NORTHCOM) and first woman to lead a combatant command. It is time for the military to move beyond the power of the pen and allow women to join their brothers with the power of the sword.

NOTES

[1] Jim Miklaszewski, "All Combat Roles Now Open to Women," NBC News.

[2] Kailah Karl, "The Other Fifty Percent: Psychological Operations and Women in Eastern Afghanistan," *American Intelligence Journal*, Vol. 30, No. 2, 2012, 28.

[3] Kailah Karl, "The Other Fifty Percent: Psychological Operations and Women in Eastern Afghanistan," *American Intelligence Journal*, Vol. 30, No. 2, 2012, 31.

[4] Kailah Karl, "The Other Fifty Percent: Psychological Operations and Women in Eastern Afghanistan," *American Intelligence Journal*, Vol. 30, No. 2, 2012, 32-33.
[5] Laura Loftus, *Influencing the Forgotten Half of the Population in Counterinsurgency Operations* (Carlisle, PA: U.S. Army War College, 2008), 7.
[6] Amy Martin, "America's Evolution of Women and Their Roles in the Intelligence Community," *Journal of Strategic Security* 8, no. 5 (2015), 99.
[7] National Women's History Museum, 2007, available at: http://www.nwhm.org/onlineexhibits/spies/1.htm, quoted in Amy Martin, "America's Evolution of Women and Their Roles in the Intelligence Community," *Journal of Strategic Security* 8, no. 5 (2015), 99.
[8] National Women's History Museum, 2007, available at: http://www.nwhm.org/onlineexhibits/spies/1.htm quoted in Amy Martin, "America's Evolution of Women and Their Roles in the Intelligence Community," *Journal of Strategic Security* 8, no. 5 (2015), 99.
[9] National Women's History Museum, 2007, available at: http://www.nwhm.org/onlineexhibits/spies/1.htm quoted in Amy Martin, "America's Evolution of Women and Their Roles in the Intelligence Community," *Journal of Strategic Security* 8, no. 5 (2015), 99.
[10] The History Channel, 2017, available at: http://www.history.com/topics/american-civil-war/women-in-the-civil-war.
[11] Amy Martin, "America's Evolution of Women and Their Roles in the Intelligence Community," *Journal of Strategic Security* 8, no. 5 (2015), 101.
[12] Defense Intelligence Agency, 2014, available at: http://www.dia.mil/News/Articles/tabid/3092/Article/8362/women-in-intelligence-part-2.aspx.
[13] Dan Holliday, "How Does the Intelligence Community Feel About a Woman Heading a US Intelligence Agency for the First Time?" 2013, available at: https://www.quora.com/How-does-the-intelligence-community-feel-about-a-woman-heading-a-US-intelligence-agency-for-the-first-time.
[14] Dan Holliday, "How Does the Intelligence Community Feel About a Woman Heading a US Intelligence Agency for the First Time?" 2013, available at: https://www.quora.com/How-does-the-intelligence-community-feel-about-a-woman-heading-a-US-intelligence-agency-for-the-first-time, and CBS News, "CIA Gets Its First Female Deputy Director," 2017, available at: https://www.cbsnews.com/news/cia-gets-its-first-female-deputy-director/. Both individuals mention female CIA Deputy Directors, although one notes Gina being the first "career CIA" female.
[15] National Geospatial-Intelligence Agency, "NGA in History: Letitia Long," https://www.nga.mil/About/History/NGAinHistory/Pages/LetitiaALong.aspx.
[16] National Reconnaissance Office, NRO Leadership, http://www.nro.mil/about/leadership/DNRO.html.
[17] Laura Loftus, *Influencing the Forgotten Half of the Population in Counterinsurgency Operations* (Carlisle, PA: U.S. Army War College, 2008), Abstract.
[18] Amy Martin, "America's Evolution of Women and Their Roles in the Intelligence Community," *Journal of Strategic Security* 8, no. 5 (2015), 104.
[19] U.S. Department of the Army, *Counterinsurgency*, Field Manual 3-24 (Washington, DC: U.S. Department of the Army, December 2006), Foreword.
[20] Anthony King, "Women Warriors: Female Accession to Ground Combat," *Armed Forces & Society*, Abstract.
[21] Anthony King, "Women Warriors: Female Accession to Ground Combat," *Armed Forces & Society*, 2.
[22] Brian Mitchell, *Women in the Military: Flirting with Disaster* (New York: Regnery, 1998), 341, quoted in Kim Field and John Nagl, "Combat Roles for Women: A Modest Proposal," *Parameters*, Carlisle Barracks 31.2 (Summer 2001), 74-88.
[23] Kim Field and John Nagl, "Combat Roles for Women: A Modest Proposal," *Parameters*, Carlisle Barracks 31.2 (Summer 2001), 82.
[24] Amy Martin, "America's Evolution of Women and Their Roles in the Intelligence Community," *Journal of Strategic Security* 8, no. 5 (2015), 104.
[25] Kim Field and John Nagl, "Combat Roles for Women: A Modest Proposal," *Parameters*, Carlisle Barracks 31.2 (Summer 2001), 76.
[26] Kim Field and John Nagl, "Combat Roles for Women: A Modest Proposal," *Parameters*, Carlisle Barracks 31.2 (Summer 2001), 77-78.
[27] Amy Martin, "America's Evolution of Women and Their Roles in the Intelligence Community," *Journal of Strategic Security* 8, no. 5 (2015), 109.
[28] T. Fox, "Leadership intelligence: An interview with Letitia Long of the National Geospatial-Intelligence Agency," *The Washington Post*, 2012, available at: http://www.washingtonpost.com/national/onleadership/leadership-intelligence-an-interview-with-letitia-long-of-the-national-geospatialintelligence-agency/2012/06/21/gJQAvJ2lsV_story.html? wpisrc=nl_fedinsider, quoted in Amy Martin, "America's Evolution of Women and Their Roles in the Intelligence Community," *Journal of Strategic Security* 8, no. 5 (2015), 107.

WO1 Kailah M. Murry is a Military Intelligence warrant officer in the 35th Infantry Division, Kansas Army National Guard (KSARNG), and Chief, Student Operations Division, Department of Distance Education at the U.S. Army Command and General Staff School, Fort Leavenworth, KS. She has served in multiple intelligence, psychological operations, and training and education positions throughout her 20-year career. She holds an MA in National Security Studies from American Military University, an MA in Training and Development from Midwestern State University, and is currently a graduate student in the Master of Science of Strategic Intelligence program at the National Intelligence University. She is a valued contributor to AIJ, *having written articles and book reviews in the past.*

Understanding Female Martyrdom

by Dr. Bina Patel

INTRODUCTION

Why would someone want to strap five pounds of C4 onto a suicide vest around their body? Let alone, why would a woman want to do it? To put this into perspective, 1.25 pounds of C4 can destroy a truck. Therefore, imagine the extensive damage five pounds can do. For one thing, terrorists are unlikely to offer themselves as subjects of experiments! Attempting to understand their activities from a distance has led to inaccurate conclusions. As millions of patrons who support suicide bombers can attest, one country's jihadi is another country's soldier. So what is a terrorist? Let us begin by attempting to define "terrorism."

According to Bruce Hoffman, defining terrorism has been challenging .[1] Although Hoffman states that a concrete definition is lacking, the media have taken the lead in communicating a complicated message of labeling a range of events as terrorist-related. Various sources have defined terrorism as violent events executed by extremist groups to invoke havoc and fear in society. What we do know is that terrorism is related to violent events that create terror within any society and community. Suicide terrorism is a by-product of terrorism and utilized as a tool to impose fear in any given society.

Suicide terrorism has been challenging to understand, and conclusions made by researchers, experts, and psychologists who have interviewed attempted suicide bombers have helped to create a profile of a terrorist. As with anyone, however, characteristics that define a person are unique to each individual. Hence, what is a suicide bomber? Can a general profile of one suicide bomber be applicable to the next? How does the profile differ with gender?

The purpose of this article is to depict female suicide terrorism, while understanding the radicalization process. This article will present an alternative view of suicide terrorism, which focuses on the underlying issues and self-struggle that Islamic women experience against cultural and religious stigmas, gender bias, and postpartum depression. Their allegiance, the Achilles' heel, is to end their grief, leading them to martyrdom. Regarding the theory of radicalization, a conceptual proposal will explore religion, gender bias, and allegiance by examining successful female jihadis including Wafa Idris, the Black Widows, and Muriel Degauque. Additionally, the article will conclude by introducing a potential redefined profile of the future female suicide bomber.

RADICALIZATION

Suicide terrorism may be defined as an individual who has turned to violence or has been radicalized with the intent of executing a *fatwa*, or religious decree.[2] Men who have been radicalized have traditionally carried out suicide bombings and are perceived as martyrs or entering martyrdom. Nevertheless, a new idea has emerged: female suicide terrorism. "Death to America! Death to America!" chant several hundred women wearing solid black *abayas* that cover their bodies from head to toe.[3] They are video-recorded standing in a perfect line of ten women, each wrapped in a khaki-colored suicide vest, strapped with approximately eight cylinders or de facto pipe bombs hugging their waists tightly. The cylinders are situated on the vests, which have shoulder straps that cover their entire upper torso. The vests are packed with nails, screws, bolts, ball bearings, and other substances that function as shrapnel to maximize the number of casualties in the explosion. Each vest weighs between 11 and 44 pounds. The women are preparing their own destinies in a Suicide Induction Ceremony to be the next *shaheeda* or jihadi.[4]

According to the Clarion Fund,[5] jihad is portrayed as a declaration of war against the Western culture, jihad is in a war with the West, and a jihadi is an individual who has been radicalized and wants to die as a terrorist. What percent of Muslims are considered radicals? There are over one billion Muslims in the world, and it is difficult to estimate how many of them support radical Islam. Walid Shoebat, a former PLO terrorist states, "There are 1.2 billion Muslims, of which fifteen percent support radical

Islam; this is as big as America. And the one thing that is bad about it is that they are spread all throughout."[6] In essence, radical Islamists are unseen.

Factions within the Islamic communities have taken advantage of ideologies to justify violence, which is defined as terrorism by some. Terrorist organizations have utilized the foundations of Islam to mislead followers, including women. Jihad is one such example.

Before we take a deeper dive into radical Islam, let us first gain an understanding of Islam in general. It is the youngest of the four major world religions, but the second largest with over one billion followers. The four major religions include Hinduism, Judaism, Christianity, and Islam. Islam was founded by the Prophet Muhammad in 610 C.E. in the town of Mecca. According to the BBC, Islam is the "submission to the will of God" and the way of life for all believers.[7] Islam has blossomed on the foundation of peace, loyalty, brotherhood/sisterhood, and collectivism. Group identity, groupthink, exclusions, solidarity, principles, and legitimacy are guided by the texts of the Qur'an, Hadith, and Sunnah, which include the spiritual teachings of Allah and the Prophet Muhammad. Islam's foundation is built on the belief that there is one God, Allah, who through the Prophet has developed the five pillars that serve as guiding principles. Additionally, by declaring one's faith to Allah and praying five times a day, the mind, soul, and body are united spiritually for all believers.[8]

Factions within the Islamic communities have taken advantage of ideologies to justify violence, which is defined as terrorism by some. Terrorist organizations have utilized the foundations of Islam to mislead followers, including women. Jihad is one such example. Cook defines jihad as "holy war."[9] The term has many complex meanings that vary from political to religious influences. The term today is perceived as warfare, but in truth it does not imply actual warfare. According to Cook, "The Islamic definition of 'jihad' was expanded as a result from its original meaning to encompass 'struggle' or 'striving.'"[10] The Qur'an, the Holy Scripture of Islam, emphasizes the need to use jihad as a means of spiritual warfare and wage it at the time of need. Cook further states that the Hadith, a scripture created from the teachings of the Prophet Muhammad, also indicates that "greater jihad" is not equivalent to aggressive warfare, or "lesser jihad."

"Greater jihad" represents an inner struggle, which focuses on controlling oneself from materialism, and being remorseful for desiring gold, silk, and other luxurious tangibles as well as engaging in pre-marital sex. Lesser jihad, also referred to as outer jihad, represents the duty to defend against non-Muslims. Non-Muslims were once perceived as resisting the teachings of Allah and the Prophet Muhammad. Today, this belief is operationalized by terrorist organizations. Historically, the notion of aggressive jihad was first introduced by moralists al Muhasibi and Ibn Abi al-Dunya in 894 and applied only to male warfare as women and children were not allowed to partake in combat. Cook states that the writings of both Islamic scholars focused on the combination of lesser and greater jihads including fighting aggressively for the primary purpose of spreading the teachings of Islam, while eradicating negative emotions of sorrow, lust, and fear.[11]

Based on the interpretation by Cook, are we able to take the definition of lesser jihad and apply it to suicide terrorism? For example, can suicide terrorism be considered a form of aggressive jihad, or "lesser jihad"? Or is the term completely misinterpreted and misunderstood? It is difficult to say. Moreover, is lesser jihad applicable to radical Islam? Terrorist organizations have successfully expanded the term to fit their objectives of global warfare against non-Muslims, including redefining Islam to radical Islam.

"Jihad is the word of Allah, a holy war," according to the Clarion Fund.[12] From a young age, children are taught to believe that jihad is defined as holy war. Teaching children and adults, specifically women, misinterpreted religious verbiage is key in the process of radicalization. Radicalization is a major element of the jihadi belief. In his article, "Radicalization into Violent Extremism I: A Review of Social Science," Randy Borum states "the term *radicalization* is used to refer to the process of developing extremist ideologies and beliefs. [13] The term *action pathways* will refer to the process of engaging in terrorism or violent extremist actions." Nevertheless, several social theories have attempted to define radicalization, most of which have failed to define the term.[614] For the purposes of this paper, radicalization will be defined as an individual turning to violence with the intent to mobilize a deadly attack.

Although there is no shortage of human bombs, terrorist organizations that have traditionally relied on males to execute missions are now turning to women, who are serving as successful implementers of suicide terrorism. Traditionally, women have not been allowed to serve in combat as their role is domesticized, and terrorist organizations such as Al Qaeda did not allow women to

engage in suicide missions, which are considered equivalent to combat. Today, women are heavily recruited for such missions. Consequently, what has changed in the radical societal belief? And why do women want to become martyrs? Simply, are women radicalized to become martyrs?

While we may be led by terrorist organizations to believe that women are dying in the name of religion for their country, the true understanding of any woman's desire to die as a bomber is difficult to assess. In fact, understanding why anyone would want to die with a bomb strapped to his/her body is hard to imagine. Studying women through the lens of postpartum depression as a result of cultural and gender suppression, supported by radical religious verbiage collectively, may provide an alternative view of why women desire to escape their immediate worlds.

Postpartum Depression

The National Institute of Mental Health (NIMH) defines postpartum depression as a mood disorder that impacts women based on the changes in the levels of their hormones (estrogen and proestrogen).[15] The levels of the hormones drop significantly, causing chemical changes in the brain that may trigger mood swings. Depression, sadness, and anxiety are a few of the symptoms of postpartum depression that make it difficult for women to complete daily tasks and care for themselves of their families.[16] After giving birth, women may initially experience "baby blues," or fatigue, unhappiness, and feelings of worry. This stage is usually mild and lasts approximately two weeks post-delivery.

Nevertheless, postpartum depression may begin prior to pregnancy. The NIMH states that women who are depressed pre-pregnancy, diagnosed with bipolar disorder, or have experienced a traumatic life event in their lives, such as rape, loss of a close relative/friend, and may lack strong emotional family or community support, are likely to experience a high level of postpartum depression post-delivery.[17] Extreme cases of postpartum depression range from experiencing anger or rage, losing interest in activities that were once enjoyed, and withdrawing into complete isolation from friends and family to self-harm or suicide due to the long-lasting emotions. Such symptoms may suddenly result in postpartum psychosis.

Postpartum psychosis is rare and occurs in a very small percentage of women. Approximately one to two women experience postpartum psychosis out of one thousand deliveries.[18] Symptoms include paranoia, rapid mood swings, difficulty in communication, and delusions of strange beliefs, irritation, and suicides. According to Postpartum Support International, there is also a five percent suicide rate in women who experience postpartum psychosis.[19]

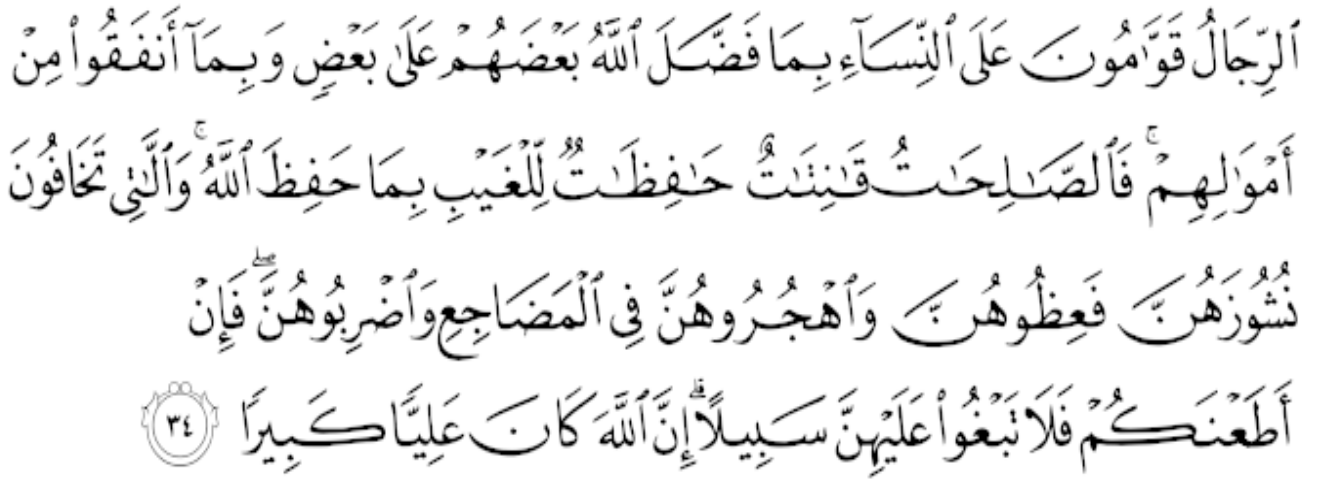
Lack of societal support combined with gender suppression may explain how postpartum depression may affect women who have chosen to commit suicide terrorism. To closely understand the relationship between gender suppression and postpartum depression, let us begin by first understanding the role of women in Islamic society. Umma Salama, one of the wives of the Prophet Muhammad, was noted in history as having asked her husband over 1,400 years ago why the Qur'an was not addressing women.[20] An answer to Umma Salama's question was never found. Instead, when the Qur'an was created, there was little room left for doubt regarding gender equality.

Gender: Role of Women in Islam

Although men and women are referenced as equals in the Qur'an, the treatment of equality has not surfaced in society. Women continue to be treated as third-class citizens in Middle Eastern societies. Traditionally, states McAuliffe, in Eastern religions such as Islam, patriarchy has set the cultural norms and expectant behaviors for the female sex, so that women are perceived to be less moral and intelligent; therefore. They are viewed as inept at interpreting religion correctly and passing judgment on the religious knowledge.[21]

Based on McAuliffe's research, historically and currently speaking, women have not been given the opportunity to question their role as females, but rather they are told in the Qur'an how to behave as females. May we assume that Umma Salama's question was not answered, as male scholars who wrote the Qur'an did not want women to become educated or equal in gender? We can assume any questions that Umma Salama may have asked in relation to the female gender equality were discarded. During Muhammad's life, men were known to thwart the provisions in the Qur'an specifically for women by misinterpreting its suras or verses. Imaginably, the intent may be to purposely manipulate religious text against women's equality, which has encompassed radical Islam led by terrorist organizations.

Although there are no claims of male dominance over women in the Qur'an directly, that is the interpretation by imams or religious clerics who claim that male dominance is a true belief of God[9]. In Arabic, the verse is listed as the following:[22]



The McAuliffe English translation states:

> Most Muslims also read Q4:34 as mandating a wife's obedience (qanitat) to her husband and giving him the right to beat (daraba) a rebellious (nushuz) wife…qanitat refers to an attitude of obedience to God on the part of all believers and not to a wife's obedience to her husband…the Qur'an did not force the Prophet's wives to obey him and neither did he. Nor did he deal with occasional marital discord (nushuz) by abusing them.

Per McAuliffe, the Qur'an reaches a general population so that God's words are to be obeyed without question, inherently implying that obeying God is equitable to conforming to one's husband or the eldest male in the family. *Imams* or religious clerics are preaching similar verses to their followers. The cycle of female suppression in Islam therefore continues.

Furthermore, according to Berko and Erez, female suicide bombers seek to participate in missions as they are longing for gender equality.[23] Traditionally, women who are born with a disability, cannot bear children, are tainted in society by a divorce, are falsely accused of adultery, desire to become educated, are lesbians, or wish to engage in other actions that are deemed to be against the norm become outcasts in society and are easier to prey upon for recruitment purposes.[24] The societal pressures foster severe depression, stress, anger, and violence in the home, thus encouraging Islamic women to gain personal freedom.[25]

According to Mia Bloom,[26] women live with misconceptions and stigmas daily in the Middle East: "The common assumption is that female terrorists must be *more* depressed, *crazier*, *more* suicidal, or more psychopathic than their male counterparts."[27] Bloom does not imply that women are depressed or crazy, but rather that the perception is that the female gender is strongly inferior to the dominant male in Islamic society.

In addition, Bloom and Winter write that the veil is another hot topic of controversy that is linked to female oppression.[28] Female followers of Islam are required to wear an abaya, burqa, or hijab. An abaya or burqua is a black veil-like gown that covers a woman's body from head to foot. A hijab is a headscarf that is loosely worn to cover the head, and is traditionally worn by both males and females. A niqab is worn to cover the full head and face, with the exception of the eyes. Women residing in countries that follow strict Wahhabism and Taliban ideologies, including Afghanistan, are required to wear the *niqab*. Islamic women in most or all Western and some Eastern nations are allowed to wear Western clothing including pants and long-sleeved shirts, with a hijab, in comparison to the traditional attire of a burqa. However, in most Middle Eastern nations, women are expected to cover themselves completely with traditional attire.[29] It is important to note that not all women in Western nations wear the *hijab*. It is the level of enforcement and personal beliefs that also enables a woman to put on the *hijab* daily.

The perception of the veil globally is believed to be a symbolic requirement established by the Prophet Muhammad. The Prophet's purpose to indoctrinate in the wearing of the veil was to protect Muslim women against the evil of a man, or hide the female body that men sexually desire. The veil, according to Benslama,[30] is also a necessary religious symbol that is required at the time of

prayers. The purpose of the veil can be understood with two varying perceptions: the theological perspective of the veil, and intuitive power.

The theological perception of the veil is to understand it as non-symbolic. According to Benslama, the veil is considered serving as a "filter of a woman's body as it protects it against the body's disturbing effects."[31] Traditionally, Islam indicates that a woman's body is evil against men, as it is used to lure them into sexual behaviors. Consequently, the belief became a religious requirement, which resulted in political reinforcement through Shari'a law. Benslama further states, "The veil is governed by the theological logic of real control over a woman's body for the purpose of subjugation…Note that some Islamist movements do not impose the wearing of the veil, based on the strict requirements of Islamic law they claim to follow."[32]

The duplicity that exists with veiling and unveiling can be revealed in the reasons why women should not become *shaheedas*. However, exceptions are made and rules are bent when needed by jihadists. Technically, in Arab society, men are forbidden to look at a naked woman's body, "even after she blows up," states Berko.[33] Why all this fuss over a veil? The veil perhaps is used as a means of control among Arab societies.

Also, Barlas[34] states that women historically were not required to wear the hijab, niqab, and burqa religiously. Rather, wealthy families requested that their wives, daughters, and sisters cover themselves so that others did not look at them. Likewise, the Prophet Muhammad also requested his wives cover themselves.[35] The tradition continued with the Prophet and the wealthy, and was later adopted by the lower class. Hence, the societal norm became ingrained as religious doctrine, making it a requirement for women to cover up. Furthermore, feminist theorists state that the veil is not only perceived as a form of control over women; it is also another tool to help a man avoid pre-marital sex. According to Benslama, Islamic women who are required to wear the *burqa* are seen as objects of "seduction-sedition."[36] Perhaps, the latter implies that Muslim women are deemed to be the forbidden fruits, alleged to be monsters of lewd and perilous charms.

One reason for insistence on the wearing of the *burqa*, *hijab*, and *niqab* is that it conceptualizes women as subjects, rather than as an individual. Hence, perceiving women as subjects has enabled terrorist organizations to hide suicide vests and bombs beneath clothing to operationalize suicide missions. Benslama states that the veil is a facade so as "in its canonical form, which does not allow any patch of skin to appear, it reduces every woman to an anonymous and undifferentiated entity insofar as she is a person."[37] So why do women participate in suicide missions and not seek to live through their own identify? Perhaps an alternative theory on radicalization may clarify why women desire to escape their world.

Allegiance: The Achilles' Heel

With the study of suicide terrorism, I find that radical religious ideologies and gender inequality are contributing elements that have also been found in publications by Berko, Bloom, and Barlas. Allegiance is an element that has not been successfully identified or associated with suicide terrorism. Although history has proven that allegiance is a powerful tool, allegiance is subject to interpretation. For the purposes of this study, allegiance is defined as loyalty and without defect to one's family, religion, culture, and group.[38] The manner in which allegiance is utilized depends on each individual.

The survival of terrorist groups today has been largely due to loyalty among the members of the organizations. Allegiance, as indicated by Eli, is the reason that there are a few solid terrorist organizations today.[39] Terrorist organizations have discovered that, in order to prevent defection, their mission of coordinating violence should become the "Achilles' heel" where loyalty begins from the suicide bomber. For example, the loyalty should be between the suicide bomber, recruiter, operator, coordinator, driver, and terrorist organization.

Eli further states that radical religious organizations experience a high level of defective constraint and a higher rate of survival. Fulfilling societal needs, while conditioning vulnerable populations, is the key for radical religious organizations to obtain and retain long-term supporters, while limiting defectors.[40] For example, recruiters are able to enter any vulnerable environment to recruit females for suicide missions. Once they penetrate, their recruitment process begins. Women are known to be targets as they are more likely to remain loyal and defect in fewer numbers, in order that shame not be brought upon their families. The women are told that their loyalty to the organization and mission will give them the opportunity to die as a shaheeda, a legitimate form of death in radical Islam. This will make their families honorable and provide them with some financial assistance. They will also die in the name of Allah, and proceed to Paradise without feeling any sense of retribution against their religion.

According to Speckhard,[41] a *shaheeda* will also attain personal liberation while dying as a "legitimate" cause. Speckard also indicates women are more likely to act on emotion than men due to a trauma they have experienced. Money, fame, and other materialistic tangibles cannot replace the emotional trauma felt.[42]

Therefore, are female suicide bombers not known to defect, as they are capable of secrecy until death? While this may be difficult to conclude as very little evidence exists to support the answer, when a female commits to a suicide mission, either through volunteering or recruitment, she is requested by the recruiter to remain discreet. In essence, she cannot relay the mission information to the patriarch of her family, who serves as her guardian.

According to Berko, a driver, escorted by another participating female, collects women who are in training for their suicide missions.[43] Therefore, when a potential suicide bomber tells her family that she is going to go out with her friend, it does not create any suspicion. The other female in the car is not a friend, but rather another recruiter. The attempted female bomber is sworn to secrecy, which she keeps until her death. Therefore, it can be concluded that a female has the ability to remain secretive, emotionally and physically strong, and aligned to executing the mission with allegiance. Allegiance is the final component and my contribution to understanding female martyrdom. We examine next how a woman is radicalized to carry out a successful suicide operation.

Theory of Radicalization

Radicalization can be characterized as involving three major steps: (1) the cognitive processes which can be examined by studying psycholinguistics; (2) the attainment of an unconditional belief in extremism and fearless desire to execute a suicide mission; and (3) the successful execution of a suicide mission. However, none of these is possible unless there is a sense of collectivism present at the macro environmental or external level, combined with personal motivations. Emile Durkheim's theory on collectivism indicates that individuals do not think independently, but rather in the form of groupthink.[44]

Radical clerics justify the need to engage in holy war by knowingly and deliberately misinterpreting Islam, which causes a behavioral shift in the belief in, and acceptance of, suicide missions as a religious duty and obligation.

Radicalization can be seen to arise when societal perceptions in political and religious environments skew the beliefs and attitudes of an individual forming a new subjective identity. "The actions of terrorists are based on a subjective interpretation of the world rather than objective reality. Perceptions of the political and social environment are filtered through beliefs and attitudes that reflect experiences and memories."[45]

In other words, the collective acceptance of suicide missions by terrorist organizations is promoted through mutual support from the community, and influenced heavily by radical clerics. Radical clerics justify the need to engage in holy war by knowingly and deliberately misinterpreting Islam, which causes a behavioral shift in the belief in, and acceptance of, suicide missions as a religious duty and obligation.

Interpretation of language may be subjective for each individual, depending on how the subject comprehends the content. Language has influential power. It is a by-product of reason. The particular use of language in messages has more or less persuasive power, depending on factors such as "the value system, the effort, and motivation of receivers."[46] Psycho-linguistics theory tells us that the manner in which content is taught and received by the subject is dependent on how it is interpreted. In the case of the female suicide bombers, it can be assumed that the Islam they know and are taught is radical jihadi ideology, not the Islam that is taught to mainstream Muslims.

In addition to the psycho-linguistic theory, language acquisition theory further examines how a subject reads and comprehends the text, as it is created in the mind.[47] The theory states that the micro and macro environmental factors may impact how an individual's vocabulary is acquired based on the textual comprehension.[48] Therefore, I conclude that radicalization is executed in a specific manner and allows a follower to accept radical Islam as the true form of Islam.

CASE ANALYSIS: CULTURE OF SUICIDE TERRORISM -- AL AQSA MARTYRS BRIGADE

Support systems operated by terrorist organizations such as Al Aqsa Martyrs Brigade succeed in dissonant environments such as Palestine. Al Aqsa Martyrs Brigade is the military and armed wing of Fatah, the primary political party of Palestine. The name Al Aqsa denotes the al-Aqsa Mosque, located in Jerusalem at a holy site known by Muslims as the Nobel Sanctuary. It is also referred to as the Temple Mount by Jews. The organization was founded in 2000 at the start of the Second Intifada.[49] It is a leaderless jihadi group that is formed of local and self-governing units that fight in common allegiance to Fatah. Fatah has been associated

with the former leader of Palestine, Yassar Arafat, who is said to have once funded the terrorist organization. Fatah was founded in 1965 by Arafat.

This organization is known to recruit women to become martyrs for the cause of ensuring Palestine becomes a free state. Per Fletcher,[50] the objective of this organization, including female volunteers, is to fight for Palestinian nationalism rather than political Islam. Following the suicide mission of Wafa Idris, the organization used widespread propaganda to effectively recruit women for future suicide missions. The marketing itself has provided a sense of allegiance within the organization, making it a highly efficacious terrorist entity that has successfully carried out suicide missions.

Wafa Idris

Wafa Idris was a female who detonated a 22-two pound bomb in Jerusalem on behalf of the Al Aqsa Martyrs Brigade on January 27, 2002. Idris' narrative includes suppression of the female role in radical Islam, postpartum depression, and religious backing by the Palestinian community, all of which resulted in a successful suicide mission. Idris, today, is known "as the first Palestinian woman to willingly martyr herself," states Speckhard.[51] Idris brought shame to her family, because she was unable to have children; and as a result, her husband was forced to divorce her and take on another wife. In Islamic society, in which a woman's role is to be a wife and mother, she was considered worthless. Idris was rejected by society and labeled as a divorcee, which is also a stigma against Islamic women. Idris was supported in her mission by her elder brother, a member of the Al Aqsa Martyrs Brigade, who consistently preached radical Islamic ideologies. Based on Speckhard's account, we find that Idris turned her depression into action. With a combination of societal suppression and stigma, Idris' depression grew worse with her inability to have children. Her husband's family also pressured her to have children, leading to emotional and physical despair. In conjunction with marital rejection and conflict, lack of family and social support, following her divorce she turned to radical Islam. She dealt with the deaths of people she witnessed while volunteering at a humanitarian organization, some of whom were injured by Israeli forces during home raids.[52]

In conclusion, Idris experienced prenatal and postpartum depression after delivering a stillborn baby that left her with an infection, resulting in the inability to have children in a conservative Palestinian culture, where marriage and the desire to have a family are customary. "A barren wife can hardly create a family," states Speckhard.[53] She was introduced to jihadi ideologies largely supported by the Palestinian community. In Palestine, although many of the families of the female martyrs reject suicide bombings by their daughters at a nuclear level, there is strong support by the public at large for female martyrdom. In fact, most women who commit suicide attacks are active in their society, whereas 49 percent of individuals who commit conventional suicide have no close friends and do not belong to any social organizations. Moreover, 45-66 percent of people who commit conventional suicide have a history of depression, and 30 percent have previously attempted suicide. We should thus expect female suicide terrorists to exhibit similar signs of mental illness prior to their attack.[54] In the case of Idris, the theory of radicalization stands as it addresses acceptance of radical religious ideologies, gender inequality, and postpartum depression, all while retaining the secrecy of her role as a female martyr.

Community support for female martyrdom in a gender-suppressed religion continues to play a vital role in encouraging women and girls to become suicide terrorists.

In Palestine, suicide missions are second nature. Societal support for suicide terrorism, including propaganda and heavy media influences, have encouraged the technical shift of utilizing women as bombers to an ideological and psychological acceptance by society, specifically when women are obligated to respond to a call of duty by terrorist organizations to become martyrs. Therefore, community support for female martyrdom in a gender-suppressed religion continues to play a vital role in encouraging women and girls to become suicide terrorists.

The Chechen Rebels: Black Widows

In comparison to the Palestinian community, I find that community support, radical ideologies, and gender inequality once existed in Chechnya. A major study conducted by Speckhard and Akhmedova[55] provides insight into the first female terrorist organization, the Black Widows. The name Black Widows was coined by the Russian press in reference to the black burqa, worn by the women during their suicide missions. The fame of the Black Widows arose after their unsuccessful attempt to launch an attack at the Dubrovka Theater in Moscow in October 2002. Nineteen females appeared in black mourning attire with bombs fastened to their bodies.

According to Speckhard and Akhmedova, the suicide mission was an attempt to take vengeance against Russia for the deaths of their sons, brothers, and fathers during the struggles in the Chechen war with Russia. This was a

politically-based attempt to gain revenge against Russia. Speckhard and Akhmedova also state that, aside from the smaller part that religion played in the attempted mission, other motivational factors influenced the women to become human bombs, including trauma, revenge, and gender empowerment.[56]

Nineteen of the 26 female subjects accepted radical Wahhabist ideologies connected to suicide missions. An additional seven female subjects were also strong believers in radical Wahhabism and were connected through family members when they joined the suicide mission. Also, Speckhard and Akhmedova found that the women were initially non-radicalized Muslims with strong traditional roots, but suffered from depression following trauma due to the death of a loved one or the disappearance of a family member after an arrest made by the Chechen police.[57]

Al Qaeda recognized the fight between Muslims and Russians as an opportunity to propagate radicalism.

To understand the rise of the Black Widows, it is vital to focus on the history of Chechnya.[58] Prior to the start of the war, Chechnya enjoyed a de facto independent period, which later resulted in high crime, corruption, and mass armament. As tensions between the Russians and Chechens grew, the first war broke out. The two-year battle resulted in the destruction of 60-70 percent of housing and infrastructure due to heavy bombings.[59] The post-war unemployment rate reached 80 percent. Furthermore, the number of Chechens residing in refugee camps reached over 10,000, which caused long-term mental and physical damage, including depression. It was during this time that radical Wahhabism took a stronger stand, and suicide terrorism became a new machine to be used against the Russians.[60]

Between the first and second Chechen-Russo wars, life for the Islamic community deteriorated. During this time, states Billingsley, radical Islam took hold among the youth and women, an extremely vulnerable population.[61] The politicization of Islam increased, as Chechen Muslims were encouraged to follow the jihadist ideology. With the growing trend of Wahhabism and a continuous cognitive effort instilled by the *imam* to preach radical ideologies, unity resided in social nationalism, where the religion served as a righteous alternative to desalinate the young and faithful.[62]

Furthermore, al Qaeda recognized the fight between Muslims and Russians as an opportunity to propagate radicalism. Al Qaeda's effort to send fighters against Russians was to expand their efforts of global jihad, which began in Chechnya as early as 1995.[63] The time between the first and second war was a strong period of transition for the youth and military commanders who widely accepted radical jihad. At the forefront, Umar Ibn al-Khattab, a Saudi native, led the radicalization process of the foreign mujahedeen in Chechnya. According to Billingsley, the radicalization process was highly effective as it served the self-reinforcing cycle.

The cycle became a breeding ground as youth from the Middle East and Europe flocked to Chechnya to join the cause against Russia and increase terrorism. Ibn al-Khattab, a Saudi-born Chechen military leader present during the first and second Chechen wars, became a key figure with the rise of global jihad in the Eastern European region.[64] Using funds being sent by Osama bin Laden, propaganda increased with the distribution of videos in the Chechen region and the assistance of Ibn al-Khattab's input.[65] His contributions included promoting the videos, which portrayed Chechen fighters as jihadists, and the "endeavors" of the mujahedeen. The videos were being launched and distributed at local mosques, which resulted in creating sympathy for the radicals. Suicide terrorism was supported by the community, a key element in the theory of radicalization.

Women also began to respond to the call of duty emphasized by Ibn al-Khattab. It is important to note that, prior to 2000, no suicide attack occurred in Chechnya. In the Chechen community, al-Khattab is famously known for the rise of female suicide terrorism.[66] In June 2000, al-Khattab successfully recruited Khava Barayeva and Luiza Magomadova as the first members of the Black Widows or Brides of Allah. Their mission was to drive a truck full of explosives into the Russian army base in Chechnya. Following the successful completion of the first female suicide mission, community support began to experience a shift in the female role, as women were asked to fulfill their duties as "martyrs."[67] Were these women suffering from survivors' guilt and post-traumatic stress disorder?

Furthermore, in Chechnya several religious schools were funded by foreign monies that taught only radical Wahhabist ideologies. Women were now forced to cover their bodies and follow Shari'a law.[68] This was the initial foundation set forth with Wahhabist radical influences on women. O'Rourke states, "Chechen females who join terrorist groups in Chechnya actually move backwards in some ways—they take on the traditional Arab dress

which has never been indigenous to Chechnya, dress hijab and devote themselves to more traditional roles within groups except for when they enact violent missions."[69]

In support of the theory of radicalization, we find that women who were seeking to overcome post-traumatic stress disorder, trauma, and depression were inherently conditioned to turn to radical ideologies to fulfill a sense of self-identity and belonging, while retaining the secrecy of their suicide missions and allegiance to terrorism, proving that they could be *shaheedas* while living in a community of gender inequality. Speckhard's and Akhemdova's study illustrates this phenomenon. Moreover, with the history of female suicide terrorism in Chechnya, Speckhard expands her research to study the first Westernized female terrorist, Muriel Degauque.

Muriel Degauque

This woman became the first "white" or Western female suicide bomber from Europe.[70] Degauque's background consists of a troubled youth growing up in a staunch Catholic religious system. She was a rebellious teenager who experimented with drugs and dropped out of school at the age of 16. Perhaps it was during this time that she experienced depression, turning to drugs as a form of substance abuse.[71] As a teenager, she experienced severe trauma after her brother died in a motorcycle accident. This was the turning point in her life as they had a close relationship. According to Speckhard, who interviewed the neighbors of the family, Degauque's mother had stated that her daughter should have died that day in the accident and not her son, as he had a more meaningful life than her daughter. Based on Speckhard's account, it may be concluded that Degauque experienced depression as a teenager, which followed her during her young adult years, when she sought to find herself.[72]

Degauque's use of drugs and her depression impacted her ability to work routinely at a local bakery store. It was also during this time that she entered into a marriage with a Turkish man, who introduced her to Islam.[73] The family of the Turkish man wanted him to get married in order to obtain Belgian citizenship. Her conversion to Islam, according to Degauque's friends, was apparent when she began wearing the headscarf.

Shortly after the conversion, the marriage ended quickly and Degauque met Isaam Goris, a Belgian born of Moroccan origin. In 2000 the couple married. According to Speckhard, it was at this time that Degauque was introduced to radical Islam. Over the next couple of years, she learned Arabic and began to take on the traditional role of women, wearing the *abaya*, while supporting her husband's extreme belief of how men and women eat separately and abstaining from alcohol.[74] Degauque's mother also grew tired of her daughter preaching radical Islamic ideologies and accepting radical Islamic gender roles. "We told them that we had had enough of them trying to indoctrinate us," states Goris.[75] Goris' belief in radical Islam became evident as the couple not only traveled to the Middle East but there was evidence Goris had executed his suicide mission. Degauque's ability to remain loyal and retain her secret mission came as a complete shock to her mother, who was given the message of her own daughter's suicide operation by Belgian police.[76]

With the case of Degauque, we find a depressed youth who was troubled by her mother's words upon the death of her son. Based on Speckhard's accounts, it can be assumed that Degauque may have been depressed, as she turned to drugs to feel better about herself during her teenage years, a vulnerable time for youth.[77] With her conversion to radical Islam, not only did her behavior change but she followed her husband to Iraq to execute her mission successfully on November 9, 2005. Speckhard states:

> When I look at Muriel Deguauque's psycho-social history and try to reconstruct what happened with her I see again the lethal cocktail of suicide terrorism: a vulnerable individual exposed to a group that is willing and able to equip her with violence; an ideology that met her psychological needs of cleansing her survivor guilt, offering her instant admission to paradise, where she may hope to reunite with her brother, and that gave her courage and social support to carry out the act.[78]

To assess Degauque's acceptance of the Islamic ideology and bridge it with the theory of radicalization, the influence and legitimacy of the jihad ideology played a large part in her ability to become a female martyr. This is not to say that her conversion into Islam influenced her to become a martyr; rather, it was her marriage with Goris, whose radical beliefs influenced her into martyrdom. To reemphasize the radicalization process, Degauque's depression followed her from youth to adulthood. The sense of belonging and comfort lacking at home was found in drugs. Her marriage to Goris established her identity built upon by radical ideologies, a place she felt she was accepted and belonged. She gave up her Western freedoms as a female to be conditioned to die as a martyr, experiencing the gender inequalities of women. She found liberation of her soul in her suicide mission. Degauque's suicide mission is an important narrative in the world of terrorism, as it was the first Western death originating from Europe. This was a successful mission that sent a strong message globally to future jihadis today and tomorrow.

JIHAD TODAY

Jihad today has taken on a deeper role than mere recruitment for soldiers in the military; jihad today has been the fuel for the proliferation of radical Islam. Consistently over time, hard attacks or violent acts that occur among dense populations have become the norm.

Traditionally, bombings of major monuments such as the World Trade Center and the U.S. Embassy in Kenya were and are the common areas where terrorist organizations attack. These are known as hard attacks.[79] Soft attacks are those that occur with random shootings in restaurants or at nightclubs, where large crowds exist. Suicide attacks are also known to occur globally in marketplace squares, cafes, and stores. Such "soft" forms of attack are now trending globally.[80]

Radicalization has become popular with the benefits of technology. Technology has enabled terrorist organizations to increase their efforts with propaganda and recruitment.

Western Female Terrorism and the Islamic State

From Wafa Idris to the Black Widows to Muriel Degauque, we find that their identities were reconditioned by radical jihadi ideologies. All the women experienced some form of depression and trauma in personal dissonance environments. Turning to collective radical ideologies and influences that existed in their societal realms, they were able to accept suicide terrorism. Nevertheless, the trend continues today. Radicalization has become popular with the benefits of technology. Technology has enabled terrorist organizations to increase their efforts with propaganda and recruitment. Several hundred websites live on the Internet today and major online magazines such as *Rumiyah* encourage women to enter the world of terrorism. For example, propaganda with live action music, personal testimonials, and the application of logical fallacies has resulted in influencing the emotions, attitudes, opinions, and behaviors of individuals.[81] Although it is difficult to assess if women are radicalized by simply watching videos and/or believing the content presented, perhaps those who are vulnerable seek allegiance to terrorist organizations in order to fulfill their desire to belong to something. Similarly, Tugwell states, "Propaganda and terrorism are identical insofar as they both seek to influence a mass audience in a way that is intended to benefit the sponsors . . . terror might be seen as a sub-species of propaganda."[82]

Female-specific propaganda is also supported by al Qaeda, which during the time of Bin Laden followed the traditional role of women not fighting in combat. Today, we find that al Qaeda is a strong supporter of female suicide terrorism. According to O'Rourke:

> The August 2004 issue of the online magazine *Al Khansaa*, published by the Arabian Peninsula Women's Information Bureau—which acknowledges ties to Al-Qaeda—stated, 'Woman in the family is a mother, wife, sister and daughter. In society she is an educator, propagator, and preacher of Islam, and a female jihad warrior…When jihad becomes a personal obligation, then the woman is a summoned like a man, and need ask permission neither from her husband nor guardian, because she is obligated, and none need carry out a commandment that everyone must carry out.'[83]

In other words, a woman is to fulfill her obligation as a martyr when summoned. This is a shift in ideology from the traditional belief by Bin Laden, who followed the principles of the Prophet that women were not to fight in combat. It is evident that psychological manipulation by radical Islam has created a spurious role for women when needed to carry out a suicide bombing. Bin Laden's al Qaeda "…refrained from including women in their operations except in supporting roles. The religious and ideological leap (to use female suicide bombers) apparently represents a daunting challenge for Al Qaeda."[84] Repeatedly, in the Qur'an, women are not to be called for battle, but rather support the operations as spouses of soldiers. Al Qaeda in Chechnya held this belief.[29] According to Bloom and Winters, women have traditionally joined terrorist organizations if they have "dishonored" their families in some way.[85] Nevertheless, this is not the case with the Islamic State of Iraq and the Levant (ISIL), formerly known as al Qaeda in Iraq. [Editor's Note: The draft of this article was submitted long before the recent battlefield victories against the Islamic State.]

Although ISIL has attempted to claim it utilizes women as female suicide bombers, there is little evidence to support it. Instead, women, specifically those from Western nations, are recruited heavily to join the organization by asking them to make the *hijrah* or migration to the "caliphate."[86] Propaganda has played an important role in the recruitment of young women in their twenties to make this journey.

In English- and French-language propaganda, women are told that they will have an exciting and fulfilling life in the Caliphate…women are also important disseminators of

propaganda to the outside world—especially young Western women curious about life in the caliphate…these women meet through Twitter, Tumblr, Telegram, and Kik, where they exchange verses of the Quran, ISIL propaganda, statements from radical English-and Arabic-speaking preachers, and news of ISIL's territorial advances. The girls converse using a range of slang and emojis mixed with a handful of Islamic phrases, a reflection of their youth and upbringing.[87] Some of the young women have made the move from North America and Europe to marry soldiers of ISIL based on the promises made via social media. In fact, the real life under ISIL is quite the contrary.

Female recruits are required not only to convert to ISIL's Islam, but also wear the veil so as to hide ammunition and guns beneath their clothing for executing non-Muslims.

Within ISIL, women are a commodity: they are bought, sold, and traded. Leaders worry about defection and the loss of troops, and use women as tools to retain their male foreign fighters. The women help create anchors that ensure men will stay with the cause: a job, a house, a wife and a child…ISIL also ranks its women, and considers foreign women converts to be especially valuable…ISIL foreign fighters actually prefer foreign women and jihadis because they find Syrian women uppity and sexually unaccommodating.[88]

Female recruits are required not only to convert to ISIL's Islam, but also wear the veil so as to hide ammunition and guns beneath their clothing for executing non-Muslims. ISIL's effort to recruit foreign fighters has been successful due to its global expansion tactics through technology and the establishment of a caliphate perceived as the Islamic utopia. The organization's strength and resilience to accept all those who commit soft and hard attacks are able to align with ISIL illegitimately. The point is that, being ISIL's competitor, al Qaeda does not allow just any lone attacker to align with the organization. Al Qaeda has a legitimate process of induction to become a member, as it is an earned right.[89] Also, the women of al Qaeda are asked to join when needed, not lured into terrorism on a fallacy as are the females of ISIL.

Additionally, ISIL's strategic messaging has further resulted in recruitment of foreign fighters. In 2015 Jayne Huckerby reported that approximately 600 women from the West had joined ISIS: "Western female recruits can be drawn by many of the same factors as men: alienation, inequality, marriage, adventure, and pull of the cause."[90] Approximately 700 women have joined from Tunisia. Although propaganda may be a tool to recruit a certain type of personality successfully, to what extent does propaganda succeed with women who are depressed, alienated, and hence join to escape their current environment? Do women seek equality so as to utilize their gender to become the jihadi princesses? Or is self-identity the primary motivator?

According to Peresin, "In terms of self-identification, Muslim women who have joined ISIL and moved to the 'Caliphate' call themselves muhajirat," a term that is considered "honourable value…the same term has been used to specify female suicide bombers." [91] Women are not perceived as the *muhajirat*, unless they are needed for a suicide mission, a politically motivated goal. We find the latter to be true with the soft attacks that recently took place in Paris, France.

CONCLUSION: THE FUTURE PROFILE OF FEMALE TERRORISM

"Shera: Princess of Power" — Power, Romance, and Sexuality

After visiting Paris in summer 2016, I saw that the city is heavily guarded by military men and women carrying heavy artillery and machineguns. Approximately every quarter of a mile, the military is seen guarding the streets. Safety is an understatement. Major tourist attractions, such as the Palace of Versailles, the Eiffel Tower, and the Louvre are under heavy security. The reason for such heavy security is that a high terror alert was issued due to the multiple terror attacks that had taken place in France over the past couple of years.

On November 13, 2015, Hasna Aitboulahcen was labeled as Europe's first female ISIL suicide bomber. She was known as the "cowboy girl."[92] Hasna blew herself up in an apartment in the French suburb of Saint-Denis as police raided the flat in which she was residing, alongside her male cousin. Hasna was a unique individual who rebelled against the Eastern norms of radical Islam. In fact, she was known to dress in Western clothing, depicting a rebellious, non-traditional image of a girl dressed in cute crop tops, jeans, and cowboy hats. As a fearless outspoken soldier, she was fun, sexy, and enjoyed her spirits. She opened herself up to the world by posting images of herself in bubble baths, with skin and body showing. She was known as a jihadi princess who was a "bad" girl, but one who died as a martyr. Can we assume that she is deemed a sexual figure, which every man may desire in a culture where the forbidden fruits of sexuality and lesbianism are repressed? Hasna's personality and habits

supported the preferences desired by ISIL soldiers. Although very little is known about Hasna, her unstable childhood and being forced to grow up in multiple foster homes possibly led her to want to join ISIL and find stability. Perhaps ISIL may propagate Hasna as the new poster girl, deemed to be a powerful untouchable female soldier who is an ideal sexual reward for males who become suicide bombers to attain Paradise. Or perhaps she is the poster girl for future jihadi princesses, who are encouraged to openly portray their sexuality, wear Western clothing, and cast their lesbianism, while fulfilling martyrdom. If so, this may be a shift in the ideal profile of a female suicide bomber, which is a Westernized lesbian *shaheeda*.

Radicalization is a difficult process to assess. Religion and gender inequality are common factors which parallel allegiance to terrorist organizations by female suicide bombers.

Radicalization is a difficult process to assess. Religion and gender inequality are common factors which parallel allegiance to terrorist organizations by female suicide bombers. From Wafa Idris, the Black Widows, and Murial Degauque to Hasna Aitboulachen, depression from a young age to postpartum, have also been additional factors that have contributed to the act of suicide terrorism. Perhaps each woman sought martyrdom as a spurious justification to escape her existence in hopes of attaining personal liberation. Or was it that she sought allegiance to personal liberation? The major takeaway from this article is to understand that a woman who straps C4 to her chest and detonates it in a supermarket may be labeled as a "female suicide bomber," or "terrorist," but there is a very real story behind her life, one that helps us see that she is human and needs help in a world where help is limited due to political, religious, and violent turmoil. She is just a woman who seeks unconditional happiness, love and, more importantly, freedom.

NOTES

[1] Hoffman, B. (2006). *Inside Terrorism.* New York: Columbia University Press.
[2] Hoffman, B. (2006). *Inside Terrorism.* New York: Columbia University Press.
[3] *Obsession: Radical Islam's War Against the West.* Dir. Peter Burton. The Clarion Fund, 2004. DVD.
[4] *Obsession: Radical Islam's War Against the West.* Dir. Peter Burton. The Clarion Fund, 2004. DVD.
[5] *Obsession: Radical Islam's War Against the West.* Dir. Peter Burton. The Clarion Fund, 2004. DVD.
[6] *Obsession: Radical Islam's War Against the West.* Dir. Peter Burton. The Clarion Fund, 2004. DVD.
[7] BBC. (2013). Islam. Retrieved from http://www.bbc.co.uk/religion/religions/islam/.
[8] Borum, R. (2011). "Radicalization into Violent Extremism I: A Review of Social Science Theories." *Journal of Strategic Security* 4(4), 7-36.
[9] Cook, D. (2005). *Understanding Jihad*. Los Angeles: University of California Press.
[10] Cook, D. (2005). *Understanding Jihad*. Los Angeles: University of California Press.
[11] National Institute of Mental Health. (2016). "Postpartum Depression Facts." Retrieved from http://www.nimh.nih.gov/health/publications/postpartum-depression-facts/index.shtml.
[12] *Obsession: Radical Islam's War Against the West.* Dir. Peter Burton. The Clarion Fund, 2004. DVD.
[13] Borum, R. (2011). Radicalization into Violent Extremism I: A Review of Social Science Theories." *Journal of Strategic Security* 4(4), 7-36.
[14] Hoffman, B. (2006). *Inside Terrorism.* New York: Columbia University Press.
[15] National Institute of Mental Health. (2016). "Postpartum Depression Facts." Retrieved from http://www.nimh.nih.gov/health/publications/postpartum-depression-facts/index.shtml.
[16] Postpartum Support International. (2010). "Postpartum Psychosis." Retrieved from http://www.postpartum.net/Get-the-Facts/Postpartum-Psychosis.aspx.
[17] Postpartum Support International. (2010). "Postpartum Psychosis." Retrieved from http://www.postpartum.net/Get-the-Facts/Postpartum-Psychosis.aspx.
[18] Postpartum Support International. (2010). "Postpartum Psychosis." Retrieved from http://www.postpartum.net/Get-the-Facts/Postpartum-Psychosis.aspx.
[19] Postpartum Support International. (2010). "Postpartum Psychosis." Retrieved from http://www.postpartum.net/Get-the-Facts/Postpartum-Psychosis.aspx.
[20] McAuliffe, Jane D. (2006). *The Cambridge Companion to the Qur'an*. New York:
Cambridge University Press.
[21] Dukes, K. (2011). *Qur'an*. Retrieved from http://corpus.quran.com/translation.jsp?chapter=4&verse=34.
[22] Dukes, K. (2011). *Qur'an*. Retrieved from http://corpus.quran.com/translation.jsp?chapter=4&verse=34.
[23] Berko, A. & Erez, E. (2006). Women in Terrorism: A Palestinian Feminist Revolution or Gender Oppression? Retrieved from www.ict.org.il/Articles/tabi/66/Articlsid/234/currentpage/8/Default.aspx.
[24] Skaine, R. (2006). *Female Suicide Bombers*. McFarland & Company, Inc., Publishers.
[25] Skaine, R. (2006). *Female Suicide Bombers*. McFarland & Company, Inc., Publishers.
[26] Bloom, M., & Winter, C. (2015). Women of ISIL. Retrieved from http://www.politico.eu/article/the-women-of-isil-female-suicide-bomber-terrorism/.
[27] Bloom, M., & Winter, C. (2015). Women of ISIL. Retrieved from http://www.politico.eu/article/the-women-of-isil-female-suicide-bomber-terrorism/.

[28] Bloom, M., & Winter, C. (2015). Women of ISIL. Retrieved from http://www.politico.eu/article/the-women-of-isil-female-suicide-bomber-terrorism/.
[29] Skaine, R. (2006). *Female Suicide Bombers*. McFarland & Company, Inc., Publishers.
[30] Benslama, F. (2009). *Psychoanalysis and the Challenge of Islam*. University of Minnesota.
[31] Benslama, F. (2009). *Psychoanalysis and the Challenge of Islam*. University of Minnesota.
[32] Benslama, F. (2009). *Psychoanalysis and the Challenge of Islam*. University of Minnesota.
[33] Berko, A. (2009). *Path to Paradise: The Inner World of Suicide Bombers and Their Dispatchers*. Potomac Books, Inc.
[34] Barlas, A. (2009). *Believing Women in Islam: Unreading Patriarchal Interpretations of the Qur'an*.
Austin: University of Texas Press.
[35] Barlas, A. (2009). *Believing Women in Islam: Unreading Patriarchal Interpretations of the Qur'an*. Austin: University of Texas Press.
[36] Benslama,F. (2009). *Psychoanalysis and the Challenge of Islam*. University of Minnesota.
[37] Benslama,F. (2009). *Psychoanalysis and the Challenge of Islam*. University of Minnesota.
[38] Eli, B. (2009). *Radical, religious, and violent: The new economics of terrorism*.
Cambridge, MA: Massachusetts Institute of Technology.
[39] Eli, B. (2009). *Radical, religious, and violent: The new economics of terrorism*. Cambridge. MA: Massachusetts Institute of Technology.
[40] *Jihadi Terrorists, Mass Hostage Takers, Suicide Bombers & Martyrs*. McLean, VA: Advances Press.
[41] Speckhard, A. (2012). *Talking to Terrorists: Understanding the Psycho-Social Motivations of Militant*
Jihadi Terrorists, Mass Hostage Takers, Suicide Bombers & Martyrs. McLean, VA: Advances Press.
[42] Speckhard, A. (2012). *Talking to Terrorists: Understanding the Psycho-Social Motivations of Militant*
Jihadi Terrorists, Mass Hostage Takers, Suicide Bombers & Martyrs. McLean, VA: Advances Press.
[43] Berko, A. (2009). *Path to Paradise: The Inner World of Suicide Bombers and Their Dispatchers*. Potomac Books, Inc.
[44] University of Twente. (2013) *Groupthink*. Retrieved from https://www.utwente.nl/cw/theorieenoverzicht/Theory%20Clusters/Organizational%20Communication/goupthink/.
[45] Botha, A. (2015). Radicalisation to Terrorism in Kenya and Uganda: A Political Socialisation Perspective. *Perspectives on Terrorism* 9(5), 2-14.
[46] University of Twente. (2017). Psycho-Linguistic Theory. Retrieved from https://www.utwente.nl/cw/theorieenoverzicht/Theory%20Clusters/Language%20Theory%20and%20Linguistics/Psycho-Linguistic_theory/.
[47] University of Twente. (2017). Model of Text Comprehension. Retrieved from https://www.utwente.nl/cw/theorieenoverzicht/Levels%20of%20theories/micro/Model_text_comprehension/.
[48] University of Twente. (2017). Psycho-Linguistic Theory. Retrieved from https://www.utwente.nl/cw/theorieenoverzicht/Theory%20Clusters/Language%20Theory%20and%20Linguistics/Psycho-Linguistic_theory/.
[49] Fletcher, H. (2008). Al-Aqsa Martyrs Brigade. Retrieved from http://www.cfr.org/israel/al-aqsamartyrs brigade/p9127.
[50] Fletcher, H. (2008). Al-Aqsa Martyrs Brigade. Retrieved from http://www.cfr.org/israel/al-aqsamartyrs brigade/p9127.
[51] Speckhard, A. (2012). Talking to Terrorists: Understanding the Psycho-Social Motivations of Militant.
[52] Speckhard, A. (2012). Talking to Terrorists: Understanding the Psycho-Social Motivations of Militant.
[53] Speckhard, A. (2012). Talking to Terrorists: Understanding the Psycho-Social Motivations of Militant.
[54] O'Rouke, L.A. (2009). What's Special about Female Suicide Terrorism? *Security Studies* 18, 681-718.
[55] Speckhard, A., & Akhmedova, K. (2006). Black Widows: The Chechen Female Suicide Terrorists. Retrieved from http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDQQFjAB&url=http%3A%2F%2Fkms1.isn.ethz.ch%2Fserviceengine%2FFiles%2FISN%2F91164%2Fichaptersection_singledocument%2Fe4d7c6af-4921-4a41-82ab-5a379e34396b%2Fen%2F07_Black%2BWidows_The%2BChechen%2BFemale%2BSuicide%2BTerrorists.pdf&ei=3htPUaCSIpKm8ATEuoCIBg&usg=AFQjCNF2vEiIsjVxiGFNDVa8curvl02Qog&bvm=bv.44158598,d.eWU.
[56] Speckhard, A., & Akhmedova, K. (2006). Black Widows: The Chechen Female Suicide Terrorists. Retrieved from http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDQQFjAB&url=http%3A%2F%2Fkms1.isn.ethz.ch%2Fserviceengine%2FFiles%2FISN%2F91164%2Fichaptersection_singledocument%2Fe4d7c6af-4921-4a41-82ab-5a379e34396b%2Fen%2F07_Black%2BWidows_The%2BChechen%2BFemale%2BSuicide%2BTerrorists.pdf&ei=3htPUaCSIpKm8ATEuoCIBg&usg=AFQjCNF2vEiIsjVxiGFNDVa8curvl02Qog&bvm=bv.44158598,d.eWU.
[57] Speckhard, A. & Akhmedova, K. (2006). Black Widows: The Chechen Female Suicide Terrorists. Retrieved from http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDQQFjAB&url=http%3A%2F%2Fkms1.isn.ethz.ch%2Fserviceengine%2FFiles%2FISN%2F91164%2Fichaptersection_singledocument%2Fe4d7c6af-4921-4a41-82ab-5a379e34396b%2Fen%2F07_Black%2BWidows_The%2BChechen%2BFemale%2BSuicide%2BTerrorists.pdf&ei=3htPUaCSIpKm8ATEuoCIBg&usg=AFQjCNF2vEiIsjVxiGFNDVa8curvl02Qog&bvm=bv.44158598,d.eWU.
[58] Billingsley, D. (2013). *Fangs of the Lone Wolf: Chechen Tactics in the Russian-Chechen War 1994-2009*. USA: Helion and Company.
[59] Billingsley, D. (2013). *Fangs of the Lone Wolf: Chechen Tactics in the Russian-Chechen War 1994-2009*. USA: Helion and Company.
[60] Billingsley, D. (2013). *Fangs of the Lone Wolf: Chechen Tactics in the Russian-Chechen War 1994-2009*. USA: Helion and Company.
[61] Billingsley, D. (2013). *Fangs of the Lone Wolf: Chechen Tactics in the Russian-Chechen War 1994-2009*. USA: Helion and Company.

[62] Billingsley, D. (2013). *Fangs of the Lone Wolf: Chechen Tactics in the Russian-Chechen War 1994-2009.* USA: Helion and Company.
[63] Billingsley, D. (2013). *Fangs of the Lone Wolf: Chechen Tactics in the Russian-Chechen War 1994-2009.* USA: Helion and Company.
[64] Vidino, L. (2005). "How Chechnya Became a Breeding Ground for Terror". *Middle East Quarterly.* Summer, p. 57-66.
[65] Vidino, L. (2005). "How Chechnya Became a Breeding Ground for Terror". *Middle East Quarterly.* Summer, p. 57-66.
[66] Vidino, L. (2005). "How Chechnya Became a Breeding Ground for Terror". *Middle East Quarterly.* Summer, p. 57-66.
[67] Schaefer, R. (2011). *The Insurgency in Chechnya and the North Caucasus: From Gazavat to Jihad.* USA: Praeger Security International.
[68] O'Rouke, L.A. (2009). What's Special about Female Suicide Terrorism? *Security Studies*, 18, 681-718.
[69] O'Rouke, L.A. (2009). What's Special about Female Suicide Terrorism? *Security Studies*, 18, 681-718.
[70] Speckhard, A. (2012). Talking to Terrorists: Understanding the Psycho-Social Motivations of Militant.
[71] Speckhard, A. (2012). Talking to Terrorists: Understanding the Psycho-Social Motivations of Militant.
[72] Speckhard, A. (2012). Talking to Terrorists: Understanding the Psycho-Social Motivations of Militant.
[73] Speckhard, A. (2012). Talking to Terrorists: Understanding the Psycho-Social Motivations of Militant.
[74] Speckhard, A. (2012). Talking to Terrorists: Understanding the Psycho-Social Motivations of Militant.
[75] Speckhard, A. (2012). Talking to Terrorists: Understanding the Psycho-Social Motivations of Militant.
[76] Speckhard, A. (2012). Talking to Terrorists: Understanding the Psycho-Social Motivations of Militant.
[77] Speckhard, A. (2012). Talking to Terrorists: Understanding the Psycho-Social Motivations of Militant.
[78] Speckhard, A. (2012). Talking to Terrorists: Understanding the Psycho-Social Motivations of Militant.
[79] Walt, S. (2015). The Soft Logic of Soft Attacks. Retrieved from, http://foreignpolicy.com/2015/08/28/the-soft-logic-of-soft-targets-france-train-attack-security/.
[80] Walt, S. (2015). The Soft Logic of Soft Attacks. Retrieved from http://foreignpolicy.com/2015/08/28/the-soft-logic-of-soft-targets-france-train-attack-security/.
[80] Tugwell, M. (1986). Terrorism and Propaganda: Problem and Response. Retrieved from https://journals.lib.unb.ca/index.php/JCS/article/viewFile/14713/15782.
[81] Tugwell, M. (1986). Terrorism and Propaganda: Problem and Response. Retrieved from https://journals.lib.unb.ca/index.php/JCS/article/viewFile/14713/15782.
[82] Tugwell, M. (1986). Terrorism and Propaganda: Problem and Response. Retrieved from https://journals.lib.unb.ca/index.php/JCS/article/viewFile/14713/15782.
[83] O'Rouke, L.A. (2009). What's Special about Female Suicide Terrorism? *Security Studies*, 18, 681-718.
[84] Zedalis, D. (2004). Female Suicide Bombers. Retrieved from http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB408.pdf.
[85] Bloom, M., & Winter, C. (2015). Women of ISIL. Retrieved from http://www.politico.eu/article/the-women-of-isil-female-suicide-bomber-terrorism/.
[86] Peresin, A. (2015). Fatal Attraction: Western Muslimas and ISIS. Retrieved from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/427/html.
[87] Bloom, M., & Winter, C. (2015). Women of ISIL. Retrieved from http://www.politico.eu/article/the-women-of-isil-female-suicide-bomber-terrorism/.
[88] Bloom, M., & Winter, C. (2015). Women of ISIL. Retrieved from http://www.politico.eu/article/the-women-of-isil-female-suicide-bomber-terrorism/.
[89] Peresin, A. (2015). Fatal Attraction: Western Muslimas and ISIS. Retrieved from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/427/html.
[90] Huckerby, J.(2015). Why Women Join ISIS. Retrieved from, http://time.com/4138377/women-in-isis/
[91] Peresin, A. (2015). Fatal Attraction: Western Muslimas and ISIS. Retrieved from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/427/html.
[92] TheTelegraph.com. (2015). "Paris attacks: female suicide bomber Hasna Aitboulahcen liked wearing cowboy hats but joined an Islamic State terror cell." Retrieved from http://www.telegraph.co.uk/news/worldnews/europe/france/12004720/Paris-attacks-female-suicide-bomber-shouted-Help-me-Help-me-to-police-during-Saint-Denis-raid.html.

[Author's Note: My deepest gratitude to both Mr. David Moore, MSSI, U.S. Department of Defense, and Dr. William Spracher, EdD, National Intelligence University, for their expertise and generous commitment to sharpening my work. David, I am indebted to your copious assistance and guidance in making this commentary come to life. Bill, a special thanks for your patience, support, and willingness to publish this article.]

Dr. Bina Patel earned her doctorate in Conflict Resolution and Peacekeeping Analysis in 2014 and a master's in International Business in 2007, both from Nova Southeastern University. Her undergraduate degree in Business Administration, with a minor in Spanish, was earned in 2004 from the University of Florida. Currently, Dr. Patel continues to conduct research in the area of Islamic fundamentalism with a focus on gender inequality in war-torn countries. She also enjoys studying human psychology and behavior in countering violent extremism. Dr. Patel published Depicting Female Suicide Bombers: Understanding the Radicalization Process *in May 2017. The in-depth content depicts the role of women in suicide terrorism in vulnerable climes. Currently she serves as Organizational Ombudsman for the National Ground Intelligence Center in Charlottesville, VA.*

Expanding Integrated Coalition and NGO ISR to Better Support HA/DR Operations

by Lt Col (USAF) Jesse Winkels

SUMMARY

U.S. military operations are increasingly coalition in nature and intelligence sharing is a force multiplier.[1] Traditional intelligence-sharing methodologies have limitations, but many of those challenges can be overcome by integrating coalition partners and non-governmental organizations (NGOs) into the processing, exploitation, and dissemination (PED) of intelligence, surveillance, and reconnaissance (ISR) operations. United States Air Forces Europe/Air Forces Africa (USAFE/AFAFRICA) developed a system that enables near-real-time (NRT), combined U.S.-partner nation PED of full motion video (FMV). Other combatant commands (CCMDs) would benefit from similar systems, and there are several ways CCMDs can field this capability. Humanitarian assistance/disaster relief (HA/DR) operations, in particular, would realize increased effectiveness if integrated ISR systems were used to better understand the operational environment (OE).

THE PROBLEM

In 2010 a 7.0-magnitude earthquake struck Haiti, killing 230,000, injuring 300,000, and leaving nearly one million homeless and 45,000 American citizens stranded.[2] Much of Haiti's infrastructure was destroyed; hospitals, roads, airports, bridges, and seaports were rendered inoperable. The President of Haiti declared a national emergency and requested immediate assistance from the United States. President Obama declared humanitarian operations in Haiti his number one priority. U.S. military forces were assigned to Joint Task Force (JTF) Haiti and started arriving within days, as did elements from nearly 60 nations and hundreds of NGOs.

In 2010 a 7.0-magnitude earthquake struck Haiti, killing 230,000, injuring 300,000, and leaving nearly one million homeless and 45,000 American citizens stranded.

Relief forces experienced difficulties due to a lack of understanding the OE. According to Joint Publication 3-29, *Foreign Humanitarian Assistance*, understanding the OE is a key task in HA/DR operations.[3] In Haiti several factors impaired JTF leadership decision-making. Host nation officials lacked an accurate assessment of infrastructure damage, could not quickly determine which areas were in most urgent need of aid, and were forced to make operational decisions based on assumptions. According to the USSOUTHCOM Chief of Staff, "Many of the early assessments were simply guesses… SOUTHCOM guessed at what would be needed and sent them forward without ever being requested by the lead agency."[4] Although relief efforts saved countless lives, a delayed understanding of the OE impaired efforts to acquire situational awareness and distribute supplies to the areas most needed.

One Operation UNIFIED RESPONSE case study states the most valuable tool to determine infrastructure damage was Google Earth…which was not updated until day five of relief efforts.

JTF leadership eventually obtained a clear understanding of the OE, but only after weeks of working through intelligence-sharing protocols. To illustrate the difficulties and delay, one Operation UNIFIED RESPONSE case study states the most valuable tool to determine infrastructure damage was Google Earth…which was not updated until day five of relief efforts.[5] In spite of SOUTHCOM Headquarters designating all materials relating to Operation UNIFIED RESPONSE as UNCLASSIFIED, it was not until the end of week two that "much needed FMV [was disseminated] to forces on the ground to monitor food distribution efforts, indigenously displaced personnel movement, and respond to any dynamic tasking directed by the JTF-Haiti commander."[6] Future HA/DR efforts could be improved if host nation personnel and NGOs are involved in the PED of real-time FMV before disasters occur. Fortunately, a viable solution already exists within the U.S. Air Force (USAF).

THE SOLUTION

USAFE/AFAFRICA created a stand-alone Distributed Common Ground Station (DCGS)-like system called the European Partnership Integration Enterprise (EPIE) to enable coalition PED of U.S. and partner nation FMV. This was accomplished through a cooperative effort among the 693rd ISR Group for systems expertise, USAFE/AFAFRICA staff for partner nation engagement, and base communications personnel for network expertise. EPIE is comprised of a facility which receives FMV feeds, analyst workstations that can view those feeds, and a bilateral or multilateral network called the Battlefield Information Collection Exploitation System (BICES) to disseminate information to coalition customers. EPIE achieved initial operating capability in 2013, and in 2015 the system supported 49 unmanned aerial vehicle (UAV) bilateral operations in support of two CCMDs.[7]

Integrating coalition partners into the PED of ISR operations is directly in line with Department of Defense (DoD) and USAF strategic guidance.

USAFE/AFAFRICA realized several benefits from integrating coalition partners into the PED of FMV during multinational operations. For example, integrated ISR exposed partner nation analysts to U.S. ISR tactics, techniques, and procedures (TTPs), gave U.S. analysts experience working in coalition environments, and informed partners of options for future foreign military sales.[8] Another benefit of integrated ISR is that it leverages the expertise of coalition partners who often possess a deeper understanding of their country's OE. For example, consider the value of adding host nation personnel and interagency partners to a FMV PED cell tasked with evaluating measures of effectiveness during an HA/DR operation. While a U.S. analyst relatively unfamiliar with the OE would be able to report basic damage levels and activity observed, the coalition partner could offer a more complete assessment to include current versus average crowd sizes at markets, insights into key roads or bridges upon which the population relies, and a working knowledge of the OE required to recognize unusual absences of activity that may signal current relief efforts are not sufficient. In addition, partner nations may be more willing to allow overflight of U.S. ISR platforms knowing their analysts are involved in the PED process. While this may not be a factor when partner nations are requesting U.S. assistance during HA/DR situations, integrated PED can be used during exercises in peacetime operations and leveraged throughout the range of military operations.

ALIGNMENT WITH DEPARTMENT OF DEFENSE AND USAF STRATEGY

Integrating coalition partners into the PED of ISR operations is directly in line with Department of Defense (DoD) and USAF strategic guidance. The 2015 National Military Strategy (NMS) places strong emphasis on preserving alliances, expanding partnerships, and conducting training exercises, security cooperation activities, and military-to-military engagements.[9] Each of these mission areas would benefit from, or be directly enabled by, the proliferation of systems that allow integrated ISR. Additionally, this DoD-level guidance underscores how disaster relief missions are "essential to maintaining regional peace."[10] The NMS not only states the importance of working closely with international and interagency partners; it directly tasks components to do so through "integrated joint and partner ISR."[11]

Integrating coalition partners into the PED of ISR operations is also aligned with USAF strategic guidance. For example, the 2015 USAF Future Operating Concept details how ISR is the "foundation upon which every joint, interagency, and coalition operation achieves success."[12] While this statement can be viewed as a testament to the value of ISR, it also underscores how military operations must increasingly strive to include interagency and coalition partners. General Mark Welsh, former USAF Chief of Staff, shared his vision for integrated ISR for 2035 by stating, "Collected data will be integrated in an open, adaptive information construct unburdened by unnecessary classification barriers."[13] Systems similar to USAFE/AFAFRICA's EPIE offer the potential to integrate coalition and interagency professionals into an environment USAF senior leaders envision. However, it is important to understand CCMD requirements to determine if integrated ISR systems would be valuable in other areas of responsibility (AORs) before exploring solutions.

COMBATANT COMMAND REQUIREMENTS

An evaluation of CCMD Posture Statements is useful in identifying requirements for integrated ISR capacity, to include the prevalence of HA/DR operations and insight into other mission areas in which EPIE-like systems could be used. Because U.S. Africa Command and U.S. European Command are already supported by USAFE/AFAFRICA's EPIE system, U.S. Southern Command (USSOUTHCOM) and U.S. Pacific Command (USPACOM) Posture Statements will be reviewed in detail. These CCMDs, in particular, support numerous HA/DR events annually and explicitly focus on

bolstering information sharing and building partner nation capacity missions. Of note, USPACOM is collocated with a DCGS having the expertise available to create an EPIE-like integrated ISR PED capability if directed.

USSOUTHCOM and USPACOM support numerous HA/DR events annually and explicitly focus on bolstering information sharing and building partner nation capacity missions.

USSOUTHCOM states that, no matter the mission set, "**building partner capacity** [bolded for emphasis in CCMD Posture Statement] is the cornerstone of everything we do."[14] These efforts are designed to "build and nurture committed and capable partners who can control their borders and respond to natural and man-made disasters...which generates an extended and layered defense of the US homeland."[15] Integrated ISR operations offer the capacity to advance each of these mission sets through leveraging coalition partners' understanding of the OE. Coupling U.S. technology and PED TTPs with host nation and NGO understanding of the OE would offer a powerful combination for USSOUTHCOM's priority mission sets. Additionally, USSOUTHCOM participates in a robust set of multinational exercises through its State Partnership Program. These exercises offer the opportunity to introduce integrated ISR to 19 nations in the AOR and further USSOUTHCOM's goal of building a strong inter-American system of persistent defense cooperation.[16]

USPACOM also offers strong potential to leverage integrated ISR and advance its priority mission sets. The USPACOM Posture Statement aligns priorities with the four elements of former Secretary of Defense Ash Carter's Asia-Pacific Rebalance strategy: (1) invest in future capabilities relevant to challenges in the Asia-Pacific; (2) field the right numbers of existing capabilities; (3) adapt our regional force posture; and (4) reinforce allies and partnerships.[17] The USPACOM Commander, Admiral Harry Harris, describes the USPACOM AOR as "the world's most disaster-prone region, experiencing over 2,700 disasters that affected nearly 1.6 billion people in the past decade alone."[18] USPACOM has realized increased access through its response to natural disasters in the region and, because natural disasters are so prevalent in the AOR, created the Center for Excellence for Disaster Management (CFE-DM) to "increase regional governments' readiness to respond to natural disasters by developing lessons learned and sharing best practices."[19] Due to the prevalence of natural disasters in USPACOM's AOR, integrated ISR may prove invaluable in reinforcing allies and partner nations. Additionally, USPACOM's stated intent may signal a willingness to invest in developing an integrated ISR capability to better support the CFE-DM.

WAYS TO EXPAND INTEGRATED ISR CAPABILITIES

There are several ways the USAF can expand its capacity to benefit from integrated ISR operations. These approaches include expanding the USAFEAFAFRICA model to active duty DCGS sites that support worldwide operations, expanding the same model to DCGS sites collocated with supported CCMD headquarters, expanding the USAFE/AFAFRICA model to USAF Reserve DCGS sites, and developing deployable systems in support of Joint Task Forces. Each approach offers unique advantages and disadvantages, and a universal approach may not be ideal for both CCMDs.

Expanding the USAFE/AFAFRICA EPIE model to active duty DCGS sites is one viable way of enhancing the USAF's integrated ISR approach to better support USPACOM and USSOUTHCOM. DCGS-1, at Joint Base Langley-Eustis, VA, and DCGS-2, at Beale Air Force Base, CA, are the two main DCGS sites that conduct round-the-clock PED of worldwide ISR operations. These sites possess the knowledge required to build and maintain a stand-alone EPIE-like system. Additionally, DCGS 1 and DCGS 2 analysts could be assigned to an integrated ISR cell to support short-notice HA/DR missions. However, this option presents challenges as well. For example, to best enable integrated ISR support to HA/DR operations, coalition and NGO participants would need to travel to Virginia or California to participate. This challenge could undermine the effectiveness of integrated operations if coalition partners experience delays entering the U.S., which could occur due to partner nation infrastructure damage precluding flights to the U.S. or delays incurred due to the U.S. visa process. Therefore, this course of action would be rather straightforward to implement, but difficult to execute in time-sensitive situations.

Another potential means of expanding integrated ISR is by developing and maintaining EPIE-like capabilities in facilities collocated with USSOUTHCOM and USPACOM Headquarters in Florida and Hawaii. One benefit of this option is that CCMD leadership and their planning teams, by virtue of planners being collocated with the integrated ISR facility, would be more likely to advocate for integrated operations and include the capability into their planning efforts. Additionally, this option provides the benefit of access to coalition liaisons prepositioned within CCMD staffs in the event of an HA/DR operation.

These liaisons could quickly apply their knowledge of the OE to better HA/DR ISR support. However, not all coalition partners are represented and many of the delays referenced above may be encountered. Additionally, this option may prove appropriate for USPACOM as it is collocated with a DCGS site in Hawaii, while the same is not true for USSOUTHCOM in Miami, FL. Therefore, this option has unique advantages and disadvantages which CCMD planning staffs should consider while expanding integrated ISR capabilities.

Expanding integrated ISR operations to vulnerable Guard and Reserve bases would increase their relevance and potentially protect these sites from closure.

A third way the USAF can expand integrated ISR operations is by leveraging Guard or Reserve DCGS sites. The DCGS enterprise consists of 22 Guard or Reserve sites that provide "varying levels of capability and capacity to support the intelligence needs of the warfighter."[20] Some of these sites offer the systems and analytical expertise of active duty DCGS sites, but only use a portion of their operational capability on a day-to-day basis. Therefore, these sites possess the potential to expand operations to host coalition and NGO partners. With the addition of a BICES network, as leveraged in USAFE/AFAFRICA's EPIE system, these sites could operate at the UNCLASSIFIED level and bypass information-sharing obstacles involved with bilateral and multilateral operations. Another advantage of this option is that it expands the mission sets of Guard and Reserve installations that are vulnerable to Base Realignment and Closure (BRAC) actions. Expanding integrated ISR operations to vulnerable Guard and Reserve bases would increase their relevance and potentially protect these sites from closure. However, this option contains the same challenges associated with locating coalition and NGO partners with main DCGS sites.

A fourth and radically different way the USAF can expand integrated ISR operations is through developing deployable EPIE-like systems. These deployable systems could be individually tailored to support unique CCMD requirements. For example, a small-scale system could possess limited capacity (two to four work stations), but offer the advantage of operating as a palletized system, rapidly deployable with analysts and systems configuration specialists, and sustainable for short-duration multinational operations. CCMDs could also task supporting USAF Major Commands to develop larger, yet still deployable, systems similar to the Contingency Airborne Reconnaissance System (CARS) the USAF used in the early 1990s. These systems would need to be smaller than the CARS, which took several C-17s to deploy. For example, a deployable system with eight to ten work stations could be an ideal solution to fulfill CCMD requirements. This capability would not be as responsive as a rapidly deployable palletized system, but it would offer additional work stations to accommodate a full complement of coalition and NGO partners.

Another deployable system which offers the potential to expand integrated ISR operations could draw lessons learned from the U.S. Army's DCGS-Army system. The Army's system routes signals received from truck-mounted antennas to PED workstations located in tents.[21] Each of these deployable options would offer JTF commanders flexibility to establish coalition and NGO ISR PED centers in-country at the location which best meets their mission requirements. Additionally, this capability could be tasked via operations order to rapidly deploy if host nation infrastructure can support Air Mobility Command (AMC) transport aircraft. The reliance upon AMC assets, however, is a limitation of this option, as is the conditional use of host nation airfields. These airfields, as experience has shown, may be inoperable based on the severity of the humanitarian disaster or being clogged with relief supplies.

Integrated SIGINT PED centers could mitigate U.S. linguist shortfalls in low-density/high-demand languages by utilizing native speakers who are fluent in the host nation language and dialects.

ADDITIONAL RESEARCH AREAS

This project's timeline did not allow for the extensive research required to explore all integrated ISR solutions. The following should be evaluated in follow-on ISR research projects or by major command (MAJCOM in the USAF) or CCMD planning staffs:

(1) Integrated Signals Intelligence (SIGINT) PED centers to pair coalition language skills with advanced U.S. SIGINT collection technologies. Integrated SIGINT PED centers could mitigate U.S. linguist shortfalls in low-density/high-demand languages by utilizing native speakers who are fluent in the host nation language and dialects.

(2) Security risks involved with expanding integrated ISR operations. While coalition operations offer numerous advantages FOR U.S. military operations, integrating coalition and NGO partners into ISR PED cells may create security vulnerabilities.

(3) Matching MQ-1Bs with deployable integrated ISR systems to showcase FMV capabilities of the MQ-1B to partner nations lacking FMV platforms. This effort could inform partner nations seeking ISR solutions of a low-cost platform the USAF is planning to divest itself of in the next two fiscal years.

(4) The use of integrated ISR operations to overcome host nation reluctance to allow U.S. overflight of sovereign territory. While some nations are leery of allowing overflight of U.S. ISR platforms, integrating host nation analysts into integrated ISR PED cells may overcome this obstacle.

CONCLUSION

The proliferation of integrated ISR capabilities would offer a number of advantages to Combatant Command and JTF Commanders. Expanding integrated ISR PED systems is in accordance with the NMS and USAF Future Operating Concept, and the USPACOM and USSOUTHCOM Posture Statements contain requirements for this initiative. HA/DR operations would be well served to leverage the OE expertise of host nation and NGO staffs, but this capability could also improve other coalition missions. While this initiative could incur increased security risks, the USAF must recognize the benefits of multilateral operations and pursue the full potential of integrated ISR operations.

NOTES

[1] Chairman, Joint Chiefs of Staff. (2015). *National Military Strategy of the United States of America 2015*. Washington, DC, 8.
[2] DiOrio, D.R. (2010). Operation Unified Response – Haiti Earthquake 2010 (Case Study). Joint Forces Staff College, 1.
[3] Joint Chiefs of Staff, United States. *Foreign Humanitarian Assistance*. Washington, DC: Joint Chiefs of Staff, 2009, IV-5.
[4] DiOrio, D.R. (2010). Operation Unified Response – Haiti Earthquake 2010 (Case Study). Joint Forces Staff College Study, 11.
[5] Ibid., 14.
[6] Ibid., 14.
[7] USAFE/AFAFRICA Senior Intelligence Officer briefing, September 2015, slide 2.
[8] USAFE/AFAFRICA SIO Briefing, slide 5.
[9] *National Military Strategy 2015*, 9.
[10] Ibid., 10.
[11] Ibid., 10.
[12] Welsh, M.A. (2015). The USAF Future Operating Concept: A View into the Air Force in 2035, September 2015, 23.
[13] Ibid., 9.
[14] Tidd, K.W. (2016). Posture Statement of Admiral Kurt W. Tidd, Commander, U.S. Southern Command, 10 March 2016, 8.
[15] Ibid., 8.
[16] Ibid., 14.
[17] Harris, H.B. (2016). Statement of Admiral Harry B. Harris, Jr., U.S. Navy Commander, U.S. Pacific Command Before the Senate Armed Services Committee on U.S. Pacific Command Posture, 23 February 2016, 1.
[18] Ibid., 2.
[19] Ibid., 7.
[20] United States Air Force (2015). Air Force Distributed Common Ground System. Retrieved from: http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104525/air-force-distributed-common-ground-system.aspx.
[21] General Dynamics (2016). DCGS-A: The Intelligence Analyst's Weapon of Choice. Retrieved from: https://gdmissionsystems.com/c4isr/dcgs-a-tactical-ground-station/.

[Editor's Note: This article is based on an academic paper which earned the author the National Military Intelligence Association Writing Award for 2017 at the Air Command and Staff College, Maxwell Air Force Base, AL.]

Lieutenant Colonel (USAF) Jesse Winkels is a career intelligence officer assigned to Special Operations Command-Africa in Stuttgart, Germany. He has held multiple ISR-focused assignments to include airborne operations on the RC-135V/W RIVET JOINT in support of USCENTCOM and USSOUTHCOM, ISR Operations Branch Chief at U.S. Air Forces Europe and Africa, and his current position as Deputy Chief of Intelligence Operations at Special Operations Command-Africa. Jesse has been a strong proponent of integrating coalition partners into ISR operations since witnessing its potential in a deployed location and through his involvement in bringing the European Partnership Integration Enterprise (EPIE) to its initial operating capability. He is a 2017 graduate of the U.S. Air Command and Staff College, holds a master's degree in Management from the University of Phoenix, and earned a BS from Marion College in Fond du Lac, WI.

U.S. Intelligence and Cross-Strait Relations: Intelligence Failures and U.S. Policy Toward the "Two Chinas"

by Alex Herkert

After years of civil war, Mao Zedong and the Chinese communists forced the nationalist Republic of China government led by Chiang Kai-shek to flee to the island of Taiwan across the strait from the mainland. The United States, unwilling to acknowledge the communist victory, refused to engage in diplomatic relations with the newly established People's Republic of China (PRC) in Beijing, and instead recognized Taipei as the true government of China. The United States maintained no form of diplomatic contact with mainland China, the world's most populous nation, for the next three decades. It was not until 1979 that Washington shifted diplomatic representation to Beijing, closing the embassy in Taipei and altering the status quo in the Asia-Pacific region. The rapprochement with China was accomplished by Presidential initiative taken during the Nixon and Carter administrations, as traditional diplomatic and intelligence efforts had failed to make progress on the issue of cross-strait relations.

Intelligence analysts and diplomats failed to assess realistic scenarios, operated on outdated assumptions, and suffered from groupthink mentality that prevented creative solutions to Sino-American problems. Almost four decades later, Beijing remains the sole Chinese diplomatic entity and Taipei operates as a quasi-official U.S. partner. However, new leadership in both Taiwan and the United States, coupled with an increasingly hawkish mainland, may force the status quo to be re-examined in the near future. Learning from the past, the Intelligence Community must think beyond the confines of traditional diplomacy, lest the United States once again fail to act strategically toward China.

BACKGROUND OF CHINA AND TAIWAN

Following millennia of dynastic rule, the Qing Dynasty fell in 1911 to Sun Yat-sen and the newly founded Republic of China (ROC), the first attempt at republican rule in China. Sun and his successors were unable to unify disparate Chinese provinces under cohesive leadership, and by 1927 the country had become embroiled in a civil war between forces loyal to the ROC government and those loyal to the newly founded Chinese Communist Party (CCP).[1] The United States, fearful of the Soviet-backed communists, delivered aid and military assistance to the ROC forces now under Generalissimo Chiang Kai-shek, despite his inability to draw support from an impoverished and starving population. Undeterred, the communists' new leader, Mao Zedong, led his followers through the 1940s, and continued to win territory and critical cities until the remaining ROC forces were forced to flee to Taiwan in 1949. Due to a strong pro-ROC lobby in the United States, coupled with inaccurate reporting of the successes of Chiang by the likes of Henry Luce, founder of *Time* magazine (the Chiangs appeared on the cover of *Time* 11 times between 1927 and 1955), the loss by the nationalists caught U.S. leadership and the general public entirely by surprise.[2]

Taiwan was ruled as an authoritarian dictatorship by Chiang Kai-shek and maintained government departments for each Chinese province.

The ROC quickly subjugated the native Taiwanese and recreated their government on the island, biding time and planning the eventual takeover of the mainland. Both the PRC in control on the mainland and the ROC on Taiwan considered themselves to be the true inheritors of Sun Yat-sen's government, and the only legitimate representative of the Chinese people.[3] Taiwan was ruled as an authoritarian dictatorship by Chiang Kai-shek and maintained government departments for each Chinese province.[4] The failure by the PRC to fully eliminate the ROC government during the Chinese Civil War led to the creation of two unique political entities laying claim to the same nation and the same history—although the ROC physically controlled only the Taiwanese island.

THE SPLIT BETWEEN CHINA AND TAIWAN

The relative ineffectiveness of U.S. intelligence toward the PRC and the ROC began to be reflected in the years before the conclusion of the civil war. CIA Presidential Daily Briefs (PDBs) from 1948 concede that Chiang's unwillingness to implement military or government reforms created a space in which the communists were able to expand. Even with high levels of U.S. aid, the Nationalist government had little hope of taking back control of China.[5] The intelligence briefing documents further claim that the predicted communist victory would result in a coalition government between the communists and the nationalists, although Chiang would be removed from the helm of the ROC.[6] It was not until mid-1949 that briefs acknowledged the fact that the "coalition government" would actually take the form of a communist dictatorship, and that the struggle between Taiwan and the mainland would last beyond the conclusion of the civil war.[7,8] According to these intelligence reports, Chiang was confident that the potential for conflict between the United States and the USSR would force the Americans to intervene on his behalf.

Into the 1950s, intelligence briefings to the President and other government officials continued to suffer from a lack of creative thinking, and ultimately did not advance the U.S. relationship with China, Taiwan, or other Asian allies.

A June 1949 PDB first stated that, if confined to Taiwan, the nationalists would never be able to take back the mainland. Intelligence analysts predicted that many countries would recognize Beijing as the Chinese capital over Taipei even if the United States chose to stay loyal to the nationalists on Taiwan.[9] Although intelligence officials cited the reality of the situation, the Truman administration chose to retain formal diplomatic relations with Taipei, and cut off all contact with the 500 million people under communist rule on the mainland.[10] This decision can be seen in part as a failure by the Intelligence Community—a failure to look beyond the U.S. fears of communist rule and to recognize that China represented a fundamentally different entity from the Soviets.

Into the 1950s, intelligence briefings to the President and other government officials continued to suffer from a lack of creative thinking, and ultimately did not advance the U.S. relationship with China, Taiwan, or other Asian allies. Briefs from the early 1950s claimed that the presence of the U.S. 7th Fleet in the Taiwan Strait, meant to deter Chinese aggression toward the island, was among the only barriers preventing the Chinese from using force against Taiwan, such as, "The Chinese communists have the capability for mounting an amphibious attack on Taiwan."[11] The true military power of the Chinese at this moment in history has since been debated, and U.S. intelligence analysts may have placed too great an emphasis on Soviet willingness to aid in a potential invasion.[12] China's foreign policy throughout the 1950s focused mainly on taking back Taiwan and reducing Western influence in the Asia-Pacific, and PRC statements emphasized "liberating" the people of Taiwan from ROC oppressors.[13]

The 1954 shelling by the Chinese of Quemoy and Matsu (islands near Taiwan) encouraged Congress to pass the Formosa Resolution, allowing President Eisenhower a "blank check" to defend Taiwan and the surrounding islands.

As the 1950s drew to a close, classified U.S. intelligence documents provided to President Eisenhower made clear that the PRC would seek entrance into the United Nations, and that it was committed to resolving the Taiwan issue peacefully, free of U.S. interference.[14] By 1957 mainland China had established diplomatic relations with almost one-third of all the nations in the world, including India, Burma, and Pakistan. The relevant CIA document stated that U.S. influence was the sole reason more countries had not yet switched recognition to Beijing.[15] The 1954 shelling by the Chinese of Quemoy and Matsu (islands near Taiwan) encouraged Congress to pass the Formosa Resolution, allowing President Eisenhower a "blank check" to defend Taiwan and the surrounding islands. In spite of the communists' steadfast diplomatic focus on Taiwan, the United States signed a mutual defense treaty with Taiwan in 1954 and increased the U.S. naval presence in the Taiwan Strait following further shelling by the Chinese.[16] In 1961 newly elected President John F. Kennedy went as far as to send a letter to Generalissimo Chiang, stating, "I wish to assure you that my government will continue to work closely with you and support your government."[17] Throughout the decade, U.S. intelligence analysts fell prey to collective thinking, assuming that any relationship with the communist power would be impossible, regardless of the U.S. stance toward Taiwan.

Intelligence briefs did not often mention Taiwan in the 1960s due to the growing divide between China and the USSR, which led to the Sino-Soviet split in 1961. The

divide between the communist powers came as a shock to the United States, as intelligence briefings failed to predict the development, assuming that because both countries were communist powers and China was a Soviet puppet no such split would be possible. Had analysts considered historic context, they would have found that China viewed itself as a once great empire with a hereditary right to hegemony in Asia, and Soviet intervention in Southeast Asia created tensions between the countries' leaders.[18] Analysts maintained that the two would coordinate their actions as the only major communist powers, and their inability to read signs of change and think outside established norms created missed opportunities for the United States. The split changed the landscape of the trilateral relationship among the United States, China, and the Soviet Union, but late realization of ideological differences between Mao and Khrushchev eliminated the possibility of using the communists against one another, perhaps producing leverage on Taiwan, nuclear proliferation, and/or a number of other issues.[19]

The insignificant advances toward addressing the Taiwan issue by the Intelligence Community in this time period were mirrored by lackluster back-channel diplomatic efforts. From 1955 to 1970, talks were held between the U.S. government and the PRC in Geneva, Switzerland, through the U.S. ambassador to Czechoslovakia and the Chinese ambassador to Poland. Although these talks enabled the repatriation of several hundred U.S. and Chinese citizens, the inability to make progress on the issue of Taiwan prevented further diplomatic breakthroughs.[20] Diplomacy between the two nations remained at a standstill until 1969, when newly elected President Nixon and his National Security Advisor, Henry Kissinger, took the initiative to achieve rapprochement with the mainland. Their first move involved relaying to Pakistani Information Minister Sher Ali that the United States would stop 7th fleet patrols in the Taiwan Strait as a gesture of good will toward the PRC. Following the relay of the message in October 1970, Nixon referred in a public speech to the "People's Republic of China" for the first time while in Romania.[21]

RAPPROCHEMENT

Following efforts by Nixon and Kissinger to establish a connection with the PRC, Kissinger began secret talks in July 1971 with Zhou Enlai, Premier of the PRC and Mao's chief advisor. Through the secret talks, some of which took place in Beijing, Kissinger conveyed that the United States would move arms away from Taiwan, and that the U.S. would not support an independent Taiwan separate from mainland China.[22] Kissinger's visits coincided with the removal of the ROC from the United Nations in October 1971, by a vote of 76-35.[23] PDBs dating to the same summer confirmed Zhou's concern regarding U.S. military presence in Taiwan, and concluded that removal of U.S. forces from the island could provide a path toward the establishment of diplomatic relations with Beijing.[24] In a 1971 address to Congress, Nixon stated, "We are prepared to establish a dialogue with Peking," and "the United States is prepared to see the People's Republic of China play a constructive role in the family of nations."[25] He did continue, however, that "it is also a question of whether Peking should be permitted to dictate to the world the terms of its participation"[26]—the United States was not yet willing to concede on the issue of Taiwan. The PRC later invited the U.S. national table tennis team and accompanying reporters to Beijing in order to compete in an international competition, setting the stage for a Presidential visit.[27]

President Richard Nixon arrived in China on February 21, 1972, the first U.S. President to visit the PRC since the communist takeover in 1949.

President Richard Nixon arrived in China on February 21, 1972, the first U.S. President to visit the PRC since the communist takeover in 1949. Before the trip, Secretary of State William Rogers advised the President that he must at once establish a U.S. diplomatic presence in Beijing while maintaining the U.S. relationship with the ROC in Taipei. Rogers realized that Taiwan was "less like China with every passing year," and hoped that the PRC had become less dogmatic in regard to Taiwan.[28] At the conclusion of the trip, after multiple meetings among Kissinger, Nixon, Zhou, and Mao, the PRC and the United States issued the Shanghai Communiqué. The document stated, "Taiwan is a province of China which has long been returned to the motherland," and the United States added that "all Chinese on either side of the Taiwan Strait maintain that there is but one China and Taiwan is a part of China."[29] Additionally, both sides agreed upon a peaceful resolution of the Taiwan issue, and that the United States would begin to cut back military installations on Taiwan.[30]

The Communiqué represented a major step forward in Sino-American relations, although it refrained from explicitly indicating U.S. intentions to recognize Beijing as the Chinese capital. The President and his advisor accomplished more during their seven-day visit than the Intelligence Community had been able to achieve over more than a decade. Systematic and bureaucratic problems in the IC, including a "groupthink" mentality that the PRC would be entirely unwilling to negotiate or work with the United States, prevented production of useful insights. Additionally, analysts had failed to consider the possibility of a

Presidential trip to Beijing or potential recognition of the PRC, as a 1970 National Intelligence Estimate (NIE) proclaimed that there would be no headway on the Taiwan issue in coming years—just months before Kissinger's historic trip to Beijing.[31] The success of Nixon's trip was in spite of, not due to, intelligence analysis.

Intelligence briefs confirmed in September 1972 that Japan recognized Beijing as the Chinese capital and would not maintain official diplomatic relations with Taipei following the switch. The analysts suggested that, although the announcement could result in reduced trade between Japan and Taiwan, the economic relationship between the two countries would continue, and that China would not object to this continuation of trade.[32] This move by Japan signaled to the world that the status quo was changing, and had significant implications for the United States. The Shanghai Communiqué indicated to China and U.S. partners that future recognition of Beijing was under consideration, and China reacted by pushing to resolve the Taiwan question. Intelligence briefings to President Nixon throughout 1973 and 1974 (when he resigned as a result of the Watergate scandal) mentioned intensified rhetoric regarding the reunification of Taiwan,[33] and that Zhou Enlai had come under pressure from his Chinese opponents to resolve the dilemma.[34] Nixon and Kissinger had discussed with Beijing the possibility of recognition during Nixon's second presidential term,[35] but Nixon's resignation led to a brief cessation of inertia toward diplomatic relations with Beijing.

FROM TAIPEI TO BEIJING

Nixon's Vice President, Gerald Ford, became President in August 1974, and promptly visited China in 1975. His trip yielded little progress, serving only to reaffirm Nixon's commitments to the normalization of relations with Beijing.[36] That same year, Carter Burgess, President of the Foreign Policy Association, made an extended trip to Beijing and circulated his observations around Washington upon his return. He noted that the "Japan model" of relations with Taiwan was likely the only path toward normalization, and would involve removing the U.S. ambassador and all troops from the island.[37] He suggested, however, that expediency might not be the first priority stating, "China is impressive and we should build a patient and improving friendship with her, but not meet her every price in the process. Don't forget, Stalin's picture is still on the wall!"[38] In the months surrounding Ford's 1975 visit, CIA reports cited leniency by the PRC toward Taiwan, encouraging visits across the strait and granting amnesty to 300 nationalist "war criminals."[39]

Ford was unwilling to capitalize upon Chinese openness to compromise, and the CIA, due to lack of imagination and inability to proscribe policy, was unable to encourage action. Intelligence reports from late in Ford's short tenure focused on the death of Chiang Kai-shek and increasing Taiwanese domestic weapons development.[40] Jimmy Carter was elected President in 1977, and the Chinese feared he would, in the mold of his predecessor, ignore the issue of Sino-American and Sino-Taiwanese relations.[41] Carter's National Security Advisor, Zbigniew Brzezinski, outlined the administration's approach to Taiwan in a secret "first six months" policy document, stating a goal of slowly reducing arms in Taiwan while maintaining defense commitments to the island.[42] Further intelligence briefings to President Carter refused to acknowledge a future scenario in which the United States might abandon diplomatic relations with Taipei, stating, "No conditions should be sought from either side with respect to Taiwan."[43] As late as 1977, elements of the U.S. diplomatic and intelligence communities were unable to imagine cessation of diplomatic relations with Taiwan.

As late as 1977, elements of the U.S. diplomatic and intelligence communities were unable to imagine cessation of diplomatic relations with Taiwan.

In order to quell concerns and demonstrate commitment to resolution of the Taiwan question, Carter sent Secretary of State Cyrus Vance on a high-profile visit to Beijing in 1977. Vance stuck strictly to rhetoric confirming U.S. commitment to steps outlined in the Shanghai Communiqué, saying vaguely that "it is in our mutual benefit that we join in making efforts to move towards our common objectives."[44] Although Vance discussed with his counterparts the initiation of official diplomatic contact with Beijing, PRC officials rejected the advances, unwilling to agree to normalization while the United States still maintained diplomatic contact and military alliance with Taipei.[45] Global media outlets interpreted the visit as tantamount to recognition, with the Italian *La Nazione* of Florence writing that Vance's presence in China "represents an implicit acknowledgement of a tacit, hidden working alliance between the west and China. It is an alliance for which it is worth sacrificing Taiwan."[46] Deputy Secretary of State Warren Christopher traveled to China a year later in 1978, but the "Christopher Mission" again failed to make any traction in solving the issue of diplomatic relations with Beijing.[47] In both negotiations, all other talking points fell to secondary importance behind the "major obstacle" of Taiwan, on which the

Chinese were willing to wait.[48] As Mao Zedong stated in 1959, "It is unimportant if they do not return Taiwan to us for another 100 years."[49]

On January 1, 1979, the Carter administration released the Joint Communiqué on the Establishment of Diplomatic Relations between the United States of America and the People's Republic of China, reversing decades of U.S. China policy and recognizing Beijing as the official capital of China. In recognizing the PRC as the sole government of China, the United States ended diplomatic relations, as well as the Mutual Defense Treaty, with Taiwan. However, the United States would "maintain commercial, cultural, and other unofficial relations with the people of Taiwan."[50] Carter chose to act outside the boundaries of traditional intelligence analysis, and abandoned years of U.S. policy that prevented a working relationship with a country that had become one of its most important economic and political global powers.

In recognizing the PRC as the sole government of China, the United States ended diplomatic relations, as well as the Mutual Defense Treaty, with Taiwan. However, the United States would "maintain commercial, cultural, and other unofficial relations with the people of Taiwan."

Intelligence Community and State Department documents in the years leading to recognition often mention adhering to the ethos of the Shanghai Communiqué and following the "Japan model" of Taiwanese relations, but there was little to no discussion of normalization. The ROC government and representatives of the United States in Taipei were among those most surprised by the sudden switch in policy. As late as December 1978, ROC Foreign Minister Y.S. Tsiang issued a statement saying, "I do not consider that the U.S. government has any justifiable cause at all to unilaterally announce its intention to terminate the defense treaty which, as you know, is a treaty of alliance."[51] The last U.S. ambassador to Taiwan, Leonard Unger, was not made aware of the major policy decision until just hours before the announcement was to be made public on December 15, 1978. A public affairs officer working in Taipei at the time recalled that "a cable came in late at night… that Carter was going to announce the normalization of China and the de-recognition of Taiwan."[52] Unger eventually found Chiang Ching-kuo, the Taiwanese President, at his personal residence, where he read him a letter from Carter indicating that relations would be brought to an end, but all treaties other than the Mutual Defense Treaty would continue in full.[53]

It was not only the Intelligence Community that had fallen out of pace with the Taiwan issue; the U.S. Congress was also not aware in advance of Carter's decision. National Security Advisor Brzezinski purposefully left U.S. officials uninformed, as he was concerned that if given too much information the U.S. Congress would attempt to stop Sino-American normalization.[54] The decision did anger many in Congress, who believed the decision was motivated by the desires of the American business community to seek greater profit from the growing Chinese market, and felt that the U.S. was abandoning an ally and friend.[55] Protests broke out in Taipei outside the U.S. embassy, and angry students and nationalist protesters attacked cars in U.S. motorcades, throwing eggs, rocks, and even shattering a window with a flagpole.[56] U.S. allies held on to hope that Taiwan was not a "canary in a coal mine" indicating a reversal of policy on other U.S. commitments in Asia.[57]

In order to alleviate concerns, Secretary of State Vance gave a speech on January 15, 1979, in which he clarified that the United States would be ending the Mutual Defense Treaty after one year's notice, but that "we will continue our previous policy of selling carefully selected defensive weapons to Taiwan." He also affirmed to the U.S. business community that the economic relationship with Taiwan would continue unimpeded.[58] The Taiwan Relations Act (TRA) was passed on April 10, 1979, stating that "commercial, cultural, and other relations between the people of the United States and the people on Taiwan" would continue. These semi-official activities would be conducted through the newly established American Institute in Taiwan (AIT), a private corporation replacement for the embassy in Taipei.59 The counterpart of the AIT, the Taipei Economic and Cultural Representative Office (TECRO), would likewise establish branches throughout major U.S. cities, and would conduct affairs with the United States through these outposts.[60] China was, and remains, hostile toward the TRA but has refrained from taking action against it.[61]

Taipei now occupies the role Beijing once did, capital of a quasi-sovereign entity without formal diplomatic relations with the United States.

Three decades after the PRC established control in Beijing the United States had come to terms with the reality of Chinese communist rule. Taipei now occupies the role Beijing once did, capital of a quasi-sovereign entity without formal diplomatic relations with the United States.

INTELLIGENCE LESSONS

As Secretary Vance stated in early 1979, "It was just short of seven years from the Shanghai Communiqué to normalization of relations… Opportunities previously denied to us have now begun to take shape."[62] What would have been deemed highly improbable or outright impossible in 1948 happened—the United States voluntarily recognized Mao Zedong's communist government in Beijing, relegating the Republic of China to secondary status. Throughout the entire period, U.S. intelligence in regard to China tended to confirm information and ideas that were already known.[63] Starting with the outcome of the Chinese civil war, briefs prepared by the IC failed to predict an accurate outcome until it had already come to pass, as analysts were unwilling or unable to recognize the momentum and dogmatic nature of the CCP. Throughout the next several decades, Taiwan was mentioned regularly in CIA documents as the major impediment to the improvement of Sino-American relations, but these briefs presented no definitive statements that the issue would be unsolvable without movement on policy toward Taiwan.

In the trilateral relationship among the United States, China, and Taiwan, intelligence ultimately served as a hindrance to progress rather than an actionable source of information.

Once the Intelligence Community had established that the United States would unwaveringly maintain official diplomatic relations with the ROC, there was no space for creative solutions or workarounds to relations with Beijing. Sino-American hostility became something assumed to be unavoidable.[64] Additionally, the communist government in Beijing was assumed to possess qualities similar to those of the communist regime in Moscow, simply due to ideological connections.[65] These errors and failures may have also stemmed in part from issues of intelligence collection, as the United States was entirely isolated from mainland China during the period between 1949 and 1972. The majority of foreign-sourced intelligence came from analysts based in Taipei, and as such contained inherent bias toward maintaining diplomatic relations with Taiwan.

In the trilateral relationship among the United States, China, and Taiwan, intelligence ultimately served as a hindrance to progress rather than an actionable source of information. Kissinger, Nixon, and Carter acted drastically because the change was not going to be initiated at any other level of government. It is not the job of the Intelligence Community to make policy prescriptions, but in the name of being objective its analysis became irrelevant, failing to imagine how far the United States might be willing to go (i.e., de-recognizing Taiwan) to establish diplomatic relations with the world's most populous nation.[66] Intelligence should also have focused on China's development trajectory. China is now exponentially more powerful than it was in the 1970s, and it will therefore be much more difficult to apply pressure on the Taiwan issue. Had intelligence analysts emphasized this point, the U.S. might have taken a harder line toward China regarding Taiwan in 1979, rather than pushing the issue of unification aside.

LOOKING TOWARD THE FUTURE

Since normalization in 1979, the China-Taiwan relationship has remained in a delicate balance, with both sides agreeing in 1992 that there is only one China, but with different interpretations as to what that China is.[67] Taiwan transitioned to a democratic government in 1996, and amended the original ROC constitution that had been in place since establishing control on the island in 1949. In response to democratization, Beijing shelled the Taiwan Strait, protesting what was perceived as movement away from the One China Policy.[68] The first democratic President, Lee Teng-hui, further angered Beijing in 1999 by stating that Taiwan and China had a special "state to state" relationship.[69] An NIE from the same year predicted that Beijing would continue to take small actions in protest against Lee's statement, but it was unlikely to launch any full-fledged invasion of the island. The NIE also clarified several "red lines" that, if crossed by Taiwan, would mean invasion—an explicit declaration of independence, foreign support for independence, development of nuclear weapons, or widespread social instability and upset on the island.

In the U.S. Intelligence community, analysts must think beyond the One China Policy, and beyond the status quo. Just as analysts could not have imagined normalization with China in the early 1970s, it is likely that at present there are few who imagine future normalization with Taiwan.

Popular opinion on Taiwan has turned entirely against the 1992 consensus and the "One China Policy" in recent years, with 90% of the population identifying as distinctly Taiwanese rather than Chinese,[70] and 66% of the

population disapproving of any path toward eventual reunification with mainland China.[71] These demographic changes have led to the election of Tsai Ing-wen, a pro-independence leader eager to create a new global role for Taiwan. In the United States, then-President-Elect Donald Trump accepted a call from the Taiwanese President, the first U.S. President to do so since 1979, and he has openly questioned the nature of the United States' unofficial relations with the island. These two leaders may bring about yet another large shift in U.S. policy toward the Taiwan issue.

By avoiding complications posed by groupthink and mirror-imaging, and by thinking resourcefully, the Intelligence Community can prepare U.S. leadership to make the difficult decisions required.

Although more recent intelligence documents related to the trilateral relationship have not been declassified, intelligence has likely followed traditional patterns in recent years. The assumption that the United States will abide by the One China Policy is the foundation upon which Sino-American relations have been built, but this may not always be true. In the same manner, the Taiwan Relations Act is not a permanent solution, and the longer Taiwan exists as a de facto independent state the more it will be perceived as one in the international community.[72] In the U.S. Intelligence community, analysts must think beyond the One China Policy, and beyond the status quo. Just as analysts could not have imagined normalization with China in the early 1970s, it is likely that at present there are few who imagine future normalization with Taiwan. However, analysts must be careful, as any assumption that China would not act against its own interest on the Taiwan issue could be based on mirror-imaging on behalf of the United States, rather than based on fact. President Trump, as Nixon and Carter before him, has taken the initiative on an issue that was seen as a stalemate at all other diplomatic levels.

INTELLIGENCE AND DIPLOMACY

There is a Chinese saying which Cyrus Vance, in his 1977 visit to Beijing, chose to write hastily on a piece of scrap paper upon hearing it from a Chinese colleague: "As distance tests the horse's strength, so time reveals a person's heart."[73] China is determined that time will prove its commitment to reunification with the island of Taiwan, listing it among the country's only "core interests."[74] U.S. intelligence analysts must look carefully at all possible future scenarios, ranging from the status quo to a complete break with accepted U.S. policy. Better human intelligence capable of analyzing sentiment in Beijing and Taipei, along with close diplomatic relationships with leadership of both entities, will ensure that any actions moving forward can be made thoughtfully. Intelligence analysts have the potential to positively inform policymakers as to the consequences and benefits of different courses of action. The issue of Taiwan must eventually reach a permanent conclusion, and the United States will ultimately play a role in this decision. By avoiding complications posed by groupthink and mirror-imaging, and by thinking resourcefully, the Intelligence Community can prepare U.S. leadership to make the difficult decisions required.

NOTES

[1] Chiu, Hungdah, *China and the Taiwan Issue*, p. 10. New York: Praeger, 1979.
[2] Bradley, James, *The China Mirage: The Hidden History of American Disaster in Asia*, New York: Little, Brown, 2015.
[3] Times Staff. "How China and Taiwan Split: A Look Back, as Leaders Meet." *Latimes.com*. *Los Angeles Times*, 6 November 2015. Web. 7 April 2016. < http://timelines.latimes.com/la-fg-china-taiwan-relations-timeline/>.
[4] Kristof, Nicholas, "A Dictatorship That Grew Up," *The New York Times*, 15 February 1992. Web. 19 December 2016. <http://www.nytimes.com/1992/02/16/magazine/a-dictatorship-that-grew-up.html?pagewanted=all>.
[5] Confidential Central Intelligence Agency document: The Current Situation in China, p. 1. CIA Reading Room, 22 July 1948. <https://www.cia.gov/library/readingroom/docs/DOC_0001086057.pdf>.
[6] Confidential Central Intelligence Agency document: Prospects for a Negotiated Peace in China, p. 1. CIA Reading Room, 3 August 1948. <https://www.cia.gov/library/readingroom/docs/DOC_0001086034.pdf>.
[7] Confidential Central Intelligence Agency document: Possible Developments in China, p. 1. CIA Reading Room, 19 November 1948. <https://www.cia.gov/library/readingroom/docs/DOC_0001098225.pdf>.
[8] Confidential Central Intelligence Agency document: Probable Developments in China, p. 1. CIA Reading Room, 16 June 1949. <https://www.cia.gov/library/readingroom/docs/DOC_0001086039.pdf>.
[9] Ibid.
[10] "Chinese Nationalists Move Capital to Taiwan," *History.com*. A&E Television Networks, n.d. Web. 1 December 2016. <http://www.history.com/this-day-in-history/chinese-nationalists-move-capital-to-taiwan>.
[11] Confidential Central Intelligence Agency document: National Intelligence Estimate, Nationalist China. CIA Reading Room, 17 January 1951. <https://www.cia.gov/library/readingroom/docs/DOC_0001084983.pdf>.
[12] Khan, Sulmaan Wasif, "The Aesthetic of Analysis: National Intelligence Estimates and Other American Appraisals of the Cold War Triangular Relationship," *Diplomatic History* 32.5 (2008): 869-897. Web. < http://onlinelibrary.wiley.com/doi/10.1111/j.1467-7709.2008.00733.x/full>.

[13] Confidential Central Intelligence Agency document: National Intelligence Estimate Number 13-56, Chinese Communist Capabilities and Probable Courses of Action Through 1960, p. 2. CIA Reading Room, 5 January 1956. <https://www.cia.gov/library/readingroom/docs/DOC_0001098223.pdf>.
[14] Confidential Central Intelligence Agency document: National Intelligence Estimate Number 13-58, Communist China. CIA Reading Room, 13 May 1958. <https://www.cia.gov/library/readingroom/docs/DOC_0001085002.pdf>.
[15] Confidential Central Intelligence Agency document: National Intelligence Estimate, Communist China Through 1961, p. 19, 19 March 1957. <https://www.cia.gov/library/readingroom/docs/DOC_0001098224.pdf>.
[16] Chronology: China and the United States: From Hostility to Engagement, 1960-1998. DNS Collection: China, 1960-1998. <http://search.proquest.com/dnsa_ch/docview/1679041228/fulltext/50037677657F4383PQ/1?accountid=15172>.
[17] Declassified White House document: Letter from President John F. Kennedy to Taiwanese President Chiang Kai-shek, 8 May 1961. Gale Group U.S. Declassified Documents Online. <http://gdc.galegroup.com/gdc/artemis/MonographsDetailsPage/MonographsDetailsWindow?disableHighlighting=false&displayGroupName=DVI-Monographs&currPage=23&dviSelectedPage=&scanId=&query=KE+taiwan&source=fullList&prodId=USDD&search_within_results=&p=USDD&mode=view&catId=&u=29002&limiter=&displayquery=KE+taiwan&displayGroups=&contentModules=&action=e&sortBy=&documentId=GALE%7CCK2349687605&windowstate=normal&activityType=BasicSearch&failOverType=&commentary=>.
[18] Khan, Sulmaan Wasif, "The Aesthetic of Analysis: National Intelligence Estimates and Other American Appraisals of the Cold War Triangular Relationship," *Diplomatic History* 32.5 (2008): 869-897. Web. < http://onlinelibrary.wiley.com/doi/10.1111/j.1467-7709.2008.00733.x/full>.
[19] Ibid.
[20] "Milestones: 1953-1960 – Office of the Historian," U.S. Department of State, n.d. Web. 1 December 2016. <https://history.state.gov/milestones/1953-1960/china-talks>.
[21] Chronology: China and the United States: From Hostility to Engagement, 1960-1998. DNS Collection: China, 1960-1998. <http://search.proquest.com/dnsa_ch/docview/1679041228/fulltext/50037677657F4383PQ/1?accountid=15172>.
[22] Ibid.
[23] Chiu, Hungdah, *China and the Taiwan Issue*, p. 179, New York: Praeger, 1979.
[24] Confidential Central Intelligence Agency document: The President's Daily Brief, 24 June 1971, p. 4, CIA Reading Room. <https://www.cia.gov/library/readingroom/docs/DOC_0005992715.pdf>.
[25] Chiu, Hungdah, *China and the Taiwan Issue*, p. 178, New York: Praeger, 1979.
[26] Ibid.
[27] Ibid.
[28] Declassified White House document: Policy Document from Secretary of State William Rogers to President Richard Nixon on U.S. Policy towards Taiwan, 2 February 1972, p. 10. Gale Group U.S. Declassified Documents Online. <http://gdc.galegroup.com/gdc/artemis/MonographsDetailsPage/MonographsDetailsWindow?disableHighlighting=false&displayGroupName=DVI-onographs&currPage=1&dviSelectedPage=&scanId=&query=KE+taiwan&source=fullList&prodId=USDD&search_within_results=&p=USDD&mode=view&catId=&u=29002&limiter=&display-query=KE+taiwan&displayGroups=&contentModules=&action=e&sortBy=&documentId=GALE%7CCK2349695794&windowstate=normal&activityType=BasicSearch&failOverType=&commentary=>.
[29] Sheng, Lijun, *China's Dilemma: The Taiwan Issue*, p. 11. London: I.B. Tauris, 2001..
[30] Ibid.
[31] Khan, Sulmaan Wasif, "The Aesthetic of Analysis: National Intelligence Estimates and Other American Appraisals of the Cold War Triangular Relationship," *Diplomatic History* 32.5 (2008): 869-897. Web. < http://onlinelibrary.wiley.com/doi/10.1111/j.1467-7709.2008.00733.x/full>.
[32] Confidential Central Intelligence Agency document: President's Daily Brief, 12 September 1972, p. 10, CIA Reading Room. <https://www.cia.gov/library/readingroom/docs/DOC_0005993515.pdf>.
[33] Confidential Central Intelligence Agency document: President's Daily Brief, 2 March 1973, p. 5, CIA Reading Room. <https://www.cia.gov/library/readingroom/docs/DOC_0005993760.pdf>.
[34] Confidential Central Intelligence Agency document: President's Daily Brief, 2 April 1974, p. A1, CIA Reading Room. <https://www.cia.gov/library/readingroom/docs/DOC_0006007713.pdf>.
[35] Chronology: China and the United States: From Hostility to Engagement, 1960-1998. DNS Collection: China, 1960-1998. <http://search.proquest.com/dnsa_ch/docview/1679041228/fulltext/50037677657F4383PQ/1?accountid=15172>
[36] "U.S.-China High Level Visits," U.S. Department of State, n.d. Web. 3 December 2016. <https://2001-2009.state.gov/p/eap/rls/64713.htm>.
[37] Cyrus R. and Grace Sloane Vance Papers, 1919-2005. Series II. Government Service Papers (Carter Presidential Administration). Box 9, China Trip: Carter Burgess 1975 China Journey Notes. Yale University Manuscripts and Archives.
[38] Ibid.
[39] Confidential Central Intelligence Agency document: The President's Daily Brief, 20 March 1975, p. 6, CIA Reading Room. <https://www.cia.gov/library/readingroom/docs/DOC_0006014750.pdf>.
[40] Confidential Central Intelligence Agency document: The President's Daily Brief, 24 June 1975, p. 4, CIA Reading Room. <https://www.cia.gov/library/readingroom/docs/DOC_0006014832.pdf>.
[41] Confidential Central Intelligence Agency document: The President's Daily Brief, 13 January 1977, p. 2, CIA Reading Room. <https://www.cia.gov/library/readingroom/docs/DOC_0006466947.pdf>.
[42] Cyrus R. and Grace Sloane Vance Papers, 1919-2005. Series II. Government Service Papers (Carter Presidential Administration). Box 9, China Trip: 1976 First 6 Months Policy Planning Document from NSA Brzezinski to Carter. Yale University Manuscripts and Archives.
[43] Cyrus R. and Grace Sloane Vance Papers, 1919-2005. Series II. Government Service Papers (Carter Presidential Administration). Box 9, China Trip: Overview of Foreign Affairs and Defense Issues, prepared for Carter/Mondale,

Policy Planning by Paul C. Warnke. Yale University Manuscripts and Archives.
[44] Cyrus R. and Grace Sloane Vance Papers, 1919-2005. Series II. Government Service Papers (Carter Presidential Administration). Box 9, China Trip: Chinese Visit Welcome Banquet Toast. Yale University Manuscripts and Archives.
[45] Chiu, Hungdah, *China and the Taiwan Issue*, p. 183, New York: Praeger, 1979.
[46] Cyrus R. and Grace Sloane Vance Papers, 1919-2005. Series II. Government Service Papers (Carter Presidential Administration). Box 9, China Trip: August 1977 Collected News Clippings, *La Nazione* of Florence. Yale University Manuscripts and Archives.
[47] Chiu, Hungdah, *China and the Taiwan Issue*, p. 185. New York: Praeger, 1979.
[48] Cyrus R. and Grace Sloane Vance Papers, 1919-2005. Series III. Papers on Professional and Personal Activities, 1957-1992. Box 19, China Trip: Report of the World Affairs Delegation to the People's Republic of China, by Allen S. Whiting, National Committee on United States-China Relations, Inc. 1975. Yale University Manuscripts and Archives.
[49] Chiu, Hungdah, *China and the Taiwan Issue*, p. 243.,New York: Praeger, 1979.
[50] Sheng, Lijun. *China's Dilemma: The Taiwan Issue*, p. 12. London: I.B. Tauris, 2001.
[51] Chiu, Hungdah. *China and the Taiwan Issue*, p. 261, New York: Praeger, 1979.
[52] "The U.S. De-recognizes Taiwan in Favor of Communist China - January 1, 1979." Association for Diplomatic Studies and Training, N.p., 19 December 2013. Web. 3 December 2016. <http://adst.org/2013/12/the-u-s-recognizes-communist-china-not-taiwan-january-1-1979/>.
[53] Cheung, Han. "Taiwan in Time: Taiwan's Last US Ambassador," *Taipei Times*, N.p., 29 May 2016. Web. 4 December 2016. <http://www.taipeitimes.com/News/feat/archives/2016/05/29/2003647366>.
[54] Ibid.
[55] "The U.S. De-recognizes Taiwan in Favor of Communist China - January 1, 1979." Association for Diplomatic Studies and Training, N.p., 19 December 2013. Web. 3 December 2016. <http://adst.org/2013/12/the-u-s-recognizes-communist-china-not-taiwan-january-1-1979/>.
[56] Cheung, Han, "Taiwan in Time: Taiwan's Last US Ambassador," *Taipei Times*, N.p., 29 May 2016. Web. 4 December 2016. <http://www.taipeitimes.com/News/feat/archives/2016/05/29/2003647366>.
[57] Ibid.
[58] Twining, Daniel, "The Taiwan Linchpin," Hoover Institution, N.p., 1 February 2013. Web. 5 December 2016. <http://www.hoover.org/research/taiwan-linchpin>.
[59] Cyrus R. and Grace Sloane Vance Papers, 1919-2005. Series II. Government Service Papers (Carter Presidential Administration). Box 9, China Trip: January 15th Speech, 1979. Yale University Manuscripts and Archives.
[60] "American Institute in Taiwan," American Institute in Taiwan - AIT Introduction. N.p., n.d. Web. 6 December 2016. <http://www.ait.org.tw/en/ait-introduction.html>.
[61] Ibid.
[62] Steiner, Fred, Chu-lien Yen, and Ti-ju Lin, TRA 20: The Legacy of the Taiwan Relations Act: A Compendium of Authoritative 20th Anniversary Assessments. Taipei, Taiwan: Published by the Government Information Office, Republic of China, 1999.
[63] Cyrus R. and Grace Sloane Vance Papers, 1919-2005. Series II. Government Service Papers (Carter Presidential Administration). Box 9, China Trip: January 15th Speech, 1979. Yale University Manuscripts and Archives.
[64] Hengjun, Yang, "How US Intelligence Gets China Wrong," *The Diplomat*, 26 April 2016. Web. 6 December 2016. <http://thediplomat.com/2016/04/how-us-intelligence-gets-china-wrong/>.
[65] Khan, Sulmaan Wasif, "The Aesthetic of Analysis: National Intelligence *Estimates and Other American Appraisals of the Cold War Triangular Relationship," Diplomatic* History 32.5 (2008): 869-897. Web.
[66] Ibid.
[67] Ibid.
[68] "China-Taiwan Relations." Council on Foreign Relations, N.p., n.d. Web. 5 December 2016. <http://www.cfr.org/china/china-taiwan-relations/p9223>.
[69] Sheng, Lijun. *China's Dilemma: The Taiwan Issue*, p. 28. London: I.B. Tauris, 2001.
[70] Pike, John, "Taiwan Confrontation – 1999." *Global Security*, N.p., n.d. Web. 5 December 2016. <http://www.globalsecurity.org/military/ops/taiwan-1999.htm>.
[71] Nylander, Johan, "Strong Support for Independence in Taiwan." *Forbes* Magazine, 14 February 2015. Web. 8 April 2016. < http://www.forbes.com/sites/jnylander/2015/02/14/strong-support-for-independence-in-taiwan/#67ffaf956f8f>.
[72] Hsiao, Russell, "America Needs a Taiwan Strategy." *The Diplomat*, 5 October 2012. Web. 8 April 2016. < http://thediplomat.com/2012/10/u-s-needs-a-taiwan-strategy/>.
[73] Steiner, Fred, Chu-lien Yen, and Ti-ju Lin, TRA 20: The Legacy of the Taiwan Relations Act: A Compendium of Authoritative 20th Anniversary Assessments. Taipei, Taiwan: Published by the Government Information Office, Republic of China, 1999.
[74] Cyrus R. and Grace Sloane Vance Papers, 1919-2005. Series III. Papers on Professional and Personal Activities, 1957-1992. Box 19, China Trip: Notes on 1984 Visit to China. Yale University Manuscripts and Archives.
[75] Wong, Edward, "Security Law Suggests a Broadening of China's 'Core Interests'." *The New York Times*, N.p., 4 July 2015. Web. 4 December 2016. <http://www.nytimes.com/2015/07/03/world/asia/security-law-suggests-a-broadening-of-chinas-core-interests.html>.

Alex Herkert was an undergraduate student at Yale University at the time this article was written. Beginning in the fall of 2017 he will be studying at Oxford University in the United Kingdom.

Rebalancing the Intelligence Analyst Career Cycle

by Dr. John A. Gentry

All intelligence services employ people they want to be "good" at what they do. Agencies identify backgrounds they expect effective employees to have, which they use to choose the people they hire, and they have many ways to improve employees' skills over the course of a career. The central argument of this essay is that the U.S. Intelligence Community (IC) has in recent years skewed these decisions about its analysts in favor of the *training* part of the career cycle—at the expense of *selection*, *education*, and *professional development* stages of the cycle—and that this imbalance both reflects and causes systemic analytic performance problems. Rebalancing the stages of management of employees' careers would help the IC improve its performance. While IC leadership must choose to make such changes, the colleges and universities that provide the IC's recruits would be affected by such de facto reforms—on balance positively, I argue—and would have roles to play in their implementation. This essay addresses strategic all-source analysis in the IC; to the extent that other IC career tracks and other nations' intelligence services operate similarly, it may also be applicable to them.

THE CURRENT SITUATION

The career cycle for U.S. intelligence analysts is now drastically skewed in favor of *training*. While the emphasis on training of "tradecraft" was apparent in the 1990s at the Central Intelligence Agency (CIA), it received a dramatic boost after 2001 when President George W. Bush ordered the CIA to increase its intelligence analyst corps by 50 percent in the wake of the September 11 attacks, and IC agencies (with the exception of the State Department's Bureau of Intelligence and Research, or INR) rushed to comply.[1] They *selected* for hire large numbers of relatively young and inexperienced individuals, often with modest levels of formal education. They de-emphasized experience and the *education* needed to earn graduate degrees in favor of recruiting bright young people they could mold through training into analysts who mainly produced current intelligence—which surveys long have shown senior consumers prefer and which seemed even more appropriate in wartime.[2] Management made clear that frequent shifts in positions were career-enhancing and evolving intelligence priorities led to regular reassignments that made "generalist" skills adequate for both analysis and rapid career progression. The most important skill was writing well, and fast, and many analysts reported that they felt their jobs were morphing from that of scholar to journalist.[3]

Expertise is typically produced by a combination of education and experience.

This practice led to a de facto IC de-emphasis on expertise as an intellectual asset for analysts despite the fact that IC policy in the form of Intelligence Community Directive (ICD) 610, *Competence Directories for the Intelligence Community Workforce*, strongly supports creation and maintenance of analytic expertise.[4] A quarter century ago, senior analyst Harold Ford argued that overemphasis on current intelligence at the expense of research which builds collective knowledge and the intellectual capital of individual analysts causes intelligence failures.[5] Perceptions that the emphasis on current intelligence is now even stronger have recently prompted numerous prominent, senior intelligence analysts to rue current trends and call for re-emphasis on substantive expertise.[6]

Expertise is typically produced by a combination of education and experience. Virtually by definition, 22-year-olds directly out of colleges' and universities' bachelor's programs have little of either of intelligence value, however natively able they may be. Prominent psychologist and IC consultant Philip Tetlock argues that IC agencies erroneously believe they can train people in the wiles of their agencies, give them some training on structured analytic techniques and critical thinking skills, and thereby achieve the performance levels they need.[7] Nevertheless, with the agencies' concurrence in the confederacy that is the IC, the Office of the Director of National Intelligence (ODNI) in 2007 promulgated ICD 203, *Analytic Standards*, which ostensibly provides rigorous standards but in fact is little more than a list of preferred processes and presentational formats. ODNI does not even try to measure adherence to the only

substantive standard, Tradecraft Standard 8 – "Makes accurate judgments and assessments."[8] Even ODNI officials responsible for monitoring compliance with the standards claim only that the standards help by "raising the floor" of acceptable intelligence analysis—a very modest contribution.[9] Mark Lowenthal thinks their emphasis on process over content may actually hurt, not help, analysis.[10]

Professional development of analysts within the IC is also weak...

Professional development of analysts within the IC is also weak, but unsurprising given the low regard most agencies have for substantive expertise. Even if IC agencies wanted to provide their personnel more educational opportunities, they do not have the luxury the U.S. military has in being able to train and educate its troops frequently and extensively. Instead, IC agencies offer mid-career training courses that usually are short—a week or less—which accommodate employees' busy schedules. Agencies provide few opportunities for analysts to return to universities for master's degrees or doctorates. Internally, the National Intelligence University can educate only a modest number of IC professionals in a limited number of specialty areas in its one-year-long master's program.[11] Hence, professional development that generates substantive expertise is largely a matter of on-the-job learning—an important process damaged by the IC's preference for regular rotations of its personnel and its consequently purposeful discarding of expertise—and the evidently rare personal initiative of driven autodidacts.

CHARACTERISTICS OF STRATEGIC INTELLIGENCE ANALYSTS AS PEOPLE

Most IC agencies do not appreciably consider the basic human characteristics of good intelligence analysts. The idea that some personality types are especially good at analysis is old, although it clearly has fallen from favor in recent years in both the IC generally (again, except in INR) and the academy. Contemporary expectations for employees' aptitudes, attitudes, and performance characteristics contrast markedly with those of the Cold War era; they are now lower in the IC generally than in the better analytic organizations of old. For example, Sherman Kent wrote in 1949 that strategic intelligence analysis requires:

> … people to whom research and rigorous thought are the breath of life, and [agencies] must accordingly have tolerance for the queer bird and the eccentric with a unique talent. They must guarantee a sort of academic freedom of inquiry and must fight off those who derogate such freedom by pointing to its occasional crackpot finding. They must be built around a deference to the enormous difficulties which the search for truth often involves.[12]

In 1972 Cynthia Grabo, a Defense Intelligence Agency specialist on strategic warning, finished writing a now-classic book on warning analysis that identified characteristics of good warning analysts, including: "basic intellectual attributes" of insatiable curiosity, aptitude for detailed research, imagination, a retentive memory, and recognition of that which is important; and "attributes of character or temperament," including motivation, capacity for hard work, and initiative.[13] Grabo's characteristics remain good ones for strategic analysts but appear nowhere in ODNI discussions of desirable analyst attributes or work processes. Former CIA analyst and retired senior executive James Simon argued that the most important characteristic of an analyst is curiosity.[14] Former CIA analyst Michael Turner similarly suggested that the CIA should focus on hiring the "right kind of people."[15] In 2015 Philip Tetlock identified characteristics of people especially good at forecasting, one of the tasks of a strategic all-source analyst: "… superforecasting [sic] demands thinking that is open-minded, careful, curious, and—above all—self-critical. It also demands focus."[16] Tetlock added that the key determinants of forecasting success are such personal propensities, followed by native intelligence, then followed more distantly by possession of skills that can be taught.[17] The IC's recruitment and training philosophy thereby emphasizes what Tetlock, an authority on the subject, considers to be the *least* effective way to improve forecasting accuracy.

This gradual "blue-collarization" of the work force in some agencies appeals to people who choose government work because it offers attractive job security and regular work hours, not intellectual challenges, and also is detrimental to analytic performance.

Most IC agencies make little effort to identify such individuals during *selection* processes.[18] The idea that people's basic characteristics and propensities are important—not just their demographic category or training after joining government—is inconsistent with the IC's philosophy of hiring reasonably bright but inexperienced people who have not had a chance to demonstrate such characteristics in the workplace. (Again, INR is an exception to this generalization.) This view may also create unattractive vulnerabilities to

accusations of political incorrectness. It is equally evident that many analysts who do not have such traits become, and remain, analysts—a result of dysfunctional federal personnel policies and managers' reluctance to do an unpleasant part of their jobs.

In addition, some agencies have de-professionalized intelligence work in recent years by incrementally adopting government-wide personnel rules (despite their ability to claim exemptions) that, for example, administratively punish employees who work more than 40 hours per week without prior permission. This gradual "blue-collarization" of the work force in some agencies appeals to people who choose government work because it offers attractive job security and regular work hours, not intellectual challenges, and also is detrimental to analytic performance. Hence, the IC, while containing many fine analysts, also employs some people with traits fundamentally incompatible with those Kent, Grabo, Tetlock, and others identify as essential in good strategic analysts.

A GOVERNMENT "SOLUTION"

This assessment suggests numerous desirable changes in IC policy that would require fundamental changes in management philosophy. A better philosophy would require higher educational and/or experience levels of new and existing employees, better formal and informal career educational opportunities for employees, and expectations of better professional *self*-development, while de-emphasizing training, at least relatively. It would require the IC to think differently about the basics of recruiting, leading, and managing an analytic work force. I suggest the following more specific changes for parts of the IC that perform all-source, strategic analysis. The presence or absence of these factors also could be used as criteria for assessing the ongoing competence of analytic agencies and prospects for success of reform proposals.

The IC should restore organizational respect for substantive expertise. It should recruit expertise, as INR does, and build it through research programs that require analysts to research and learn. The building process can occur in many ways, but it will not happen in the classrooms of IC agencies devoted to "training." These steps are complementary. They both are necessary to give the IC the reservoir of organizational knowledge and substantive analyst expertise needed to warn of threats and opportunities in rapidly unfolding events and to make sense of important mysteries. The IC should better maintain its intellectual capital by leaving most analysts on accounts for extended periods—the practice abandoned in the late 1980s and 1990s in most agencies in favor of the rapid rotations of the generalist career track. Expertise is essential for sound warning, estimative, research, ***and*** current intelligence—all of the aspects of intelligence analysis. The IC should mainly hire people with master's degrees and doctorates. It should promote people on the basis of their possession of expertise, as INR does, and encourage analysts to reach outside their organizations (and the government) to find expertise when they do not have it, not cloister analysts due to security concerns.

IC leaders should show some backbone by scaling back the share of current intelligence in the IC's product mix.

IC leaders should show some backbone by scaling back the share of current intelligence in the IC's product mix. Certainly consumers like it, but the IC is massive; there is room for enhanced research efforts to help prevent the intelligence failures of tomorrow. One less-than-optimal solution is to reestablish an organizational dichotomy of old—separate current and research offices that follow the same general functions and/or regions of the world. A better way is to return to a philosophy that includes a research program to which many all-source analysts contribute when they are not working on current intelligence articles.[19]

IC leadership should recognize that "procedural expertise" that is a major focus of training programs is not really expertise.[20] It is instead knowing how to work in one's bureaucratic environment. Knowing where the restrooms are does not constitute expertise of genuine intelligence value.

The IC should abandon the notion that there is such a thing as "generalist expertise." Inquisitive and iconoclastic generalists without expertise, some produced by classical liberal educations, have value in some circumstances. Analysts can become real experts and then move on to other areas of responsibility, bringing to new challenges background knowledge and the analytic methods acquired through the rigorous process of becoming an expert. Such late-career generalists have considerable value in some situations—as members of "red teams," for example. However, neither skill set substitutes for substantive expertise focused on important intelligence issues.

The IC should think small—and high-quality—like INR. It should think like prominent British scientific intelligence officer Reginald Victor Jones who, soon after the end of World War II in Europe, outlined his ideas for the future of British intelligence:

> A fundamental difficulty of Intelligence work is that input is by source, and output is by subject. A changeover [from the goals of wartime intelligence] has thus to occur inside the Intelligence machine, which therefore has to act as far as possible as a single perfect human mind, observing, remembering, criticizing and correlating different types of information, and then giving expression to the result. No card index can do it, although indexes are useful adjuncts. The larger the organization, the less can it resemble a single mind. ***An Intelligence organization has therefore to consist of as small a number as possible of individuals with abilities as great as possible.*** For the same reason, Intelligence is better done by a staff than by a committee [emphasis added].[21]

Former CIA analyst Richard Russell similarly advised the IC, well over half a century later: employ fewer, better people.[22] Former senior Israel military intelligence officer Shlomo Gazit argued that intelligence analysts "must be very carefully selected at all echelons."[23] Furthermore, Harold Ford believed that the Office of National Estimates in the 1950s was a fine producer of national estimates because it employed only top-notch people. O/NE's performance, he argued, declined when leadership assigned lesser people to it.[24] Unfortunately, the IC except INR has done the opposite of what these men recommended.

Intelligence schools have a role to play in what might finally be the long-proclaimed but elusive "transformation" of the IC that would affect selecting, educating, training, and professionally developing career analysts.

WHAT COLLEGES AND UNIVERSITIES CAN DO

Intelligence schools have a role to play in what might finally be the long-proclaimed but elusive "transformation" of the IC that would affect selecting, educating, training, and professionally developing career analysts.[25] While a "down-sized" IC would need fewer junior analysts, better candidates would still be hired and other aspects of reform would be more clearly positive for schools by leading them to take steps that could include:

- Better helping students understand just what IC analytic work entails, including expectations about daily life, career progression, and organizational cultures. This work is not for everyone. Intelligence programs can still usefully serve budding intelligence analysts in business and other arenas and many other student interests—including understanding what an important element of government actually does.
- Helping students to develop the kinds of personal traits Grabo and others identify as essential for sound analytic work—and for professionally well-regarded analysts. Some people argue that leaders are born, not trained, but military services spend much time and effort to improve the leadership skills of all of their troops with some success. I suggest that curiosity, perseverance, and imaginative thinking can be encouraged in young minds, but these traits are not produced in "critical thinking" classes.
- Better incorporating a concentration in a substantive area in general undergraduate programs preparing students to apply for IC jobs.
- Enlarging master's programs, with increased emphasis on incorporating substantive regional or functional expertise useful for real intelligence analysis.
- Developing tailored graduate programs, perhaps in the form of certificate programs, which could provide appreciable expertise to current IC analysts on evolving issues of national importance. These might be residence courses provided by universities in the Washington, DC, area or other areas where there are appreciable concentrations of analysts, concentrated short courses in residence anywhere, short courses taught at agency training centers, or online courses. Because such needs could cover a wide variety of functional and geographical topics, this effort would require intelligence program managers to closely coordinate with university administrators and other departments, and regularly to communicate with IC agencies to monitor their evolving needs for substantive expertise. It also would require an ability to build courses quickly to respond to evolving IC needs. A modest degree of security vetting perhaps would satisfy an IC that is paranoid about leaks in the post-Snowden era, making this form of "outreach" less threatening while not giving professors security clearances that would burden them with non-disclosure agreements.

American colleges and universities responded appreciably and effectively to the IC's changing desires after 9/11 and should expect more changes in the future. Inertia of rest is powerful in government but the IC does change, especially in response to sharp criticism. Russell Travers, a senior IC official who wrote a prescient article in 1997 anticipating a major intelligence failure in 2001, penned another article in 2015 again expressing worry about the performance prospects of the IC.[26] Will a new round of IC reforms, perhaps triggered by another major failure, mirror those outlined herein? Surely not exactly. But many in the IC share Travers' concerns, and universities should be alert for a new window of IC receptivity to reform when, I think inevitably, it does come.

NOTES

[1] Walter Pincus, "Bush Orders the CIA to Hire More Spies," *The Washington Post*, November 24, 2004, A4.
[2] Harold P. Ford, *Estimative Intelligence: The Purposes and Problems of National Intelligence Estimates* (Lanham MD: University Press of America, 1993), 176.
[3] For example, Rob Johnston, *Analytic Culture in the U.S. Intelligence Community* (Washington, DC: Center for the Study of Intelligence, 2005), 27.
[4] John A. Gentry, "Has the ODNI Improved U.S. Intelligence Analysis?" *International Journal of Intelligence and CounterIntelligence* 28, no. 4 (Winter 2015): 640-641.
[5] Ford, *Estimative Intelligence*, 121.
[6] For example, Bowman H. Miller, "Improving All-Source Intelligence Analysis: Elevate Knowledge in the Equation," *International Journal of Intelligence and CounterIntelligence* 21, no. 2 (Summer 2008): 337-354; Mark M. Lowenthal, "A Disputation on Intelligence Analysis and Reform: My 18 Theses," *International Journal of Intelligence and CounterIntelligence* 26, no. 1 (Winter 2013): 31-37; Roger Z. George, "Reflections on CIA Analysis: Is It Finished?" *Intelligence and National Security* 26, no. 1 (February 2011): 77.
[7] Welton Chang and Philip E. Tetlock, "Rethinking the training of intelligence analysts," *Intelligence and National Security* 31, no. 6 (October 2016): 903-920.
[8] ICD 203, *Analytic Standards*, pp. 2-4. See http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf, accessed February 14, 2016. The Intelligence Reform and Terrorism Prevention Act of 2004, section 1019(a), specifies the five overall standards. IRTPA section 1019(b) specifies the first four tradecraft standards, the ODNI the rest. See also Mark M. Lowenthal, "Towards a Reasonable Standard for Analysis: How Right, How Often on Which Issues," *Intelligence and National Security* 23, no. 3 (June 2008): 308; Jim Marchio, "Analytic Tradecraft: Enduring Value, Intermittent Emphasis," *Intelligence and National Security* 29, no. 2 (March-April 2014): 160-168.
[9] Gentry, "Has the ODNI Improved U.S. Intelligence Analysis?" 645.
[10] Lowenthal, "A Disputation on Intelligence Reform," especially 33.
[11] Author's personal experience.
[12] Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, NJ: Princeton University Press, 1949), 74.
[13] Parts of the book later were published as Cynthia M. Grabo, *Handbook of Warning Intelligence: Assessing the Threat to National Security* (Lanham, MD: Scarecrow, 2010), 103-112.
[14] James M. Simon, Jr., "Intelligence Analysis as Practiced by the CIA," 643-644.
[15] Michael A. Turner, *Why Secret Intelligence Fails*, 117.
[16] Philip E. Tetlock and Dan Gardner, *Superforecasting: The Art and Science of Prediction* (New York: Crown, 2015), 20.
[17] Ibid., 191-192.
[18] Author discussion with people who train new all-source analysts at a large IC agency and managers of other agencies.
[19] George, "Reflections on CIA Analysis."
[20] Stephen Marrin, "CIA's Kent School: Improving Training for New Analysts," *International Journal of Intelligence and CounterIntelligence* 16, no. 4 (2003): 613.
[21] R.V. Jones, *The Wizard War: British Scientific Intelligence 1939-1945* (New York: Coward, McCann & Geoghegan, 1978), 493-494.
[22] Richard L. Russell, *Sharpening Strategic Intelligence: Why the CIA Gets It Wrong and What Needs to Be Done to Get It Right* (New York: Cambridge University Press, 2007), 124.
[23] Shlomo Gazit, "Estimates and Fortune-Telling in Intelligence Work," *International Security* 4, no. 4 (Spring 1980): 39.
[24] Ford, *Estimative Intelligence*, 83-84, 98-99.
[25] For a set of excessive and very premature claims, see Richard H. Immerman, "Transforming Analysis: The Intelligence Community's Best Kept Secret," *Intelligence and National Security* 26, nos. 2-3 (April-June 2011): 159-181.
[26] Russell E. Travers, "Waking up on another September 12th: Implications for intelligence reform," *Intelligence and National Security* 31, no. 5 (August 2016): 746-761.

Dr. John A. Gentry is an adjunct associate professor with the Security Studies Program of Georgetown University's Edmund A. Walsh School of Foreign Service. For 12 years he was an intelligence analyst at the Central Intelligence Agency, where he worked mainly economic issues associated with the Soviet Union and Warsaw Pact countries. For two of those years he was senior analyst on the staff of the National Intelligence Officer for Warning. He is a retired U.S. Army Reserve officer, with most assignments in special operations and intelligence arenas. Dr. Gentry formerly taught at the National Defense University, the National Intelligence University, and the Defense Intelligence Agency's Joint Military Intelligence Training Center. His research interests primarily are in intelligence and security studies. He received his PhD in political science from The George Washington University.

Assessing Assessments: How Useful Is Predictive Intelligence?

by WO2 John Hetherington and Wg Cdr Keith Dear, British Armed Forces

OVERVIEW

This article suggests that the failure to evaluate retrospectively the accuracy of British military intelligence predictions limits its effectiveness as an aid to commanders. It argues that it must begin to include accuracy of prediction as a metric in the assessment of the professional effectiveness of our individual analysts and our intelligence organizations and process as a whole. Doing so will provide the feedback needed to improve and may also help to delineate the limitations of prediction more carefully.

A central responsibility of military intelligence staff is to predict the future actions and intentions of enemy, neutral, and allied parties. Nevertheless, how accurate and useful are these predictions? At present, the British military would be hard-pressed to answer this essential question with any rigor. No mechanism looks at how often an analyst's or analytical team's predictions are right or wrong. A retrospective evaluation of British military intelligence assessments in order to judge their accuracy would be the first step in improving future performance. This is no more than would be expected in any other domain from flight safety to a patrol debrief. In the absence of any work examining how accurate British intelligence prediction has been, this article looks at U.S. and Canadian efforts to understand the accuracy of their predictions. It focuses first on identifying practical barriers to accurate prediction, and then on the theoretical aspect of prediction—what can be successfully predicted, or what are the boundaries of prediction?

The term "assessment" is sometimes used to indicate an analytical curation of available intelligence and other information to give a general picture to a commander. In order to remove any ambiguity, this article will use the term "assessment" to mean the summarized intelligence picture delivered to a commander—a retrospective or current perspective on events. The term "prediction" indicates that portion of an assessment which is an analyst's estimate of future enemy or third-party activity. This article covers predictions pertaining to the tactical, operational, and strategic levels largely without distinction. What is at issue here comes down to one or more intelligence personnel making a prediction about the future, and in this dimension the similarities between the levels of war outweigh the differences.

In the absence of any work examining how accurate British intelligence prediction has been, this article looks at U.S. and Canadian efforts to understand the accuracy of their predictions.

U.S.-funded research (the so-called "Superforecasters" project) examining the accuracy of those it employs to make intelligence predictions[2] found that external forecasters without access to classified information were 30% more accurate in their predictions than the professionals with access to classified materials.[3] It appears that the base prediction accuracy has still not been published. However, an earlier study found that the average expert was "no more accurate than a dart-throwing chimpanzee."[4] The best forecasters in the first round of the project, those who had contributed the most in the 30% victory, were grouped together as a "Superforecasters" team. They beat U.S. intelligence analysts in accuracy of prediction by 60% in the second round of the project and, after a further round of selection, by 78% in the third. There was clearly great room for improvement among the professional predictors in the U.S. Intelligence Community.

In contrast to the U.S. results, David Mandel's subsequent work with Canadian intelligence showed that Canadian analysts achieved very high accuracy in their predictions.[5] Mandel's work is thought to have been more accurate for the following reasons: the predictions were dealing with shorter time frames (e.g., 6-12 months rather than 12-36 months), the analysts were not given anonymity, and they were not necessarily acknowledged experts in the theory of their subject.[6]

Unless the various UK intelligence agencies and staffs know empirically or rigorously how right, or how wrong, they are, it is very difficult to *systematically* improve the systems and processes that lead to those successes and failures. Former British military intelligence officer Sean Ryan[7] summarizes the current situation within UK military intelligence admirably, writing that "…success rarely influences official appraisals of intelligence professionals. It would be impossible, as no records compare the end result to the prediction. Formal 'lessons learned' processes limit themselves to broad-stroke impressions, generic issues and localised procedures. No metrics record the accuracy of intelligence analysis on an individual, team or organisational level. Rarely is the question asked: 'Why did we get that wrong?' Intelligence analysts are structurally divorced from responsibility for the accuracy of their assessments." It is critical to know how accurate these predictions are, if they are to be improved.

PRELIMINARY DIAGNOSIS

There are a number of practical and theoretical issues with how UK intelligence staffs currently approach prediction. This article deals with the practical first. It shows the need for systematic review of predictive accuracy. It discusses the importance of language, the difficulty of assessing the probability of singular events, the overweighting of confidence in military culture, and the possibility that analysis is valued too highly over the more clerical aspects of intelligence: processing and exploitation.

Whether working at the tactical or the strategic level, prediction is central to the intelligence analyst's role.

Assessment and prediction are at the heart of British military intelligence training and practice. From the commencement of phase 2 training, through every exercise and operation, intelligence staffs are obliged to predict the future actions and intentions of enemy or neutral forces and parties. Whether working at the tactical or the strategic level, prediction is central to the intelligence analyst's role.

It matters that the British military does not know how good it is at prediction. Giving a prediction, whether in a written or oral brief, has the effect of creating a position which the intelligence staff, the command staff, and the operators may all buy into. They will see future intelligence through the prism of the first assessment, being reluctant to give it up and, through confirmation bias, search for evidence to support it. Inaccurate predictions result in poor decisions and blindness to other threats and opportunities.[8] The psychological effects are well understood: by letting an incorrect assessment into collective understanding, the ability to perceive reality and predict correctly is reduced. In the jargon, the prediction becomes the baseline while the "public commitment" makes it hard to get it out of the collective brain.

PRECISION OF LANGUAGE

Clarity of language is critical. Philip Tetlock's findings were unambiguous on this: increased precision in outcome was correlated with increased precision in prediction; loose language must be avoided. This problem is formally recognized in doctrine. JDP 2-00 para 343 provides us with an uncertainty yardstick which applies numerical values to probabilistic language.

Qualitative Term	Associated Probability Range
Remote *or* highly unlikely	Less than 10%
Improbable *or* unlikely	15-20%
Realistic probability	25-50%
Probable *or* likely	55-70%
Highly probable *or* highly likely	75-85%
Almost certain	More than 90%

Figure 3.7 from JDP 2-00 – Defense Intelligence Uncertainty Yardstick.

This precise approach is critical and must be taught and applied at all levels. In practice, its routine application appears confined principally to the higher strategic and operational levels only.

When prediction is hedged around with "'may," "could," or "possibly" without such a clear framework the results can be devastating. Tetlock shows how this phenomenon contributed to a number of poor decisions. When military and political staffs discussed the possibility of a Soviet attack on Yugoslavia (1951) or the chances of the Bay of Pigs operation succeeding (1961), those present understood radically different numerical chances for the same words. UK Defence Research recommended the adoption of these measures in 2002 to allow commanders to better evaluate the weighting of risk.[9] Retrospective analysis of predictive accuracy would provide feedback on how widely this direction has been followed.

There is some evidence that the British military may not be quite as committed to precision in intelligence analysis as it might like to claim. For example, one of the few publicly available intelligence predictions in the UK is that of a terrorist attack. MI5, the Security Service, tells us that the UK threat level for international terrorism is currently at SEVERE, meaning an attack is highly likely. The threat level has been at SEVERE or SUBSTANTIAL for over a decade, since 2006.[10] The agency explains that SUBSTANTIAL means an attack is a strong possibility while SEVERE means an attack is highly likely. There is no read-across to the DI Yardstick for "strong possibility," which leads us to suggest this is a linguistic fudge masquerading as a prediction, a public exercise in risk aversion. This view is reinforced by reading across the SEVERE probability to the Yardstick. If SEVERE does mean an attack is *highly likely*, the DI Yardstick tells us there is a 75-85% chance of being attacked. No time frame for the UK threat level from terrorism is given, which is itself a significant problem. It makes it impossible to judge whether the prediction was accurate. If the predicted time frame is taken to be 24 hours, then the UK has had a greater than 75% chance of experiencing a terrorist attack every day since 2014. This is plainly absurd, given the evidence of how rare terrorist attacks are in the UK. If politics is driving the prediction, this must be opposed. It misleads the public, acts as a poor guide to policy, and indeed it might be argued that in overweighting the strength and effectiveness of terrorist groups it serves to amplify the fear, the terror, they seek to create. If the risk aversion lies within the intelligence agencies, it must be addressed. It is in such highly charged times that rigor in predictions is most important.

It is in such highly charged times that rigor in predictions is most important.

Mandel's analysis of Canadian intelligence showed that there exists within the group a relatively clear shared understanding among commanders and analysts of what the less precise verbal formulations mean. It is highly likely that this understanding exists in the British military too, and also highly likely that it has increased over time among individual intelligence and command staffs. However, if accuracy in prediction is to be assessed, more precision is needed in saying what is meant by giving a clear numeric probability against which the analyst can be examined. Clearly, if multiple predictions are made with 90% accuracy, they should be right 90% of the time. Examining this would help analysts to recalibrate their predictions for habitual over- or under-confidence, and enable organizations to see and correct systematic biases or failures. Furthermore, in large, complex international coalitions the shared understanding between commander and staff in one area is unlikely to extend to other commands and staffs across the coalition. Rigor becomes ever more important as complexity and scale increase.

Predicting singular events against a numerical probability is more complex than predicting multiple events by extending an existing pattern or trend. Suggesting there is a 35% chance of an event occurring may help a commander plan the disposition of his forces, but if the event subsequently happens it cannot be known if it was random chance or a bad prediction. Still, the given probability can be used as part of an evaluation of the totality of an analyst's or section's predictions. Even for singular events: if 70% of predictions come to pass only 33% of the time, there is a systemic or individual problem with the approach taken (or an extraordinary run of bad luck—possible, but little harm is done by a close examination of process and procedure even when it is erroneously cued by statistical improbability). It is more helpful, then, for a commander to know how good his or her intelligence staff is in making predictions than it is for him or her to know the probability assigned to the prediction of a singular event.

ANALYSTS' BEHAVIOR AND SKILLS

It may be that the wrong habits are encouraged in our analysts. To quote *Superforecasting*: "...people equate confidence and competence, which makes the forecaster who says something has a middling probability of happening as less worthy of respect." As one study noted, people "took such judgements as indications the forecasters were either generally incompetent, ignorant of the facts in a given case, or lazy, unwilling to expend the effort required to gather information that would justify greater confidence." The plausibility of the analyst may be more likely to convince the listener or reader that he/she is right, but not necessarily more likely to actually *be* right. Pioneering behavioral psychologist Daniel Kahneman notes that "declarations of high confidence may just tell you that an individual has constructed a coherent story in his mind, not necessarily that the story is true."[11] This preference for expressing certainty rather than doubt—added to group-think—was a key element in the Iraq intelligence failure. At a lower level, Ryan notes, "In OPINT exercises, students are primarily graded on their delivery and plausibility. Rarely is there a mark for accuracy. Many exercises are deliberately scripted without a right answer. The instilled effect is a focus on presentation over content, because presentation is the tangible metric on which individuals are graded. Intelligence operators are incentivised to become salespeople rather than analysts, judged not by performance but by plausibility." Prediction should nearly

always be tentative so that both analyst and commander keep the right mind-set about such intelligence predictions; they are often assessments of very difficult and dynamic situations based on incomplete information and error, and the unexpected should be routinely expected.

Finally, it is possible that prediction is over-emphasized in intelligence circles because it is a difficult and perhaps even "illusory skill." Kahneman uses this term in connection with stock market traders, describing them as highly skilled and hard-working professionals using every scrap of information to improve their predictions but still unable to consistently beat or match the stock market. This is because, despite the high-level skills being employed, the task is usually impossible. If intelligence prediction is, indeed, an illusory skill, then its importance is systemically over-rated in comparison with the more clerical aspects of intelligence work such as collection and dissemination, which are seen as more pedestrian. A full systematic review of how accurate and useful our predictions are may teach us that displaying accurate information clearly and quickly has far greater value to all staff, from command to field.

If intelligence prediction is, indeed, an illusory skill, then its importance is systemically over-rated in comparison with the more clerical aspects of intelligence work such as collection and dissemination, which are seen as more pedestrian.

THE BOUNDARIES AND VALUE OF PREDICTION

Some important conceptual challenges to analysts' ability to predict must be considered. Are the answers to the questions that the UK asks its analysts to predict even theoretically routinely predictable? "Routine" is important here; everyone will get lucky sometimes. The difficulties in successful prediction in military contexts are legion: incomplete and incorrect information, a dynamic situation receiving constant new inputs, a very large number of possible states for each actor, with many actors and parties involved, a wide range of possible outcomes, and complex interactions of friendly and enemy forces. This leads to frequent "black swan" events (possibly more common in lower-intensity warfare): rare, inherently unpredictable, and retrospectively rationalized to make them *appear* predictable—the narrative fallacy. However, even in high-intensity warfare there are parallels in the attempts to predict singular events, like the day of an invasion.[12]

Professor Jim Storr suggests that high-intensity combat consists of a large number of elements in (1) a large number of different states (attacking/defending/delaying/regrouping, etc.), in (2) a large number of different spatial positions, which (3) change often in time, while (4) continuously interacting with other friendly and enemy elements dynamically and lethally. All this occurs in an environment in which decisions (i.e., future intentions) will be made in conditions of great—sometimes mortal—danger. In addition to all of this, each side will have imperfect information about both itself and the enemy. Although describing high-intensity combat, all the situations and levels of combat that our intelligence staffs must assess will share these attributes to a large degree. In these circumstances, which Storr categorizes as "unutterably complex and [which] do not appear to be heavily determined," some might argue prediction is impossible. It is certain that it is very difficult.

Military intelligence staff training tends to be scenario-based. In such an approach a "GENFORCE mentality" can creep in: this is where an exercise enemy is used, which has stereotyped tactics and operates in an unrealistic "zero-friction" environment. Accurate "prediction" in these circumstances is analogous to solving a puzzle: finding the key bit of information will unlock the solution. Unfortunately, this tells us little about the ability to predict a real enemy operating in a dynamic and uncertain environment.[13]

Lieutenant Andy Mellows' excellent paper published in the UK Intelligence Corps journal *Cognito* examining intelligence and decision-making contains a suggestion for improving scenario-based training. Mellows suggested that exercises are created which give real situations from the past and then test intelligence staffs' ability to predict the outcomes, measuring their performance against the actual outcome.[14] Such a thoughtful approach to improve and further professionalize intelligence assessment and prediction is precisely what is needed and we could provide part of the answer. However, if Professor Storr is correct, caution is necessary in how this idea is implemented. Even the attempt at retrospective prediction based on clear historical example may fall victim to the narrative fallacy—assuming the outcome observed was the most probable, or even inevitable. If the limits of what *should* be predicted are unknown, and the ability of our analysts and organizations to make accurate predictions is similarly unclear, the value of intelligence predictions is equally uncertain.

As a second-order effect, this uncertainty calls into question the usefulness of IPB/IPE and doctrinal templates and similar products in real warfare. Dr. Storr

suggests that such products are rarely updated or even referred to after initial planning; hence, there is no way of knowing if they aided accurate prediction.[15] Even more damningly, then-MG Michael Flynn, senior military intelligence officer in Afghanistan, said in 2009: "The intelligence community's…culture is strangely oblivious of how little its analytical products, as they now exist, actually influence commanders. It is also a culture that is emphatic about secrecy but regrettably less concerned about mission effectiveness."[16] With such enormous difficulties the Intelligence Community must do everything it can to improve accuracy in prediction. It cannot afford not to.

This article has attempted to diagnose some of the practical and theoretical problems that inhibit or prevent accurate intelligence prediction. It will now briefly examine some objections to the diagnosis, answering them before turning finally to some recommendations.

OBJECTIONS

Certain objections could be made to various aspects of the diagnosis. On the more practical side it might be argued that there is (1) no discontent with current intelligence practices and therefore no problem; or (2) a shared understanding at all levels regarding the language used, both in the operations and intelligence staff making and using predictions, and with the audience for these predictions. Some may argue that (3) confident delivery is not the same as the analyst's confidence in the prediction, and does not lead deterministically to a commander's confidence in the prediction. All of this could be determined by a systematic retrospective analysis of intelligence predictions and the command and tactical decisions based on them, or made in contradiction of them.

Others might suggest that both command and intelligence staffs are happy to deal in uncertainty and neither is unduly concerned to over-defend stated positions. Again, an audit would reveal how true this is. A brief acquaintance with psychology would suggest that it is unlikely to be true.

Some have suggested that there is not time to be more precise in making intelligence predictions and/or there is insufficient time to go back and analyze their accuracy. It was noteworthy that neither Tetlock nor Mandel suggests that more accurate predictions take longer to make, but in fairness it must be considered that the conditions in which the predictions were made were different. It is possible that the extra linguistic and probabilistic precision requires a change of habit rather than a longer time in formulation of the prediction. Making sufficient time for the retrospective analysis of predictive accuracy may be more difficult. Staffs may genuinely not have the capacity to do this. It may be advisable, therefore, for an outside agency or a different staff to carry out the analysis. However, it certainly is not impossible to achieve; economists are already rated on their prediction accuracy in the U.S., where Bloomberg ranks them both quarterly and annually.[17]

A notable challenge is that a prediction can be confounded by being right. That is, an analyst may be thought to have made an incorrect prediction when the action was in fact prevented by friendly activity...

A notable challenge is that a prediction can be confounded by being right. That is, an analyst may be thought to have made an incorrect prediction when the action was in fact prevented by friendly activity, perhaps activity directly cued by the commander's desire to prevent the predicted outcome from occurring. The difficulty of friendly operations changing future enemy activity and so invalidating earlier predictions is clearly a valid objection. To a degree, however, this could be incorporated into the evaluation of the prediction; e.g., was any action taken based on the prediction? Surely one of the most powerful indicators of the utility of our predictions is how frequently they cue action to forestall the predicted outcome. Thus, this might be a key metric of the utility of the predictive intelligence. Again, it is a metric that is not currently tracked. Furthermore, any action taken should yield further information to confirm or refute the prediction's accuracy, again providing feedback to allow the analyst to improve in the future.

This article notes a final practical objection: some suggest the last decade of war has redressed the balance between assessment and the other parts of the intelligence cycle. While a theoretical objection might argue that, given sufficient current and doctrinal information, plus sufficient analytical power, complex tactical movements can be predicted.[18]

The truth is, most of these objections are impossible to refute completely and are equally difficult to uphold—the answers are unknown and are worthy of discovery through examination of our predictive accuracy. At best, commanders may gain greater confidence in their intelligence staffs; at worst, it may be discovered that some working assumptions are fundamentally unsound.

HOW DO INTELLIGENCE PREDICTIONS IMPROVE?

Some recommendations arise from this article's analysis. First and foremost, **predictions must be subject to systematic, continuous review both on a collective and individual level**. Such a review might be most effective if impartial and thus it should be led by a neutral third party—another staff, a commercial organization, or an academic partnership. The UK needs to know how good its intelligence staffs are in order to adapt its training and its approach, and analysts need to know how good they are as individuals in order to improve their individual performance.

To do this, the yardstick must be applied universally, and the UK must begin to look at the accuracy of intelligence organizations, sections, or individual analysts' predictive performance as part of such an assessment of their professional effectiveness. The simple measure of recording and then subsequently verifying the accuracy of each analyst's, section's, and organization's predictions should begin to bring a number of "quick wins." For example, (1) the accuracy of the forecasts of the intelligence staffs will be known, and in itself is a useful aid to planning; (2) once they are known there will be a measurable incentive to improve the accuracy of the forecasts: (3) this baselining will create an incentive to minimize over-confident predictions and the subsequent damage they do to the commander's mental picture of events; and (4) command staff may become happier with less certainty in their intelligence staffs' assessments and will gain greater confidence in analysts based on accurate results, not plausibility of presentation. Additionally, (5) intelligence and command staff will be better able to understand broadly what can be predicted, and to what level of accuracy, while certain things may be ruled out as definitively unpredictable—in the jargon, the boundary conditions for successful prediction in military contexts will be discovered. Finally, (6) the utility of certain staff procedures can be tested by how much or how little they contribute to the accuracy of subsequent predictions.[19]

The operational record from Operations TELIC, HERRICK, ELLAMY, and perhaps even SHADER, as currently stored in electronic format, could readily enable an analysis of the accuracy or otherwise of recent intelligence predictions at given levels of detail and time period. It might also enable the Intelligence Community to understand the differences in outcome when predicting events at the tactical, operational, and strategic levels. It must be independent and would be well suited to a military-academic partnership. The successful approach of Tetlock and the Intelligence Advanced Research Projects Activity (IARPA) program could be adopted by identifying who the British "Superforecasters" are and grouping them together, creating a sort of "special forces" of forecasters.

The successful approach of Tetlock and the Intelligence Advanced Research Projects Activity (IARPA) program could be adopted by identifying who the British "Superforecasters" are and grouping them together, creating a sort of "special forces" of forecasters.

Some recommendations emerge from the studies of Canadian and U.S. intelligence which the British military would be wise to adopt. While Tetlock's research found most professional forecasters to be unreliable, he did find certain people who reliably made accurate predictions and identified the personal characteristics they possessed. These are listed for simplicity:

- They made specific measurable forecasts.
- They constantly adjusted those forecasts in the light of new information. This information might only shift their prediction a few percentage points (the best forecasters were the most granular).
- They were not emotionally tied to their predictions.
- They were not adherents to a big, over-arching political ideology which explains everything.
- They broke down problems into constituent elements.
- They were comfortable with basic mathematics.[20]
- They improved as forecasters as they gained experience.

These might form the spine of any future analytical training and/or assessment of individual or collective competence.

In response to the conceptual challenges to prediction, its conditions must be made easier by reducing the number of elements and thus increasing the degree of accuracy in space and time. Broad patterns will generally be a lot easier to predict than anything which requires detail and precision, and Storr[21] says this is what expert military decision-makers, i.e., good commanders, actually do.

SUMMARY

This article suggests that the UK must seek to replicate, expand, and institutionalize nascent efforts in the U.S. and Canada to improve the accuracy of intelligence staffs' predictions. The first task must be to establish how good intelligence staffs are at making predictions. The second must be to make adjustments to training, processes, and procedures based upon what we have learned. Tetlock and Mandel have provided an invaluable pointer to where we need to go. It is up to the Intelligence Community to take the actions to get there.

NOTES

[1] General Colin Powell, Chairman of the Joint Chiefs of Staff, "Intelligence Reform," 2004, http://fas.org/irp/congress/2004_hr/091304powell.html.

[2] These were strategic/geopolitical assessments.

[3] David Ignatius, "More Chatter Than Needed," 2013, https://www.washingtonpost.com/opinions/david-ignatius-more-chatter-than-needed/2013/11/01/1194a984-425a-11e3-a624-41d661b0bb78_story.html.

[4] And, in the case of media pundits, worse. . .

[5] David Mandel, *Accuracy of Intelligence Forecasts from the Intelligence Consumer's Perspective*, Defence Research and Development, Canada, 2015.

[6] Philip E. Tetlock & Barbara A. Mellers, *Judging Political Judgement*, Proceedings of the National Academy of Sciences of the United States of America, July 2014.

[7] Sean Ryan, "Finding the Right Answer," *The RUSI Journal*, Vol.160, Issue 4 (2015); 50-58.

[8] Jim Storr, *The Human Face of War*. Professor Storr, former soldier and military scholar, mentions an example of a J2 cell literally making up an attack. The authors have personally witnessed similar phenomena several times.

[9] Robert Desimone and David Charles, "Towards an Ontology for Intelligence Analysis & Collection Management," Qinetiq 2002 https://www.aiai.ed.ac.uk/project/ksco/ksco-2002/pdf-parts (paper 11).

[10] https://www.mi5.gov.uk/threat-levels.

[11] Daniel Kahneman, *Thinking, fast and slow*. Macmillan, 2011.

[12] There is a good example from the Yom Kippur War: http://gladwell.com/connecting-the-dots/.

[13] Ryan, "Finding the Right Answer," is similarly skeptical.

[14] Andy Mellows, *Embracing Intuition: How an Understanding of Naturalistic Decision Making Research Can Improve the Provision of Tactical Intelligence*, published in *Cognito*, 2015.

[15] Storr, *The Human Face of War*, identifies targeting boards, IPB, and synchronization matrices as falling into this category.

[16] Michael T. Flynn, Matt Pottinger, and Paul D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan* (Voices From the Field Series, Center for a New American Security, 2010), quoted in Ryan, "Finding the Right Answer."

[17] Bloomberg, *Bloomberg Best (and Worst): Best on U.S. Economy: Forecasters*, https://www.bloomberg.com/graphics/best-and-worst/#best-on-u-s-economy-forecasters accessed 29 January 2016.

[18] The difficulties encountered in more general political, economic, climatic, and even sports forecasting invite a certain skepticism here.

[19] Tetlock, *Superforecasting*, is useful for its scoring system for those interested.

[20] Mathematical awareness appears to have a basic function in preventing an analyst holding logically incompatible views.

[21] Op. cit.

Warrant Officer Class 2 (WO2) John Hetherington is a member of the British Army's Intelligence Corps. A linguist fluent in Arabic and Pashto, he has served in translational, command, leadership, and analytical positions in Northern Ireland, the former Yugoslavia, Iraq, and Afghanistan during a career spanning 18 years. This includes several deployments working directly as an analyst in combat and operational intelligence roles, in addition to tours in IMINT, SIGINT, HUMINT, and field security units. He has also taught combat intelligence to unit intelligence cells. John has a long-standing interest in psychology and war, presenting on psychology's application to tactical planning and execution both in his current role and externally. He is particularly concerned with how insights from psychology can best be used to increase operational and tactical performance.

Wing Commander (Wg Cdr) Keith Dear is an RAF intelligence officer and CAS Fellow in the Royal Air Force. He is a candidate for the DPhil degree at Oxford University's Department of Experimental Psychology and Research Associate at Oxford's Changing Character of War Programme. His professional experience is in intelligence, surveillance, and reconnaissance (ISR), analyzing human behaviors and systems in the UK. He has served an exchange assignment with the U.S. Air Force and has deployed on multiple operations overseas. In 2011 he was awarded King's College London's O'Dwyer-Russell Prize for the highest MA grades in his studies in Terrorism and Counterterrorism, focused on the efficacy of leadership targeting. His published work, "Beheading the Hydra," remains the Journal of Defence Studies' *most downloaded article. Prior to coming to Oxford, Keith was part of the UK's cross-government Counter-ISIL Task Force and headed the targeting cell at Permanent Joint Headquarters. He is a founding member of the Defence Entrepreneurs' Forum (UK). His current studies examine the effect of surveillance on behavior.*

Technology in Foreign Intelligence Gathering

by A1C (USAF) Candace N. Stevens

When a "loss of innocence"[1] arose from events such as Pearl Harbor, this changed the way Americans thought of national security and instilled in the United States a "complex mix of diplomacy, military strength, and intelligence that would now frame and equip America's central role in international affairs."[2] The necessity for technology is crucial in keeping up with other potential threats from other countries—or the advancements of more neutral countries—yet, many of the crucial moments of innovation tend to be disregarded or placed into a catacomb-like spot in history. New technological advancements replace old building blocks which helped their creation and, consequently, become regarded as just a phase in important concepts. This research attempts to reflect on instances of past achievements as not only building blocks, but to hypothesize on these effects and indicators for what the future might hold.

The available research strives to comb through and vet mass amounts of data related to technology in the Intelligence Community (IC), and hone in on important items or "data corpus"[3] relating to foreign intelligence work conducted in the U.S. with the help of technological innovations. At times, the exact use of technological devices in the IC proves covert, yet speculation can be made upon use in foreign intelligence work. Going through different "lenses"[4] of research already conducted, this given research will piece together concepts with categorizing, labeling, and the use of "open coding."[5] Particular interest is taken in terms which encircle (and practically define) separate decades of technology. By compiling historical instances, this research attempts to compound important mindsets and dialogues over the years to dissect and compare with modern innovation, with a hypothesis that technology has had great effects on foreign intelligence work in the United States.

Ranging from topics and physical motifs sprouting during and after the 1960s, discussions include different professions, concepts, platforms, and emergent issues coming out of a process of a more or less technological enlightenment in the IC. Numerous parallels also manifest within the examination of programs spawning from 1980s technology, particularly DARPA's[6] literature on technology in the intelligence field, let alone foreign intelligence work, which is sporadic but can be dissected for review. Programs akin to ECHELON[7] stand next to more recent models and issues snowballing from increasing abilities that come out of technological interconnections, such as "cyber espionage"[8] and social media. As abilities with different technologies and cyber realms become strengthened, so do concerns. Further analysis and findings are reviewed with programs bordering with "Trailblazer" and "TIA"[9] that attempt to expose and defend against threats. This research specifically tries not to form opinions surrounding technology being used in these fields similar to foreign intelligence, merely how it could potentially provide assistance.

Programs akin to ECHELON stand next to more recent models and issues snowballing from increasing abilities that come out of technological interconnections, such as "cyber espionage" and social media.

The incorporation of technology into everyday life has only intensified and is now becoming an intrinsic part of operations; thus, it must be considered for further inquiry. The necessity to analyze this potential is key. Propositions in the future which allow for the control of aircraft by "devices such as [an] iPhone,"[10] in coming years, is strongly indicative of destruction that could come, with ease, in the palm of an individual's hand. With this conceived power, looking at past developments in technology and effects it has on U.S. foreign intelligence work will help efforts in understanding the future of technology in these fields and the meaning of devices that have evolved immensely in such a short time.

LITERATURE REVIEW

By researching technology in foreign intelligence work performed by the U.S., the amount of material readily and publicly available does not fully encompass every detail regarding this relationship. The elusive nature of this work does not mean that information is not out there, or therefore that inferences cannot be made using unclassified information. It is important to understand different points in history in which technology shapes the IC (especially foreign intelligence gathering and analysis) to the position it is in today, and what can be known. The sources offering information on this subject, found within, insinuate parallels to past inventions and concepts; however, the association of technology with foreign intelligence work continues beyond the confines of this research.

The appearance of Cyber Intelligence, or "CYBINT," points to growing trends of interests in cyber-related concepts involving intelligence.

Moving forward from surveillance devices like Corona in the 1960s,[11] the expansion of intelligence technology continues. For the first time, U.S. foreign intelligence efforts could physically see threats from countries such as Russia, inevitably sparking desire to continue work with technological devices. This work ushers in the collaboration intelligence takes on with modern technology. Literature on labor forces within the IC can be found in professions revolving around technology. These "intelligence disciplines"[12] perpetuated the dialogue between the IC and technology elements in these career fields that could harness intelligence in new ways. With technology, the fields of existing and new types of intelligence have expanded to include HUMINT (Human Intelligence), ELINT (Electronic Intelligence), COMINT (Communications Intelligence), SIGINT (Signals Intelligence), IMINT (Imagery Intelligence), OSINT (Open Source Intelligence), MASINT (Measurement and Signature Intelligence), GEOINT (Geospatial Intelligence), and TECHINT (Technical Intelligence). One "tradecraft" in particular explores a newer area of intelligence.

The appearance of Cyber Intelligence, or "CYBINT,"[13] points to growing trends of interests in cyber-related concepts involving intelligence. As a result, it is imperative to look at how technology has introduced itself into the IC—particularly affecting foreign intelligence—and why it matters. Additionally, the IC incrementing technology into practices appears to be more than mere interest in innovation. Technological advancements prove to hold vital mainframes in which enemies strive to harm. Readily apparent in recent times has been the determination countries have to spy on each other, as can be seen by China in 2013 penetrating U.S. cyber realms.[14] Casting aside demonstration of technological and cyber power, different countries have come to lean heavily on these same systems as "many countries' vital infrastructure, nuclear power plants, water, gas, electricity, traffic communications and other necessary public bodies such as hospitals rely on computer systems."[15] The inner workings of countries now depending of these systems (for many reasons, including reconnaissance and defense) is cause for growing interest in technology. However, importance also lies in how this gradual dependence became what it is today throughout time. Not only because it is important to look at any potential threat, the use of technology enables U.S. intelligence with the capability of detection and potential opposition.

The 1980s was a major catalyst for some developing programs used today. Instances of major technological developments can be seen throughout this time period. Early systems such as ECHELON[16] massively altered the degree of how the United States conducted surveillance. Faintly similar to more popular and recent scandals involving Edward Snowden with PRISM,[17] ECHELON was similar in the way it "intercept[ed] very large quantities of communications… using computers to identify and extract message of interest."[18] With other achievements spanning more recent years, DARPA is a major player in technological development for defense and civilian contracted work. In the 1980s, DARPA "laid the groundwork for today's Internet" with the "creation of protocols used for interconnecting networks across the Internet,"[19] with the so-called ARPA Net. The company, known for both civilian and defense contract work, innovated in programs such as "automated speech recognition (ASR), machine translation (MT), and information retrieval technologies; Department of Defense (DoD) organizations have [also] employed foreign media monitoring (FMM)."[20] DARPA has enhanced computational ability and technology since the 1950s and continues work today in "smart weapons, UAV's and ground robots."[21] Changing times have required a turnover of technology and henceforth have demanded the introduction of new tactics with evolving threats.

Changing times have not gone unnoticed in other sectors of the United States. The sometimes threatening nature that the cyber realm presents catches the attention of political leaders. With the increasing concern even in political sectors, former Director of National Intelligence James R. Clapper stated that "cyber espionage and

intrusions are growing every day…[and] siphoning off our intellectual property to hackers and nation-states alike."[22] While portions of cyber threats are being handled through clandestine defense, others can be seen in plain sight. This threat has come to the point of appearing in common social media elements used by regular individuals. In fact, terrorists use platforms like Facebook, Twitter, and YouTube, and online publications such as *Inspire* magazine that "extend well beyond any one type of device, across the continuum of both hardware and software communication platforms."[23] Finally, the foreign threats which were once battled largely behind the scenes and outside the knowledge of regular individuals are now in plain sight.

Filtering and policing social media, and possibly even more personal data, produce other potential issues. "Data mining"[24] presents meanings and limitations to different researchers. Some scholars see this term as a way to filter through potential threats, a means to an end.[25] This interpretation sees this process as another opportunity to thwart individuals meaning to inflict harm; however, other researchers perceive that data mining is a violation of privacy. Many injustices can seemingly be committed due to the fact that legislatures can lag when technology produces concepts that can completely change the meanings of laws. Examples can be seen in sections of the USA PATRIOT Act which go against previous Fourth Amendment rights.[26] Modern threats such as terrorism come with intentions to address these threats promptly, leaving laws to be held against interpretation of unprecedented situations. The temporary oversight of a legislature in needing to catch up, so to speak, harbors potential gray areas that lie behind the laws. Viewing these negative (or even less than positive) aspects of Technology along with good shows a duality of this evolution that is not completely clear cut, or right or wrong. Exemplifying dissenting viewpoints helps in assessing the true measurement of the effects technology has on foreign intelligence work, even if the issues are social in nature. It is important to consider factors outside intelligence work, which can form policy and be structured by social opinion. These same viewpoints can change how technology is used in the future. Consequently, combating foreign threats has come to the attention of many and has evoked fascination with the same technological devices that are used.

The ever-growing utilization of drones brings with it equally important issues to come, as other nations begin to enter this field. According to the article "Emerging Drone Nations" by Shashank Joshi and Aaron Stein, the development of this device is not new, but traces back to World War II, and more popularly in the 1950s "experiment[ing] with drones for high-altitude reconnaissance of Soviet missile, nuclear and military facilities."[27] Despite the concept of drones not being recent from a U.S. perspective, the increased usage of unmanned aerial vehicles (UAVs) by other countries points out the issues that countries, including the U.S., must face and continue to deal with as this device is used more frequently. An article published in 2013 estimated there were as many as "56 types of drones across more than 30 countries."[28] Undoubtedly, these numbers have grown since then. The article introduces modern issues that arise with countries experimenting with drone operations. The article points out concerns countries will encounter, including "cost, human material infrastructure, the problem of air superiority, the development of a doctrinal and legal framework, and the impact of proliferation."[29] Considerations such as cost and social issues indicate this technological development is not as simple as many perceive it.

Aside from the perceived benefits of drones, to include in combat, there has been a stigma associated with this device as it has "become synonymous with a capability: targeting individuals."

In regard to the financial obligation UAVs present, the authors expound upon common misconceptions that this device is inexpensive compared to other aircraft.[30] Given not only the basic cost of the aircraft itself, but the personnel required to maintain and operate the aircraft throughout the course of missions, drones prove to be financially taxing to the countries utilizing this device in operations.[31] Among other issues pointed out in the article, conversations on the use of drones have become popular in debate over programs such as the CIA's "targeted killing[s]."[32] Aside from the perceived benefits of drones, to include in combat, there has been a stigma associated with this device as it has "become synonymous with a capability: targeting individuals."[33] The sanctioned use of drones is fairly new in terms of established legal parameters. In terms of U.S. legislation on drone policy, the Obama administration undertook some efforts to police the use of drones,[34] but there has yet to be a major establishment of law for this unique set of surveillance, reconnaissance, and defense devices. Because the roles of this device continue to develop and change, the legalities and social implications associated with drones still need to be worked out.

As with the drone program, and other examples of high technology, there is much that is still unknown about foreign threats. Technology brings with it challenges in

foreign intelligence gathering and analysis for the U.S. Quantitative research on these challenges is presented on social media websites like Twitter.[35] Dually, the implications of terrorist threats also convey the ability to use this site as a means to acquire and analyze foreign intelligence. Despite this knowledge, although clandestine operations may be channeled through sites like Twitter, unclassified research cannot provide direct accounts of data on these terrorist threats. A large portion of data collected indicates research gives resurgent Twitter accounts "independent data points."[36] Therefore, it is unknown how large this threat is. This begs a question as to a larger number of terrorists unaccounted for on sites akin to Twitter. The research in this article evokes the possibility that more investigation, research, and intelligence gathering is necessary to learn more about developing terrorism issues.

Although research on technology in foreign intelligence gathering and analysis spans widely outside available articulation, the literature available on this topic suggests a pattern that discerns challenges and benefits yet to come in a realm that is becoming more reliant and of greater importance on using technological innovation for success.

METHODOLOGY

Approaching the continual developments of technology in the Intelligence Community, especially in foreign intelligence gathering and analysis, requires specific parameters of research. The possibility of losing focus on tangent subjects is very strong and harbors the reality of how challenging the subject is to pin down. Assessing a hypothesis that "technology is a major factor affecting foreign intelligence gathering and analysis" brings questions as to exactly what instances and examples sufficiently explain how technology has changed in the span of less than a century.

Scholastic conversation involving the topic of technology in intelligence diverges primarily beginning with the Cuban Missile Crisis in the 1960s and the early years of the Cold War.

In researching technology throughout the history of foreign intelligence, much time is spent finding key words which would offer potential sources. The methodologies approached with the impact of technology in foreign intelligence work become searching relative terms of "cyber," "technology," and "terrorism," which evoke relatively modern discussions.[37] Scholastic conversation involving the topic of technology in intelligence diverges primarily beginning with the Cuban Missile Crisis in the 1960s and the early years of the Cold War. The implementation of technology such as Corona[38] in the 1960s led to inquiries about more modern surveillance devices. Technology and foreign intelligence work coincided and collaborated during the emergence of the Cold War and continues with a motif of surveillance. Utilizing qualitative research methods including "open coding" (with the term "surveillance") proved fruitful in discovering this type of technology in further decades.[39]

Evolving into different intelligence professions that directly use technology,[40] the flow of information increases as modern inventions of intelligence appear in more scholarly conversation (though at times only to a certain extent). The question of popular topics relating technology and foreign intelligence work conducted by the U.S. became a pillar of research. The requirement to condense information derived from different data sources discovered and conversations conducted about the relationship. Compiling and categorizing the massive amounts of data found surrounding intelligence technology, a consensus of major topics includes (and subsequently guided research): technological innovation, jobs and "tradecrafts,"[41] and the modern social impact of the relationship. Now popular "lenses"[42] of foreign intelligence involved terms encircling terrorism—in its different forms and meanings—in this case technology. From this research, questioning the increase in the relationship of technology and foreign intelligence work presents paths entrenched with opinion and superfluous information.

The efforts of technology are often merely an afterthought to the intelligence work presented after the fact. Therefore, this research attempts to piece together cases which showcase this relationship that is apparent, yet neglected as a whole in scholastic conversation. The methodology of this research proved by no means linear, yet the flow of information is directed with qualitative and quantitative analysis and ranking. Pertinent information is often inserted into sources which are often tangential, opinionated, and by-products of human influence. In essence, a large portion of the research carried out follows information that is saturated in content, but this same content contains pertinent information. As a solution, more specific tactics will be necessary in finding useful information regarding narratives of technology in intelligence work.

Coding data will attempt to combat regurgitating aforementioned superfluous data and develop a potential linear path of technology over the last 60 years. Particularly,

using the different verbiage of scholars known as "in vivo coding" interlaced with finding the important issues discussed or "data corpus," the task becomes easier in searching for, as well as organizing and analyzing, linear guides. [43]As a result of fundamental inquiries, many topics surface including aforementioned early technology in the 1960s, computer technology emerging in the 1980s and 1990s, and current technology used today in intelligence work. Among these instances, unique variables surfaced with important highlights of technological advancements in the Intelligence Community.

Evolutionary to U.S. work in foreign intelligence, in addition to this research, many questions arise from the development of technology as it has become now versus remedial intentions. Within the realm of digital innovation, technology itself proves to be incomplete, in theory, because it is still developing today. Specific instances of case studies potentially are limited due to the fact that U.S intelligence continues to utilize and conduct work within computer programs. In light of the myriad uses technology has, a need to separate technology mainly in discussion of U.S. efforts in foreign intelligence work is necessary. However, the consideration of how technology is used by threatening forces is equally necessary in understanding the evolution of technology in intelligence work. Information extracted from different sources about technologies and capabilities of U.S. intelligence proves daunting. Because it is partially open-source information that is guarded from foes, research into this relationship between technology and foreign intelligence efforts by the U.S. can only extract information that is available, begging the question of how much information is hidden. This research will attempt to seek out a linear path of how technology has affected, and continues to affect, modern U.S. foreign intelligence efforts.

ANALYSIS AND FINDINGS

Specific programs and concepts relating to intelligence work in general prove to entail in-depth research of specific periods. Herein, the early 21st century shows a pattern of technological use in programs during this time, and is important in dissecting a hypothesis that technology has had major effects in foreign intelligence work conducted by the U.S. This in-depth research shows these important developments in technology, and is in certain regards a gauge of the narratives of technology over time, as well as more recent roles it plays.

Transitioning from the technological advances of the Cold War, more recent programs now show trends in a potential direction the U.S. is headed in foreign intelligence work. The implied meaning of "recent" is within the last twenty years directly following 9/11, when homeland security peaked, creating new measures of protection.

Collective change brought a "shift from the USSR-era eavesdropping technology…to technologies designed to monitor telecommunications in the cell phone, fiber optic cable, and Internet environments."

Collective change brought a "shift from the USSR-era eavesdropping technology…to technologies designed to monitor telecommunications in the cell phone, fiber optic cable, and Internet environments."[44] As a result, increased efforts in surveillance came with government influence, not to mention interest in programs reflecting technological capabilities during these times. In 2001 a project called "Trailblazer" reinforced the efforts of NSA in analyzing "the huge bodies of data of global telecommunications systems."[45] It is worth noting the similarity of this program with later efforts involving NSA mentioned earlier, which have been going on potentially with different technological platforms. In addition to interest in domestic surveillance, government programs came to light on foreign and terrorist threats involving the U.S. via digital means. Despite appearing rudimentary now, the programs during this time harken back to efforts to weaken the advancements of foreign threats, yet now these efforts are parallel to topics more familiar in the 21st century. The "TIA" (Total Information Awareness) program began to "apply information technology to identify specific terrorist threats."[46]

For the first time, since the Internet became a more widespread concept, internationally, the ability to view activity across the globe was more attainable. This growing ability allowed the U.S. government to see foreign activity and potential terrorism from the domestic front, thus proving an increasing partnership between technology and U.S. foreign intelligence work. Related to the earlier "Trailblazer" project, "Turbulence" enabled government agencies to "examine Internet for networks possibly being used by terrorists…to plan terrorist acts."[47] Similar to the technological advancements in early surveillance technology and satellites, the U.S. was able to view the activity of other countries. However, unlike viewing these threats from above with photographic means, the U.S is entering into more modern battlegrounds. The Internet is a completely new arena in which threats come out and are fought against. Moving along from descendant technology of the Cold War came

new abilities in foreign intelligence gathering and analysis that, since the 1950s, could be conducted on U.S soil. However, now foreign intelligence gathering and analysis have the capability to perform at a new level through technology. The evidence in these programs is dated and will need to be supported by more recent examples to show a linear path, yet this source proves to be an excellent bridge between technologies in previous years, as it is being directed at more modern threats such as terrorism, and will be helpful in exemplifying advancements of technology.

More recent articles are continuing discussion of technology in the intelligence field. Although it slightly differs from specifically foreign intelligence gathering and analysis, important comparisons can be seen as technology affects this field potentially in a similar manner. Just this year, debates of the fate of technology in intelligence work continue. Without a doubt, the recent article "The Future of the Intelligence Analysis Task" by Nick Hare and Peter Coghill discusses possible "foresee[able]" ways "technology is affecting and will continue to affect the drivers that determine how that task (analysis) is performed."[48] The key term in this article is "foreseeable"; however, the conceivable possibilities this piece brings forth could be an indication of a positive role technology can play in U.S. foreign intelligence efforts. Technology has a part in what the author refers to as "information-consumption patterns" that enable intelligence analysts to go through sites such as Facebook, Twitter, Google, and YouTube for pertinent information.[49] In turn, possessing the ability to wield intelligence in these types of sites also provides the opportunity to simplify the interface of receiving and giving information in other areas.

The authors present an indication that "the information that analysts need is increasingly transient, in streams, with a mixture of machine and human indices tying it together."[50] Continual use of technology in the intelligence field indicates a linear relationship that continues to grow with positive effects. To discuss the potential of technology enhancing the work of analysts within the Intelligence Community points toward an increasing belief in the ability of technology now and in upcoming years. This piece is detrimental in proving a link still stands in a chain from the 1960s to now. After analyzing decades of examples of the IC implementing technology with different processes, this piece concludes with a strong belief that technology continues to help and impact intelligence work (particularly foreign intelligence) today. With the increased amount of work that can be performed with technology, the human work of analysts will still be necessary to help "test the hypotheses" with which machines can assist.[51] Theoretically, analysts would be assisted by technology and in a role of "mutual support."[52] In an unknowable number of years to come, this piece hypothesizes the ability of technology to help analysts and "minimize their cognitive load" so they may in turn better assist "customers" requesting their services.[53] Poignantly, the author expresses that, despite some older individuals in the intelligence field who relied upon themselves, not technological help, of which "secretly hopes that IT (information technology will quietly go away is in for a severe disappointment."[54] There is a pinpointed inference that technology is not going to disappear in the IC; therefore, its increase is likely to occur. Although much of this article infers theoretical applications of technology, it shows that regardless consideration of the IC showing interest in utilizing the coming developments of technology to come, and invariably this use trickles down to foreign intelligence efforts.

These two recent components of research on technology in foreign intelligence gathering and analysis help solidify the belief that this relationship is not faltering with years of attempts and developments. Instead, these sources of information indicate the hypothesis is correct in theorizing that technology has had major effects on U.S. foreign intelligence work, and does not show indications of ending, so long as these same conditions and patterns continue. With the same vigor individuals had in preventing or opposing major threats to the U.S. throughout history, this energy could help in the advancements and application of fields such as technology in foreign intelligence gathering and analysis. Technological application in the intelligence field is not where it could be, nor should be, but is nonetheless reflecting its increasing use in this work.

CONCLUSION

The available research conducted on technology in U.S. foreign intelligence work, or even inside the Intelligence Community in general, is incomplete for at least two possible reasons. The necessity for technology in this line of work is relative to conflicts occurring in past decades. Specifically, if not for rising threats, there would be no encouragement to construct these devices which have assisted in struggles to keep up with, and maintain eyes on, adversaries. For this reason, there may be classified details of deterring threats that may not be sufficiently handled. As a result, the likelihood of devices and concepts that provide for fruitful research continues to be hidden from public view. Although this is not the panacea for productive research, scopes of future research may need to hone in on available subjects. Consequently, a second possibility for the incomplete nature of the given topic presents itself. Technology is not ending for foreign intelligence work in the U.S. Intelligence Community.

Based on current research, technology progressively intertwines with intelligence work more and more. In turn, it is then imperative that research be conducted on the existing

accounts of past technological innovation, how it synchronizes with modern times, and what is happening today. Moving forward with future research on the effects technology has on foreign Intelligence gathering and analysis, the use of technology must not be seen as a tool to be taken for granted, for the IC has functioned before. To assess this effect accurately, importance must be given to the innovations which affect modern intelligence practices.

The synopsis behind the project revolved around historical innovations of technology in relation to foreign intelligence gathering and analytical work. The research attempted to tie together key points and events that would not otherwise be specifically considered. Further contemplation was posed upon possible approaches that clandestine operations might take, with distinct deliberation of foreign intelligence work in the United States. Initial research began with general inquiries into technological innovations in the IC and evolved into filtering and honing in on instances that could pertain to operations involving U.S. foreign intelligence. Ultimately, this provided research efforts with substantive connections to be made between different decades of technological inventions relative to the topic.

Strategy trailing behind the research involved constant interpreting of moments over 60 years of relative technological history and developing conjectures on how it might be applied to intelligence being gathered and analyzed in foreign efforts. No amount of interpretation or conjecture of technological innovation is possible in determining the exact number or frequency of these devices, programs, or concepts that are used by the IC, yet for scholastic purposes it is the only alternative for relinquishing this type of information. The actual results of the research conducted revealed some interesting data.

The effects of the relationship between technology and foreign intelligence gathering and analytical work showed, for the most part, a positive result; however, the extent is unknown. Based on the results found, technology has seemingly inflicted a positive change upon intelligence work, more specifically foreign intelligence, but potential issues lurk if not faced. Instability comes with utilizing electronic devices, especially ones with the ability to interconnect across the world (i.e., technological innovations such as the Internet). For the aforementioned reasons, these devices may be susceptible to unforeseen contingencies. Given these issues, the research shows instances of important milestones, but is not to be considered the final conversation. Surely, issues will expand further for researchers than this focus or conversation. Instances of past events cannot possibly explain every detail, as this is impossible and the effects continue to evolve today. The research did provide sample concepts to consider in schools of thinking about this topic, and strives to pursue the goal of more conversations being held in the future. Dialogue is nonetheless added and potentially missed connections discovered, indicating the future applications of technology in surveillance, reconnaissance, and other means.

NOTES

[1] Roger George and James Bruce, *Analyzing Intelligence: Origins, Obstacles, and Innovations* (Georgetown University Press, 2009), 19, http://search.ebscohost.com.ezproxy2.apus.edu/login.aspx?direct=true&db=nlebk&AN=228437&site=ehost-live&scope=site.

[2] Ibid.

[3] Johnny Saldaña, *The Coding Manual for Qualitative Researchers* (Sage Publishing, 2016), 18.

[4] Ibid.

[5] Bruce Berg and Howard Lune, "An Introduction to Content Analysis," *Qualitative Research Methods for the Social Sciences*, rev. ed. (Pearson, 2012), 364.

[6] National Research Council, *Funding a Revolution: Government Support for Computing Research*, 1999 (Washington, DC: National Academy Press), 6.

[7] Mark Birdsall, "The Future of Intelligence in the 21st Century," *The Emirates Center for Strategic Studies and Research* 100 (2013), 19.

[8] U.S. Select Committee on Intelligence, U.S. Congress "Current and Projected National Security Threats to the United States," last modified March 12, 2013, https://www.intelligence.senate.gov/hearings/open-hearing-current-and-projected-national-security-threats-united-states-1#.

[9] William Ellis, "US Intelligence at the Crossroads," *Mediterranean Quarterly* 11, no. 2 (2010), 7-8.

[10] Benjamin Sutherland, *Modern Warfare, Intelligence and Deterrence: The Technologies that Are Transforming Them* (Hoboken, NJ: John Wiley & Sons, 2012), http://apus.summon.serialssolutions.com.ezproxy2.apus.edu/#!/search?bookMark=ePnHCXMwfV29DoIwEMa4qImbD9DIKiQ9sD-jEQ0ObhpH0tIyqiG-f7yjgEyOl14u6dB-3_2vorWh2uznp-vhcrMwVol4LCA31fNRJqSgJshNWSCpzdIDsPSK-McQk2AxxEkIUoXUy6hfDsYepm1M63fsMplZydDtZgUVkLSBad7Pp9uxTPqFAkmt0Uay9yB8I7yuBQKZx3-55tJaZZXLLOQKXy_nTjQcfXsrwZIoFBiQhhJytFs9DnaHb7vqUpp9HWWFV0IARa1t0Jo2MlXvMD3ipxT_UUInRlPGazRFIQ73Gs-DmCOXyEX2BYgUaUI.

[11] Thomas Graham, Jr., Keith Hansen, and Robert Huffstutler, Donald R. Ellegood International Publications, *Spy Satellites and Other Intelligence Technologies that Changed History* (University of Washington Press, 2012), http://ebookcentral.proquest.com.ezproxy2.apus.edu/lib/apus/detail.action?docID=3444456.

[12] Bruce Berkowitz, "The R&D Future of Intelligence," *Issues in Science and Technology* 27, no. 3 (2008), 28, http://search.proquest.com.ezproxy2.apus.edu/docview/195932293?pq-origsite=summon.

[13] Mark Birdsall, "The Future of Intelligence in the 21st Century," *The Emirates Center for Strategic Studies and Research* 100 (2013), 3.

[14] Mark Birdsall, "The Future of Intelligence in the 21st Century," *The Emirates Center for Strategic Studies and Research* 100 (2013), 14.
[15] Mark Birdsall, "The Future of Intelligence in the 21st Century," *The Emirates Center for Strategic Studies and Research* 100 (2013), 14.
[16] Andrew M. Colarik and Lech Janczewski, *Cyber Warfare and Cyber Terrorism* (Hershey. PA: IGI Global, 2008), EBSCO*host* (accessed February 9, 2017).
[17] Suné von Solms and Renier van Heerden, "The consequences of Edward Snowden NSA related information disclosures," *International Conference on Cyber Warfare and Security* (2015), https://search-proquest-com.ezproxy2.apus.edu/docview/1781335773?accountid=8289.
[18] Andrew M. Colarik and Lech Janczewski, *Cyber Warfare and Cyber Terrorism* (Hershey, PA: IGI Global, 2008), EBSCO*host* (accessed February 9, 2017).
[19] National Research Council, *Funding a Revolution: Government Support for Computing Research* (Washington, DC: National Academy Press, 1999), 6.
[20] Tracy Blocker and Patrick O'Malley, "Foreign media monitoring: the intelligence analyst tool for exploiting open source intelligence," *Military Intelligence Professional Bulletin* 39, no. 3 (2013), http://search.proquest.com.ezproxy1.apus.edu/docview/1477975805?pq-origsite=summon&accountid=8289.
[21] J.R. Wilson, "DARPA: Fifty Years of Inventing the Furture 1958-2008," *Aerospace America* 46, no. 2 (2008).
[22] U.S. Select Committee on Intelligence, U.S. Congress, "Current and Projected National Security Threats to the United States," last modified March 12, 2013, https://www.intelligence.senate.gov/hearings/open-hearing-current-and-projected-national-security-threats-united-states-1#.
[23] Newstex, "EconMatters: Understanding the Technology of Terrorism," *Newstex Global Business Blogs*, April 29, 2016, http://search.proquest.com.ezproxy1.apus.edu/docview/1785387872?pq-origsite=summon&accountid=8289.
[24] Sergio Koc-Menard, "Trends in Terrorist Detection Systems," *Journal of Homeland Security and Emergency Management* 6, no. 1 (2009), 4, http://search.ebscohost.com.ezproxy2.apus.edu/login.aspx?direct=true&db=tsh&AN=36641436&site=ehost-live&scope=site.
[25] Ibid.
[26] Hans Born and Marina Caparini, *Democratic Control of Intelligence Services: Containing Rogue Elephants* (Abingdon, UK: Taylor and Francis, 2007), 201, http://ebookcentral.proquest.com.ezproxy2.apus.edu/lib/apus/reader.action?docID=438374.
[27] Shashank Joshi and Aaron Stein, "Emerging Drone Nations," *Survival* 55, no. 3. (2013), 53, http://search.ebscohost.com.ezproxy2.apus.edu/login.aspx?direct=true&db=tsh&AN=91830202&site=ehost-live&scope=site.
[28] Ibid., 54.
[29] Ibid., 55.
[30] Ibid.
[31] Ibid., 56.
[32] Ibid., 59.
[33] Ibid.
[34] Ibid., 64.
[35] Shaun Wright et al., "Resurgent Insurgents: Quantitative Research Into Jihadists Who Get Suspended but Return on Twitter," *Journal of Terrorism Research* 7, no. 2 (2016), 6, https://doaj.org/article/e55900312ae64ba08f0bb3a275795d11.
[36] Ibid., 7.
[37] U.S. Select Committee on Intelligence, U.S. Congress, "Current and Projected National Security Threats to the United States," last modified March 12, 2013, https://www.intelligence.senate.gov/hearings/open-hearing-current-and-projected-national-security-threats-united-states-1#.
[38] Thomas Graham, Jr., Keith Hansen, and Robert Huffstutler, Donald R. Ellegood International Publications, *Spy Satellites and Other Intelligence Technologies that Changed History* (University of Washington Press, 2012), http://ebookcentral.proquest.com.ezproxy2.apus.edu/lib/apus/detail.action?docID=3444456.
[39] Berg, Bruce and Howard Lune, "An Introduction to Content Analysis," *Qualitative Research Methods for the Social Sciences* Rev. ed (Pearson, 2012), 364.
[40] Mark Birdsall, "The Future of Intelligence in the 21st Century," *The Emirates Center for Strategic Studies and Research* 100 (2013), 1.
[41] Mark Birdsall, "The Future of Intelligence in the 21st Century," *The Emirates Center for Strategic Studies and Research* 100 (2013), 21.
[42] Johnny Saldaña, *The Coding Manual for Qualitative Researchers* (Sage Publishing, 2016), 7.
[43] Ibid.
[44] William Ellis, "US Intelligence at the Crossroads," *Mediterranean Quarterly* 11, no. 2 (2010), 7.
[45] Ibid.
[46] Ibid., 8.
[47] Ibid.
[48] Nick Hare and Peter Coghill, "The Future of the Intelligence Analysis Task," *Intelligence and National Security* 31, 6 (2016), 859, http://www.tandfonline.com.ezproxy2.apus.edu/doi/abs/10.1080/02684527.2015.1115238.
[49] Ibid., 861.
[50] Ibid., 863.
[51] Ibid., 865.
[52] Ibid.
[53] Ibid., 868.
[54] Ibid., 869.

Airman First Class Candace Nicole Stevens is a member of the U.S. Air Force and a student at American Military University working toward a master's degree in Intelligence Studies. In 2014 she graduated from the University of Arizona in Tucson, obtaining a BA in Art History with a minor in Anthropology. In June 2015, she enlisted in the Air Force and is currently stationed in Clovis, NM, working in the field of airfield management for special operations support.

A Sunk Cost Well Spent: Powering Interagency Remote Sensing Through Civil Applications

by Daniel W. Opstal

INTRODUCTION

In business, a sunk cost is typically used to describe the cost of an investment that has been incurred and cannot be easily recovered. Bruce Elbert, who writes about the satellite communications industry, likens it to buying a warehouse that could go "unfilled" by tenants.[1] The United States' National Imagery Systems are an example of such an investment. These space-based capabilities provide unprecedented understanding of adversaries and world events for U.S. defense officials and policymakers. Yet, the user base for these capabilities goes *far beyond* the military and intelligence communities. Through the Civil Applications Committee, other federal agencies and entities can leverage these capabilities and fill up the proverbial warehouse. As its name might suggest, this committee focuses its efforts on remote sensing support for the Federal Civil Community (FCC), expanding its mandate in 2010 to include commercial imagery contracts procured by the U.S. Department of Defense (DoD) and the Intelligence Community (IC).

Whether it facilitates the precision collection of volcanic ash clouds affecting aviation over the Aleutian archipelago or the analysis of a massive wildfire, the CAC is a unique national committee with a fascinating history and a strong sense of purpose.

Given U.S. civil liberties protections, the CAC cannot function without a strong governance structure in keeping with intelligence oversight guidelines. Additionally, it requires the commitment and dedication of CAC member organizations to carry out their statutory missions *appropriately* using remote sensing technologies.

The following article explores the origins, membership, capabilities, and governance structure of the CAC, with emphasis on specific examples that outline the power of subject matter experts within the FCC leveraging the exquisite capabilities available from national and commercial imagery systems. This journey describes the power of natural phenomena and the importance of interagency collaboration in their analysis. Whether it facilitates the precision collection of volcanic ash clouds affecting aviation over the Aleutian archipelago or the analysis of a massive wildfire, the CAC is a unique national committee with a fascinating history and a strong sense of purpose.

The satellite image above of Bogoslof Island was annotated by a National Civil Applications Center analyst.[2] Remote volcanoes near commonly used air travel corridors, such as Bogoslof, pose a recognized FAA flight risk due to ash clouds, which can rise as high as 39,000 feet.

ORIGINS

Almost immediately after the 1960 launch of the United States' first photoreconnaissance satellite, CORONA, satellite imagery was used for domestic applications such as topographic mapping and emergency

preparedness (via imagery-derived products) in addition to foreign intelligence gathering.[3] A decade later, however, the IC fell under intense scrutiny over domestic spying and other issues. The Rockefeller Commission and the Church/Pike/Nedzi Committees were formed in 1974-75 to investigate misuse of U.S. IC resources. A portion of the investigations examined whether overhead imaging systems operated by the government were illegally spying on U.S. citizens. The Rockefeller Commission examined the full suite of sensors which imaged domestically and determined that the allegations of illegal spying were unsubstantiated. In fact, the Commission noted that "economy" dictated the "appropriate civilian use" of an expensive overhead national architecture. The report outlines how domestic overhead collection was used for disaster mapping, forest inventories, oil spill analysis, and Alaskan pipeline assessment. However, inappropriate domestic collection concerned the Commission. It pointed out as a success story the fact that the CIA turned down a request from the Alcohol and Tobacco Tax Unit of the Treasury Department to use infrared photography in North Carolina to locate moonshine stills.[4]

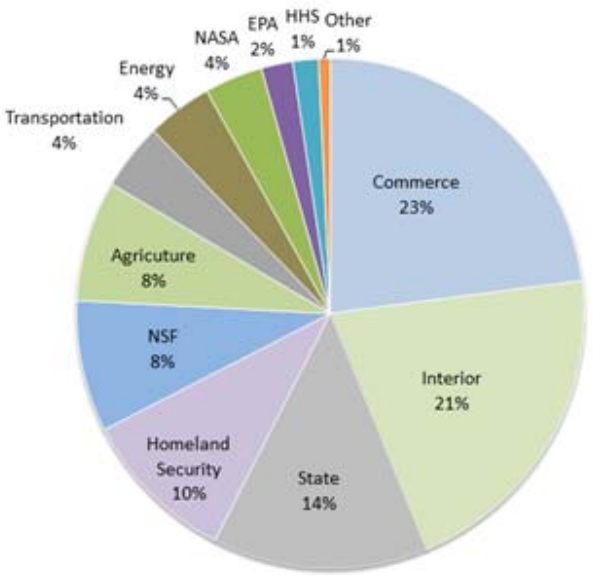
President Ford subsequently directed the establishment of a Civil Applications Committee in 1975 to "allay concerns about improper or illegal use" of National Imagery Systems.

President Ford subsequently directed the establishment of a Civil Applications Committee in 1975 to "allay concerns about improper or illegal use" of National Imagery Systems.[5] The original memorandum establishing the CAC notes that "economy dictates the use of photographs for appropriate civilian purposes."[6] A wide variety of applications such as environmental analysis began to emerge, but the use of these capabilities came with a veil of secrecy as open acknowledgment of the Committee was not possible until 1996. One example of the CAC's usefulness came in 1991. Some 20,000 U.S. military and affiliated personnel were evacuated from facilities near Mount Pinatubo in the Philippines based on a U.S. Geological Survey (USGS) volcanologist's assessment of the situation. The volcanologist's team had access to National Imagery Systems data through CAC procedures.[7] Beyond natural disasters, a challenging aspect of the CAC's work is in support to law enforcement.

The current CAC charter supports certain civil law enforcement functions, such as the collection of illicit vegetation or other untoward activity on federal lands. The collected data, subject to a Proper Use Memorandum (PUM), can support law enforcement personnel responsible for Department of the Interior lands, which account for about 20 percent of the nation's land surface.[8] A similar application supports vegetation and strip mining analysis through the use of small satellites, marking the CAC's foray into the world of global imagery coverage updated on a near-daily basis. Changes in capability are a hallmark of the geospatial intelligence business, as location-based services are nearly ubiquitous. Automation and effective use of machine learning (affectionately known by some analysts as "torturing the pixels" on an image) are no longer conceptual. Indeed, these capabilities are necessary in an ongoing "big data" environment. The CAC looks at both the dual-use and uniquely civil applications of these initiatives and how the data can be disseminated widely through the use of commercial satellite imagery. Housed within the National Civil Applications Center (NCAC), which encompasses collection, analysis, and CAC Secretariat functions, CAC members are able to use remote sensing synergistically for their statutory missions.

MEMBERSHIP AND COMMERCIAL SATELLITE IMAGERY USAGE

The CAC membership includes a tremendous amount of government expertise. Principal members of the CAC include representatives at the Departmental level of Interior, Agriculture, Commerce, Health and Human Services, and Transportation, as well as the U.S. Army Corps of Engineers, U.S. Coast Guard, Environmental Protection Agency, Federal Emergency Management Agency, National Science Foundation, and National Aeronautics and Space Administration. These members are federal organizations with primarily civil missions, typically hosting limited intelligence collection and analytic resources. Associates include representatives from the Departments of State, Energy, and Homeland Security, plus the National Reconnaissance Office, the National Geospatial-Intelligence Agency, and the Defense Intelligence Agency. These are typically IC agencies or those federal entities with a large IC component. Oversight comes via the White House's Office of Science and Technology Policy, the Director of National Intelligence, and the National Geospatial Intelligence Committee (GEOCOM). The imagery tasking requests for DoD/IC-procured commercial imagery are quite sizable. In 2016 the organizations represented by the CAC accessed over a billion square kilometers of imagery through the EnhancedView commercial imagery contract alone. Put another way, that is 110 times the land area of the United States.[9] The following chart provides a breakdown of this usage.



Federal Civil Use of EnhancedView Program Imagery

Other CAC member missions include analysis of the Zika virus (Department of Health and Human Services), vulnerabilities within domestic critical infrastructure such as power generation (Tennessee Valley Authority), and thermal events such as wildfires (Forest Service).

The imagery and geospatial information associated with CAC member missions is as rich and vibrant as the territory it covers. For example, the United States Census Bureau was a primary driver for the Department of Commerce's collection in 2016. Every 10 years, the Bureau is mandated by Article 1, Section 2, of the U.S. Constitution to count every resident in the United States. This drove 92% of commercial imagery collection associated with Commerce, while the remaining amount included National Oceanographic and Atmospheric Administration's (NOAA) functions, such as the search and rescue satellite network for civilian mariners.[10] NOAA's team is equally busy outside of its field work, as its Commercial Remote Sensing Regulatory Affairs Group licenses U.S. commercial remote sensing satellites. This recently included a crafty grade-school class in 2015 (the STMSAT-1 spacecraft was launched from the International Space Station) in addition to a wide variety of small satellite capabilities developed by Planet and other innovative companies.[11]

Other CAC member missions include analysis of the Zika virus (Department of Health and Human Services), vulnerabilities within domestic critical infrastructure such as power generation (Tennessee Valley Authority), and thermal events such as wildfires (Forest Service). Thermal events make a great case study of support to an issue that impacts health and safety across the country. These kinds of stories demonstrate the successful power of teaming at the federal, state, and local levels.

CALIFORNIA WILDFIRES (2007) CASE STUDY

The 2007 fires raging near San Diego ruined entire neighborhoods and reduced homes to rubble. The image below from NASA's Terra satellite provides a macro-level perspective of this event.

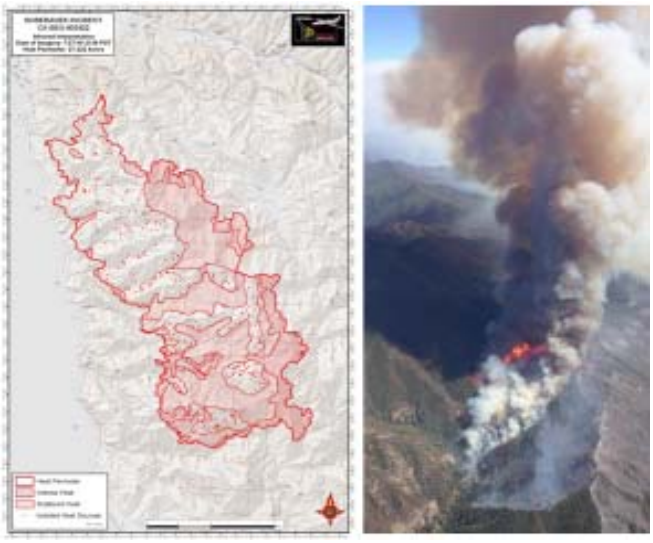
Multiple California wildfires as seen from space, October 23, 2007 (NASA's Terra Satellite)[12]

The twelve wildfires raging at the point depicted above covered the Pacific Ocean with massive plumes of smoke, burned 145,000 acres, and destroyed millions of dollars of property.[13] Airborne suppression efforts were hindered by gale-force winds. Fortunately, through the support of active duty, National Guard, and other government personnel, the flames were eventually contained.[14]

The event above is just one example of the aspects of managing a wildfire, from the proper deployment of firefighters to the effective and safe placement of fire retardant. Accurate data sets are needed quickly, including the status of fuel, weather, fire behavior, assets/personnel risk, and terrain. The CAC supports these kinds of analyses through a Thermal Working Group, which brings together experts from across the fire community to look at the full spectrum of potential remote sensing solutions to monitor fire behavior, including military and IC assets. One capability that has operated continuously since the 1960s is the U.S. Department of Agriculture's Forest Service National Infrared Operations Unit (NIROPS), which leverages two aircraft on a routine

basis to determine the "location and intensity" of fire data.[15] These efforts are complemented by National Imagery System capabilities which are tasked under the auspices of the CAC (see the governance section below).[16] Current fire mapping data can be found on a U.S. Forest Service website. At the time this article was being prepared, multiple high-profile fire events were occurring in the western United States.[17]

Once imagery by the above means is collected, firefighters receive updates on imagery-derived fire lines, which provide additional information for particular teams ahead of deployment into potentially life-threatening fire zones. In addition, headquarters units need an overview of an entire affected area. This information is provided using specialized databases and in concert with GIS analysis to create a mapping product. The following graphic shows a perimeter map used for the 2016 Sobranes, CA, fire, which was updated to aid in the deployment of wildland firefighters.[18]



Sobranes, CA, Fire Perimeter Map and Photograph (National Wildfire Coordination Group)

GOVERNANCE

One of the CAC's key missions is to facilitate the creation of Proper Use Memoranda (PUMs) for federal civil members. A PUM is a "written request expressing the need for collection and use of domestic imagery."[19] Domestic imagery, in this case, is defined as access to imagery of the 50 states, the District of Columbia, and the territories and possessions of the U.S. to a 12-nautical mile seaward limit of the land areas. This is an increasingly important aspect of governance given both the proliferation of commercial satellites and also unmanned aerial systems, more commonly referred to as drones.[2020] Nancy Cook, Remotely Piloted Aircraft Systems: A Human Systems Integration Perspective, Chichester, West Sussex, UK, Wiley, 2017.

The use of various remote sensing resources requires these PUMs to be in place and renewed on an annual basis. A CAC- established interagency workflow helps manage these processes so that changes can be made, such as adjustments to add universities working on new technologies to combat wildfires. These kinds of documents are critical to appropriately using the sensitive data acquired by the U.S. government on behalf of the taxpayer (and doubling their benefit in support of both civil and military sectors).

Each CAC principal member has access to its PUMs and can modify them through an authorized government individual. They are subject to annual renewal, although circumstances can warrant updates throughout the year (for example, when working with a new industry or academic partner using overhead systems).

CONCLUSION

The efforts of the Civil Applications Committee are a part of multiple initiatives leveraging commercial remote sensing capabilities for federal civil agencies. However, it remains the key mechanism to leverage National Imagery Systems for civil purposes. As automation continues to be a theme in the ever-expanding universe of remote sensing data, the CAC is able to be a forum for the federal civil community and its interactions with the DoD/IC.

The group's oversight efforts ensure that overhead imagery capabilities procured by the DoD/IC are used appropriately in close collaboration with the National Geospatial-Intelligence Agency.

More importantly, the group's oversight efforts ensure that overhead imagery capabilities procured by the DoD/IC are used appropriately in close collaboration with the National Geospatial-Intelligence Agency. This includes compliance with applicable executive orders and privacy protections. Through these means, the federal civil agencies can take full, appropriate advantage of the extensive overhead imagery architecture. The proverbial warehouse continues to be full of tenants.

NOTES

[1] Bruce R. Elbert, *The Satellite Communication Applications Handbook* (Boston, IL: Artech House, 2004), 483.

[2] Kim Angeli, "Bogoslof Island: Changes in Shoreline Location," December 25, 2016, JPEG, image file, United States Geological Survey/Alaska Volcano Observatory, http://www.avo.alaska.edu/images/image.php?id=103621 (accessed 19 May 2017).

[3] "Providing KH-4 imagery to EPA," June 20, 1978, *National Photographic Interpretation Center Daily Diary*, George Washington University National Security Archives, http://nsarchive.gwu.edu/NSAEBB/NSAEBB229/31.pdf (accessed 19 May 2017). Imagery-derived products in this case also refer to derived data that can be annotated on a topographic or other base map. For more information on this topic, see https://cms.geoplatform.gov/geoconops/imagery-and-derived-products.

[4] "Overhead Photography of the United States," June 1975, *Rockefeller Commission Report*, pp. 230-231, http://history-matters.com/archive/church/rockcomm/html/Rockefeller_0122a.htm (accessed 12 July 2017).

[5] "Civil Applications Committee Blue Ribbon Study," September 2005, Independent Study Group, George Washington University National Security Archives, http://nsarchive.gwu.edu/NSAEBB//NSAEBB229/40.pdf (accessed 19 May 2017).

[6] "Establishment of the Committee for Civil Applications of Classified Overhead Photography of the United States," The White House, George Washington University National Security Archives, http://nsarchive.gwu.edu/NSAEBB/NSAEBB229/18.pdf (accessed 19 May 2017).

[7] Matt Alderton, "Civil Success Stories," *Trajectory Magazine*, 7 June 2017, United States Geospatial Intelligence Foundation, http://trajectorymagazine.com/civil-success-stories/ (accessed 14 June 2017).

[8] The Civil Applications Committee Charter became effective 19 January 2017. The Department of Interior's Office of Law Enforcement Services Proper Use Memorandum became effective 5 April 2017.

[9] Paul Young, "Federal Civil Use of Commercial Satellite Data," Commercial Remote Sensing Summit, 1 May 2017.

[10] For more information on the NOAA Search and Rescue Satellite Aided Tracking Program, see http://www.sarsat.noaa.gov/.

[11] U.S. Department of Commerce – National Oceanic and Atmospheric Administration (NOAA), Commercial Remote Sensing Regulatory Affairs, NOAA Licensee - St. Thomas More Cathedral School, https://www.nesdis.noaa.gov/CRSRA/files/saint-thomas-more-cathedral-school-stmsat1.pdf (accessed 16 June 2017). For more information about the commercial remote sensing and imagery licensing process, see https://www.nesdis.noaa.gov/CRSRA/.

[12] "NASA Images of California Wildfires," 11 November 2007, NASA/MODIS Rapid Response, https://www.nasa.gov/images/content/193857main_wildfire_oct22_full.jpg (accessed 11 July 2017).

[13] "Fires in Southern California," 23 October 2007, NASA Earth Observatory, https://earthobservatory.nasa.gov/NaturalHazards/view.php?id=8155 (accessed 19 May 2017).

[14] "Military helps fight fires while personnel evacuated," CNN, October 23, 2007. http://www.cnn.com/2007/POLITICS/10/23/fire.military/index.html (accessed 11 July 2017).

[15] U.S. Forest Service National Infrared Operations, About Us, https://fsapps.nwcg.gov/nirops/pages/about (accessed 11 July 2017).

[16] Everett Hinkley, Remote Sensing and Mapping Activities in the Forest Service, Carbon Monitoring Systems Applications Speaker Policy Series, 21 July 2016, https://carbon.nasa.gov/pdfs/FS%20National%20Remote%20Sensing%20Program%20_Hinkley%202016%20NASA%20CMA%20Speaker%20Series%20V3.pdf (accessed 12 July 2017).

[17] U.S. Forest Service Remote Sensing Applications Center, "Active Fire Mapping Program," https://fsapps.nwcg.gov/afm/ (accessed 11 July 2017).

[18] Paul Young, "Federal Civil Use of Commercial Satellite Data."

[19] National System for Geospatial-Intelligence (NSG) Manual 1806, "Domestic Imagery," Revision 5, March 2009, http://nsarchive.gwu.edu/NSAEBB/NSAEBB527-Using-overhead-imagery-to-track-domestic-US-targets/documents/EBB-Doc17.pdf (accessed 2 June 2017).

[20] Nancy Cook, Remotely Piloted Aircraft Systems: A Human Systems Integration Perspective, Chichester, West Sussex, UK, Wiley, 2017.

Daniel W. Opstal is the Executive Secretary of the Civil Applications Committee on a joint assignment from the Department of Defense to the United States Geological Survey. In this capacity he facilitates the federal civil use of various classified and unclassified remote sensing capabilities. Dan is a certified GEOINT professional. He earned an MBA from Pennsylvania State University, a MS in Strategic Intelligence in 2011 from the National Defense Intelligence College (now NIU), and a BA in International Studies and Russian Language from Emory University. He is also an adjunct instructor at American Military University's School of Security and Global Studies. He has published several book reviews in earlier editions of AIJ.

Up Close and Personal: Cultural Awareness and Local Interaction as Experienced by U.S. Military Personnel During Deployment Overseas

by Dr. Rad Malkawi

OVERVIEW

The nature of the operations to which soldiers are exposed during deployment necessitates the need for improved cultural understanding programs. The interaction of soldiers with locals has become an important component of successful missions. The problem is that U.S. soldiers lack adequate educational training regarding foreign cultures; they do not have the proper tools to deal with an insurgency, or to work with local populations. This study analyzes cultural awareness and local interaction as experienced by U.S. military personnel during deployment overseas and explores the extent to which the foreign cultural training they had received supported or undermined their effectiveness during that deployment. The results of this study show the inadequacy of pre-deployment training and suggest ways in which that training could be made more effective. This qualitative study involves the analysis of fifteen interviews of soldiers who were deployed overseas during U.S. involvement in various theaters.

INTRODUCTION

"Over the past decade the United States military has increasingly engaged in lengthy overseas deployments in which mission performance required significant interface with local populations."[1] Learning to interact with local people presents a major challenge for soldiers, leaders, and civilians. For most long-distance operations, the U.S. military attempts to introduce soldiers to an awareness of shared and cultural norms for the regions in which they operate.[2] Since the invasion of Iraq in March 2003, however, the U.S. military has not educated and trained its soldiers adequately through an understanding of Iraqi society and its culture in order to establish local support and achieve mission success. To accomplish this, the U.S. military must prepare, educate, and train its soldiers in how to communicate with the Iraqi population in order to maintain its support.[3]

According to Anthony Arcuri, "Few members of the American Armed Forces are familiar with the cultural traditions of the countries in which they operate. Yet violation of local norms and beliefs can turn a welcoming population into a hostile mob."[4] For instance, Iraqis arrested by U.S. troops have had their heads forced to the ground—a position forbidden by Islam except during prayers. This action offends the detainees as well as the bystanders.[5] Another tactical difficulty based on a misunderstanding of culture is the need for American male soldiers to search Iraqi women physically. Although tactically it might be necessary, it is considered a highly disrespectful action that violates the honor of a family.[6]

Since the invasion of Iraq in March 2003, the U.S. military has not educated and trained its soldiers adequately through an understanding of Iraqi society and its culture in order to establish local support and achieve mission success.

This study investigates cultural awareness and local interaction as experienced by U.S. military personnel during deployment overseas and explores the extent to which the foreign cultural training they received supported or undermined their effectiveness during that deployment. The qualitative findings of the study were developed from 15 interviews during which 15 participants were asked to describe their experiences during deployment. (The data gathered from the 15 interviews were analyzed through the NVivo software to identify themes within the actual interviews.)

LITERATURE REVIEW

This study incorporate numerous professional articles and journals, military publications, professional textbooks, and interviews which support the central foundation of the research. For Hudson and Warman,

understanding how to identify local social structures is vital in understanding conflict from new and different angles. American soldiers must know how to operate with, and respect, the people from the various cultures they will encounter during deployment.[7]

"Recent American history has witnessed frequent failures in the application of cultural intelligence and awareness, ranging from the war in Vietnam to the ongoing deadlock over North Korea's nuclear ambitions. The U.S. military occupation of Iraq constitutes the most prominent contemporary example."[8] The basic cultural training of U.S. troops has been "insufficient, as namely illustrated by dramatic misunderstanding between troops deployed in Iraq and Afghanistan and the local population in those countries."[9] These failures have "increased the time spent in foreign combat operations and have prolonged Military Operations Other Than War (MOOTW), such as Somalia and Haiti."[10]

Acculturation is defined as a process by which individuals or groups accept, selectively, aspects of another culture, often a dominant one that those individuals or groups intend to adopt without completely relinquishing their own.

In the Vietnam War, "anthropologists such as Gerald Hickey, who went to Vietnam as a University of Chicago graduate student and remained throughout the war as a researcher for the RAND Corporation, found that their deep knowledge of Vietnam (valuable for counterinsurgency) was frequently ignored by U.S. military leaders who increasingly adopted a conventional-war approach as the conflict progressed."[11]

"The U.S. Army invaded Iraq with its forces unprepared to interact with Iraqi culture. Other than the token cultural awareness briefing (if) conducted by the unit, there was insufficient knowledge or understanding of the significance the Iraqi culture, family, tribal affiliations, and religion would have on combat and stability and reconstruction operations. There was no understanding of subjective culture which is the learned and shared patterns of beliefs, behaviors, and values of groups of interacting people."[12]

The researcher uses acculturation as a theoretical foundation. Acculturation is defined as a process by which individuals or groups accept, selectively, aspects of another culture, often a dominant one that those individuals or groups intend to adopt without completely relinquishing their own. Aspects of the adopted culture may include beliefs (e.g., religion), values (e.g., generosity, volunteerism, free speech), social norms (e.g., dress, greetings, burial), and lifestyles (e.g., foods and tobacco use).[13]

Four acculturation attitude strategies exist: assimilation, separation, integration, and marginalization. Assimilation is where people do not wish to maintain their cultural heritage and seek adapting attitudes more similar to the dominant culture to interact better with other cultures.[14] Assimilation strategy holds when individuals of the acculturating group choose to adopt the dominant culture and to shed their original culture.[15]

Berry defines separation as "the individual wanting to hold onto his or her native cultural ideology and avoid adopting the dominant cultural system."[16] On the other hand, integration strategy prevails when there is an interest in maintaining the original culture while at the same time seeking to participate as an integral part of the dominant culture.[17] Fourth, marginalization dominates when there is little interest in maintaining the original culture and little interest in adopting the dominant culture.[18]

Acculturation integration attitude strategy is used for this study because there is an interest in both retaining original culture while at the same time contributing an integral part of the dominant culture. The U.S. Army has taken a number of steps to integrate this instruction during pre-deployment training. Limited pre-deployment training occurs at home station using live role players while "graduation exercises" in negotiation training are also provided at the Combat Training Centers, to include the National Training Center (NTC) and the Joint Readiness Training Center (JRTC).[19]

METHODOLOGY

For this study, qualitative research is used to analyze cultural awareness and local interaction as experienced by U.S. military personnel during deployment overseas and to explore the extent to which the foreign cultural training they received supported or undermined their effectiveness during that deployment. To understand and examine the complex real-life activities in which multiple sources of evidence are used, the case study method was chosen to explore the perceptions and experiences of military officers in cultural understanding. The cases considered in this study are based on interviews with 15 members of the U.S. military. The interviews allow validation and a deeper understanding of how learning cultural awareness affects the members of the military.

A sample population of U.S. military personnel from units based in Northern California is interviewed. All 15 participants are staff and officers who have served in foreign countries during war. The interview process is guided by the following query: "Describe cultural awareness and local interaction as experienced by United States military during deployment overseas and explore the extent to which the foreign cultural training they had received supported or undermined their effectiveness during that deployment."

INTERVIEW FINDINGS

Positive Outcome of Pre-Deployment Training

The first thematic category is labeled Positive Outcome of Pre-Deployment Training. The thematic category pertains to perceiving ways in which pre-deployment training led to positive outcomes during deployment. Most of the participants cite understanding of the culture (six out of fifteen participants, or 39%) as a positive outcome of pre-deployment training. Table 1 contains all the codes that emerged from the thematic category, positive outcome of pre-deployment training.

Table 1
Codes for Positive Outcome of Pre-Deployment Training

Codes	# of participants to offer this experience	% of participants to offer this experience
Understanding the culture	6	39%
No response	3	20%
Respect	3	20%
Equal treatment	1	7%
Consensus building	1	7%
None	1	7%

The most cited positive outcome of pre-deployment training is the understanding of the culture where the deployment takes place. Participant 9 speaks about understanding the practices of the saying "hello" and interacting with women during the war in Vietnam:

> Saying hello to them, very rarely will they respond if you say hello to them. I'm not saying it is now but back then if you say hello to people and some say hello back but some don't. It's just the way I have… I guess I don't know… they're very untrustworthy because of their situation. I met a wife, I met her one time. I was helping this old woman, I can't remember. She had some heavy items I offered to help her and she told me get away from her. And then I ask my friend why did she get so mad for I was just trying to help her and he said yeah she thinks you're trying to get something. You might steal her groceries or you might… They just don't trust Americans. He was right. I had to play by their rules.

Participant 6 speaks about the benefits of understanding the culture of other nations during operations:

> To learn a little bit about the culture, that way we do not infringe upon negatives of foreign countries and the foreign countries can keep their negatives to their selves or learn what not to do to offend someone.

As a result of the understanding of the culture, there is more equality. Participant 1 explains:

> Everyone is treated as a human being and not simply an Arab. Much like many Americans, Arabs are equally prone to saying one thing but meaning another. When presented with such a situation, our initial inclination is to write off this behavior by saying, "It's an Arab thing." This, as emphasized by my commander, is not true. As people across all cultures do the same thing. Merely understanding this aspect, forces the military to understand the underlying message of a local sheikh and make the appropriate accommodations that satisfies both of his needs, the military's needs, and the population of the local area.

Issues/Problems

The second thematic category is labeled Issues/Problems. The thematic category pertains to the areas of cultural awareness that are experienced negatively by the participants during deployment, suggesting that improvement may be necessary. Some of the responses include cultural communication (four out of fifteen participants, or 26%) and cultural sensitivity (two out of fifteen participants, or 13%). Table 2 contains all the codes that emerged from the thematic category, areas of improvement.

Table 2
Codes for Issues/Problems

Codes	# of participants to offer this experience	% of participants to offer this experience
Cultural communication	4	26%
No response	3	20%
Cultural sensitivity	2	12%
Purpose of military	1	7%
Practices of the native	1	7%
Application	1	7%
Television	1	7%
Civilians	1	7%
Flexibility	1	7%

The results of the study indicate that cultural communication is an area relevant to cultural awareness that needs to be improved. Participant 1 speaks about further developing the cultural sensitivity of the troops, an area that he finds to be still lacking:

> I have seen the opposite of support in cultural sensitivity in other units. When this occurs, people have a tendency to brand people liars, greedy, or insurgents. The Arab World is far too complex to paint such a general picture of someone who may exaggerate, ask for money, or have links to insurgent/criminal groups. Sadly, it is more the norm than the exception that military commanders fail to realize.

Participant 7 speaks about the benefits of formalization of cultural sensitivity training in schools:

> It should be taught in schools about different cultures. They teach in the language and the culture of a country we might be transferred to. So we know ahead how they live and how they dress. It's a whole different ball game.

Suggestions for Training Improvement

The third thematic category is labeled Suggestions for Training Improvement. This thematic category pertains to the suggestions proposed by the participants that could improve the cultural awareness of the troops. Half of the participants cite immersion as a technique that could improve the cultural awareness of the troops during deployment. Table 3 contains all the codes that emerge from the thematic category, suggestions for training improvement.

Table 3
Codes for Suggestions for Training Improvement

Codes	# of participants to offer this experience	% of participants to offer this experience
Immersion	4	28%
Language	3	16%
Cultural understanding	1	7%
Diversification	1	7%
Longer training	1	7%
Structured classes	1	7%
Selective recruitment	1	7%
School	1	7%
Intelligence report	1	7%
Religion	1	7%

Half of the participants suggested immersive strategies to improve the troops' cultural awareness. Participant 9 speaks about the benefit of visiting the countries to get a better understanding of the culture: "Maybe visit the countries themselves if they have the opportunity because a lot of them are making up their minds by what they hear or what other people tell them but they should see firsthand." Participant 11 suggested interacting more with the locals to improve the cultural awareness of the troops during deployment:

> I would say first of all, let's say anything recent Iraq or Afghanistan. I would have them interact with Iraqis who work with the American government. Interact with the soldiers before they go in there. They live pretty much in a box they don't know what's going on but before you go in their country you should know are they going to school, you know some person from that country should communicate with the soldiers before they go into the country. So they have an idea what type of people they are. I think that would be very effective.

Some participants suggested the need to focus more on developing the language skills of the troops during the operation.

Some participants suggested the need to focus more on developing the language skills of the troops during the operation. Participant 1 spoke about the importance of having basic Arabic language skills:

> Senior leaders (Sergeants First Class and above and all officers) should be given a more basic understanding of the Arabic language. To understand a people, an understanding of language is critical. Since language is the genesis of all communication between people, understanding the dynamics of language can only enhance relations. Also, even the most basic introductory level of language training provides greater flexibility of the leader outside of the limitations of a key vocabulary list and phrases, as, ultimately, situations will arise that will exist beyond a pocket of phrases and words.

Participant 4 emphasized the need for language training:

> The first thing they should do with the soldiers who are deployed overseas is teach them some basic language or course. If you're going to be in another country, speaking their language should be taught.

Participant 5 spoke about people from other cultures being able to understand English, but it would be helpful to understand the language of the other culture as well:

> I think cultural orientations are helpful. If you just go to certain countries without knowing their culture or their language I don't think that will help. Even though all the places in the world know the American culture, know the language. We don't have to speak their language. We try to understand. They spoke English. They knew our culture, our language. I spoke English and so did they.

CONCLUSIONS

This study analyzes a variety of incidents witnessed by U.S. military personnel during deployment overseas and explores the extent to which the foreign cultural training they have received supported or undermined their effectiveness during that deployment. The results of the case study and interviews reveal the significance of cultural knowledge during combat operations. It is the aspect of military operations that is often overlooked in favor of technological prowess.

The purpose would not be to make every soldier a linguist but to make every soldier a diplomat in uniform equipped with just enough sensitivity and linguistic skills to understand and converse with the indigenous citizen on the street.

The foreign culture learning experiences of the participants suggest that they learn elements of the target culture when they do not conflict with those of their own culture. In cases where there is no conflict, the participants integrate the target cultural elements into their existing cultural knowledge. Acculturation of every soldier to prospective theaters of war is important. Every young soldier should receive cultural and language instruction. The purpose would not be to make every soldier a linguist but to make every soldier a diplomat in uniform equipped with just enough sensitivity and linguistic skills to understand and converse with the indigenous citizen on the street.

With regard to the positive and negative outcomes of teaching foreign cultures to members of the U.S. military, the participants indicated that they benefited significantly from acquiring basic knowledge of a country's culture during deployment. However, this basic knowledge needs to be expanded as reflected by the troops' report regarding the limitation of the current training at the operational level. Basic cultural awareness training is not sufficient in relating effectively with the locals and interpreting the behaviors of their adversaries.

Culture must be fully incorporated as a vital component of language learning. Military members can be successful in speaking a second language only if cultural issues are an inherent part of the learning process.[20] This can be done through pre-deployment training and immersion activities, allowing the troops to have enough time to be proficient in the language. Having the language skills could equip the troops with the necessary tools to hone their cultural awareness.

Basic training on cultural understanding that only covers the main characteristics and practices of a culture would be beneficial as an introduction, but not as the main training upon which the military personnel would be dependent during operations. The insufficient utility of pre-deployment training for cultural understanding to which the military is exposed suggests that more effective strategies should be explored.

The results prompt some suggestions on how cultural understanding training can be improved at the operational level. Two of the main suggestions include immersion and language training. Each suggestion can be explained in terms of the theoretical framework of the study, which is acculturation.

Immersion is the most cited suggestion by the participants to improve cultural understanding. Immersion is perceived to be a useful form of training because immersive experiences offer a way in which military personnel can learn by being part of the culture. Careful analysis of acculturation situations and sequences offer useful opportunities for understanding cultural dynamics.[21]

The Department of Defense also recognizes the importance of cultural education, training, and language proficiency for military members.

Language is another important suggestion emerging from the data. Receiving cultural and language instruction is important.[22] The purpose would not be to develop linguistic skills but to equip soldiers with the language skills that would enable them to interact and communicate with the natives. The combination of immersive and language training could be the main training framework wherein an improved cultural understanding program can be based.

The Department of Defense also recognizes the importance of cultural education, training, and language proficiency for military members. In October 2004 Secretary of Defense Donald H. Rumsfeld released a memo stating, "Foreign language skill and regional and cultural expertise are essential enabling capabilities for DoD activities in the transition to and from hostilities."[23] This suggests that there is government support toward improved cultural understanding programs. The problem, however, is in the implementation of a more effective cultural understanding training program, as evidenced by the seeming insufficient training that the military is currently receiving.

NOTES

[1] Maxie McFarland, "Military cultural education," *Military Review*, March-April 2005: 62-69.
[2] Ibid., 62.
[3] Anthony P. Arcuri, "The importance of cross-cultural awareness for today's operational environment," master's thesis, U.S. Army War College, Carlisle, PA, 2007, 6.
[4] Ibid.
[5] Ibid.
[6] Jeff D. Hudson and Steven A. Warman, "Transforming the American soldier educating the warrior-diplomat," master's thesis, U.S. Naval Postgraduate School, Monterey, CA, 22.
[7] Ibid., 26.
[8] CADS Staff, "Cultural Intelligence and the United States Military," Center for Advanced Defense Studies. Retrieved from CADS website: http://www.c4ads.org/files/cads_report_cultint_jul06.pdf, July 2006: 1-3.
[9] Ibid., 2.
[10] Ibid., 3.
[11] Montgomery McFate, "Anthropology and counterinsurgency: The strange story of their curious relationship," *Military Review*, March-April 2005: 1-20.
[12] Brian Thomas Beckno, "Preparing the American solider in a brigade combat team to conduct information operations in the contemporary operational environment," master's thesis, USACGSC, Fort Leavenworth, KS, 2006, 38.
[13] Grace X. Ma, Yin Tan,Jamil I. Toubbeh, Xuefen Su, Steven E. Shive, and Yajia Lan, "Acculturation and smoking behavior in Asian-American populations," Health Education Research 19(6), 2004: 615-625.
[14] David M. Dees. "How do I deal with these new ideas? The psychological acculturation of rural students," *Journal of Research in Rural Education* 21(6), June 28, 2006, 1-11.
[15] Glynis Anna Adams Gault, *Identity style, acculturation strategies and employment status of formally educated foreign-born African women in the United States*, doctoral dissertation, Virginia Polytechnic Institute and State University, Falls Church, VA, 2005, 14-15.
[16] John W. Berry, "Fundamental psychological processes in intercultural relations," in D. Landis & Y. Bennett (eds), *Handbook of intercultural research*, 3rd ed. (Thousand Oaks, CA: Sage, 2004), 176.
[17] Ziad Swaidan, Kimball P. Marshall, and J.R. Smith, *Acculturation strategies: The case of the Muslim minority in the United States*. 2001, http://www.sbaer.uca.edu/Research/sma/2001/32.pdf. See also David M. Dees, "How do I deal with these new ideas? The psychological acculturation of rural students."
[18] Ziad Swaidan, Kimball P. Marshall, and J.R. Smith, *Acculturation strategies: The case of the Muslim minority in the United States*.
[19] Paula J. Durlach, Timothy G. Wansbury, and Jeffery G. Wilkinson, "Cultural awareness and negotiation skills training: Evaluation of prototype semi-immersive system.," 2008, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA505896&Location=U2&doc=GetTRDoc.pdf.
[20] Elizabeth Peterson and Bronwyn Coltrane, *Center for applied linguistics*. Retrieved from Center for Applied Linguistics, December 2003, http://www.cal.org/resources/digest/0309peterson.html.
[21] H.G. Barnet, Leonard Broom, Bernard J. Siegel, Evon Z. Vogt, and James B. Watson, Acculturation: An exploratory formulation. *The Social Science Research Council Summer, Seminar on Acculturation*, American Anthropological Association, 1954,.973-1000.
[22] Robert Scales. "Army transformation: Implications for the future," statement of Major General Robert Scales, MG, USA (Ret), 2004, http://www.au.af.mil/au/awc/awcgate/congress/04-07-15scales.pdf.
[23] Anthony P. Arcuri, "The importance of cross-cultural awareness for today's operational environment," *m*aster's thesis, U.S. Army War College, Carlisle, PA, 2007, 20.

Dr. Rad Malkawi has more than fourteen years teaching experience at several universities in the U.S. and in the Middle East, such as University of Wisconsin, University of Tennessee, Prince Mohamad University, and Jordan University of Science and Technology. He holds two doctoral degrees, one in Educational Leadership from Argosy University in San Francisco, CA, and the other in Archaeology and Art History from Kaslik University in Lebanon. He works as a trainer in leadership and soft skills for several academic institutions in Jordan and Saudi Arabia. Jordanian by birth, he is a U.S. citizen and taught Arabic for five years at the Defense Language Institute.

Signal Pollution: The Unseen Threat

by H. Anthony Smith

THE GOLDEN ERA OF HOME AUTOMATION

The idea of the automated home was made real through Wi-Fi enabled devices such as washer/dryer combinations, lights, coffee pots, and security systems. It is now possible to check the status of home automation devices through applications on smart phones or tablets. Commercials about home automation portray homeowners feeling confident they will be alerted in the event of a home security breach; unfortunately, commercials do not always portray reality.

FAIL SAFE OR FAIL SECURE?

Fail safe or fail secure? Which state do you want your security devices to revert to during a service disruption? The answer to that question depends on the system. In the event of a building evacuation due to power failure, the security doors should let people out (fail safe or open). The opposite is true for spaces configured to prevent unauthorized entry such as bank vaults; they should be configured to stay locked (fail secure).

Security systems installed in private residences have options for detecting smoke, carbon dioxide, fire, unauthorized entry, and motion. During a fire event, these systems allow residents to leave after alerting them to an environmental disruption (fail safe). Battery packs in sensors and the base station allow security systems to remain functional even during power outages (fail secure). The ideas of fail safe and fail secure are put into practice daily; however, they do not always work with wireless systems.

XFINITY HOME SECURITY

In January 2016, Phil Bosco of Rapid7 announced a discovery that would shake the confidence of homeowners using Comcast home security systems: a flaw that would allow intruders inside a home without setting off alarms. The flaw is triggered after "creating a failure condition in the 2.4 GHz radio frequency band, the Comcast XFINITY Home Security System fails open, with the base station failing to recognize or alert on a communications failure with the component sensors." (Bosco, 2016)

In other words, overwhelming the base station with 2.4Ghz signal effectively disrupts remote sensors from communicating with the base station. The base station, in turn, does not report or alert on a communications failure. The homeowner with the signal-overwhelmed security system will never know there is a problem.

Exploiting this discovered flaw might feel like an impossible task for those who are not trained in the dark arts of "hacking" but, in reality, it is relatively simple. All that is needed is a 2.4Ghz jammer; flooding the area with signal e0ffectively disarms the system.

At the time of this announcement, there were "no practical mitigations to this issue." (Bosco, 2016)

WHY 2.4GHZ?

John Herman, writing for Wired in 2010, explained the reason for most devices using 2.4Ghz; it is free (Herman, 2010). The 2.4Ghz frequency is part of a selection of frequencies set aside by the FCC[1] that may be used without an individual operations license (Federal Communications Commission, 2016).

2.4GHZ DEVICES

According to the FCC, examples of devices using 2.4Ghz include wireless garage door openers, wireless temperature probes, RF universal remote control, cordless telephones, alarm systems, vehicular radar systems, Wi-Fi, and Bluetooth devices (Federal Communications Commission, 2016).

Ask yourself, "How many devices does my household have that use 2.4Ghz?" You might be surprised at the answer.

My personal list of 2.4Ghz devices includes:

- Bluetooth in automobiles
- Garage door opener
- Wireless printers, keyboards, and mice
- Computers, tablets, and phones
- Video streaming devices such as Apple TV

- Smart televisions
- Speakers and headphones
- Routers and range extenders
- Home assistance devices like Amazon Echo
- Home security system components
- Thermostats
- Smoke detectors

All of these devices transmit and receive signals using 2.4Ghz. Some of these devices connect to the Internet through Wi-Fi hotspots while others communicate only with a remote control. The number and variety of devices each household contains will vary. An awareness of the number of wireless devices and how they communicate provides homeowners insight into the number of signals present in their environment.

HOW MUCH SIGNAL? A LOT

Trouble-shooting wireless networks can be problematic. The usual procedure involves disconnecting and reconnecting to a hotspot with the hope that the Internet will once again be available on the desired device. If Internet access is still inaccessible, then power cycling the device usually works. What does one do when the first two steps fail? The answer is check the signals around your location.

Determining how much signal is being emitted by all of these devices requires a frequency spectrum analyzer; however, one can use a software application to discover nearby Wi-Fi hotspots. Knowledge of hotspots and the channels to which they are assigned will provide insight into how much signal pollution your devices are experiencing.

WI-FI ANALYZER

Detecting Wi-Fi hotspots is easy; understanding the impact of all the signals is difficult. Figure 1 depicts the Wi-Fi hotspots detected using the Wi-Fi Analyzer program. The y-axis shows the signal strength; the x-axis shows the channel number; the color-differentiated arcs show the different Wi-Fi hotspots.

The overlapping arcs show the Wi-Fi hotspots that are using the same 2.4Ghz channel. Channel 11 in Figure 1 shows seven different Wi-Fi hotspots. This overlap of signals is the connected device equivalent of being at a

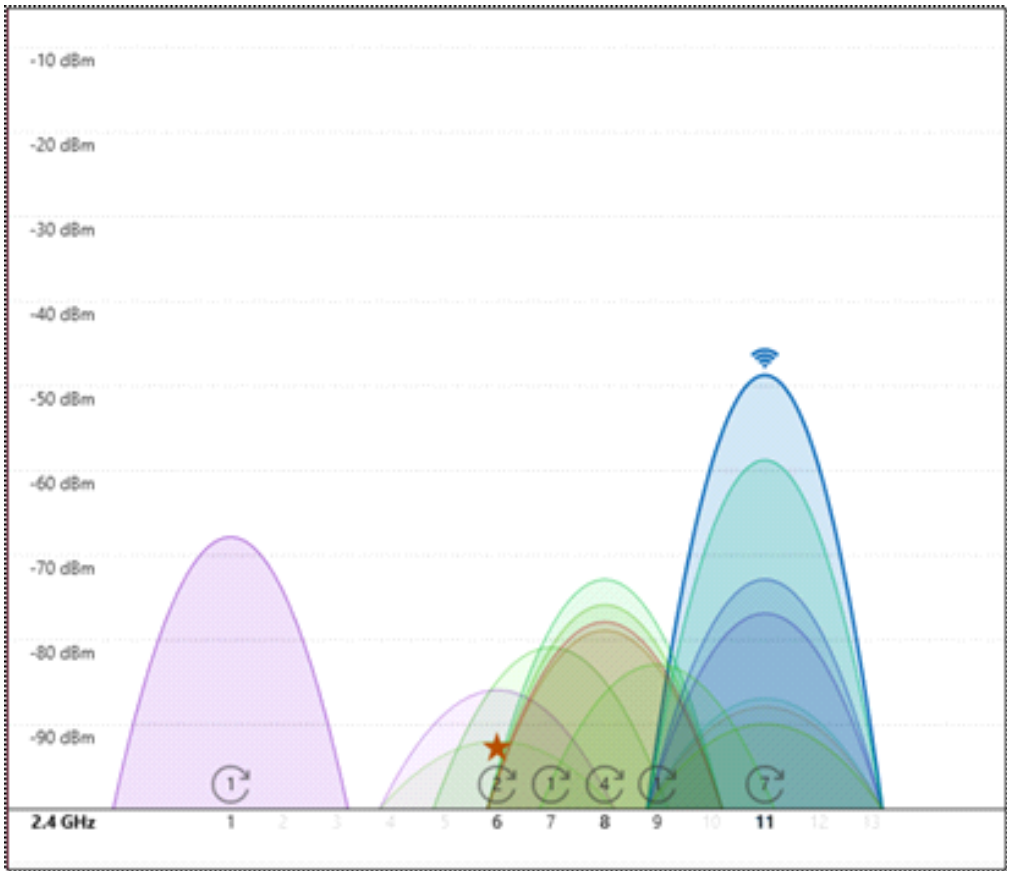


Figure 1: Screen Capture of 2.4Ghz Wi-Fi Hot-Spots and Signal Strength[2]

party and trying to converse with someone while ten other conversations are ongoing close by. It does not mean conversations are not possible, but the addition of a louder, closer conversation might prevent your conversation from continuing.

ADDITIONAL SIGNALS

Using a program called NetSpot,[3] I was able to detect both 2.4Ghz and 5.0Ghz signals. Figure 2 shows Wi-Fi hotspots using both frequencies, wireless printers, and streaming video and music devices. Over the span of one hour I was able to detect 78 unique devices transmitting in either the 2.4Ghz or 5.0Ghz frequencies.

Signal spikes, such as those appearing as vertical lines, show devices that periodically connect to Wi-Fi hotspots for content updates. For example, the recurring spikes with signal strength -60db, shown in Figure 2, originated from an Amazon Fire TV device.[4]

SELF-INFLICTED DENIAL OF SERVICE

I accidentally launched a denial of service attack on my home security network. It was very easy to do; I introduced another device into the home, specifically a Wi-Fi range extender. The range extender did exactly what it was designed to do: connect to a Wi-Fi hotspot, amplify the signal, and act as a Wi-Fi relay. I was not aware the device had a bonus feature of signal jamming my home security base station. In my day-to-day interactions with the base station, I did not notice any changes and I believed everything was functioning as expected. I was wrong.

SECURITY SYSTEM VULNERABILITY

The security system I selected uses cellular communications (4G LTE) rather than landline or Internet. I wanted to avoid systems like those offered by XFINITY Home Security. In my mind, cellular would be more secure and not be susceptible to the same types of vulnerability.

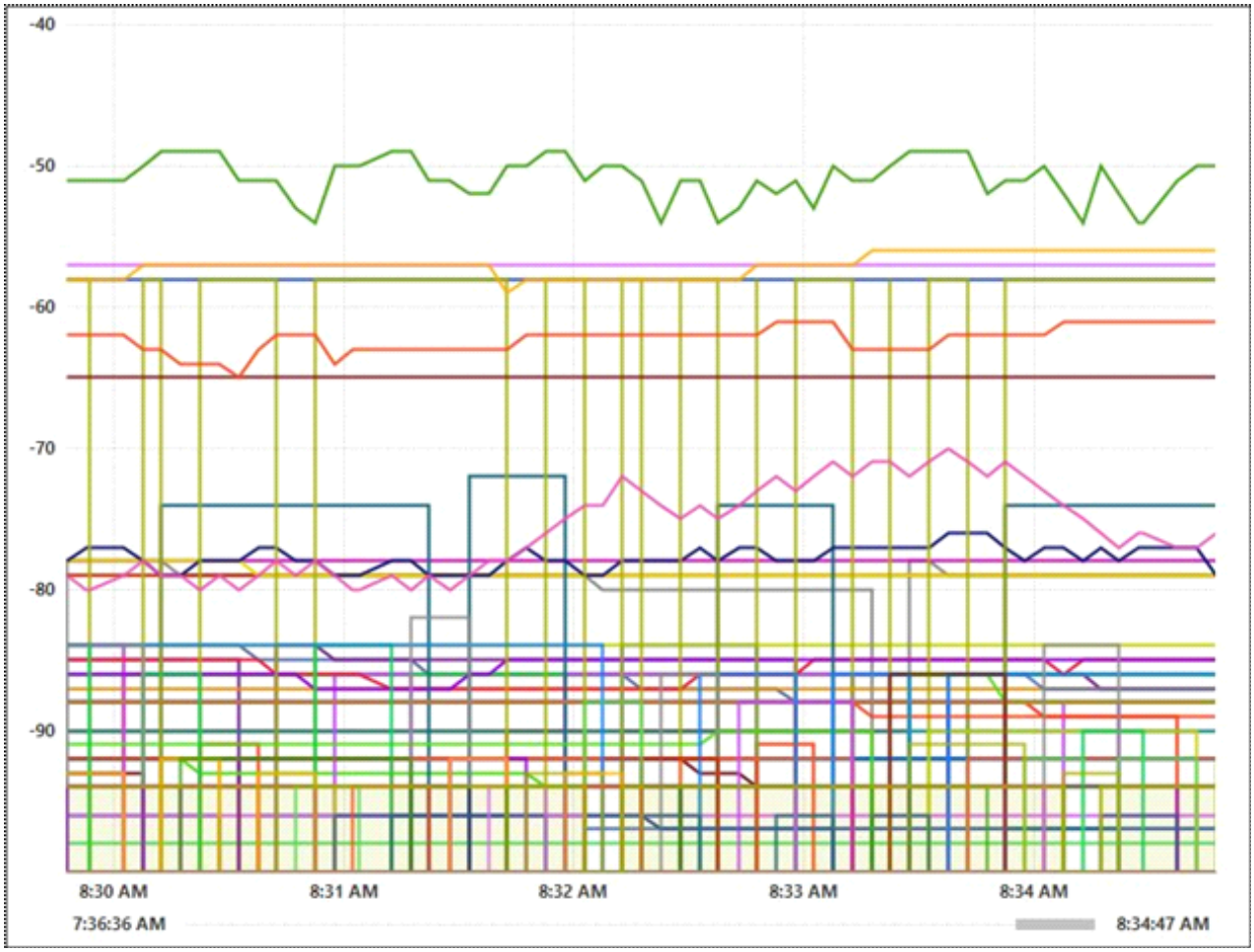


Figure 2: Screen Capture of 2.4Ghz and 5.0Ghz Devices and Wi-Fi Hotspots

I was shocked when I received an email from the home security company informing me that my base station had not updated its status in three days.

I looked online for the user's manual for the base station and went through several trouble- shooting routines. I logged into the web portal that shows the system status in a vain attempt to solve the problem. I even briefly entertained the thought that the system was faulty and needed to be replaced. I paused in the middle of dialing the helpdesk number and realized the mistake I had made: the newly installed Wi-Fi range extender was too close to the base station. After relocating the range extender to the other side of the room, updates to the monitoring center resumed.

The security base station uses Sprint's 4G LTE network to communicate; that network uses 2.5Ghz. The only conclusion I could logically come to is that signal pollution caused enough interference that I effectively caused a denial of service attack against myself.

CONCLUSION

Wireless technologies have made instant access to information and entertainment possible however, too much access and signal can create problems. In my example, I placed a range extender too close to a security system; this could also happen with other wireless devices such as Bluetooth connected keyboard, mice, and speakers. My advice is to be aware of possible interference and consider where devices are located.

NOTES

[1] The FCC regulates devices that emit radio energy by radiation, conduction, or other means. (Federal Communications Commission, 2016).

[2] Wi-Fi Analyzer, an application created by Matt Hafner, was used in the creation of Figure 1. This application is available through the Microsoft applications store.

[3] NetSpot version 1.0.0.334; Discover Mode; date collected 2017-02-09; NetSpot Team, Etwok LLC, 2017.

[4] Note: The device was not in use at the time this graphic was generated.

References

Bluetooth. (2017). *Bluetooth Core Specification.* Retrieved from Bluetooth: https://www.bluetooth.com/specifications/bluetooth-core-specification.

Bosco, P. (2016, 01 05). *R7-2015-23: Comcast XFINITY Home Security System Insecure Fail Open.* Retrieved from Rapid7 Community: https://community.rapid7.com/community/infosec/blog/2016/01/05/r7-2015-23-comcast-xfinity-home-security-system-insecure-fail-open.

Federal Communications Commission. (2016, 11 10). *Equipment Authorization – RF Device.* Retrieved from Federal Communications Commission: https://www.fcc.gov/oet/ea/rfdevice.

Herman, J. (2010, 09 07). *Why Everything Wireless is 2.4 Ghz.* Retrieved from Wired: https://www.wired.com/2010/09/wireless-explainer/.

H. Anthony Smith is currently assigned to the National Intelligence University's Anthony G. Oettinger School of Science and Technology Intelligence, where he lecturers on technology and cyber-related topics. Most of his teaching duties are within the Cyber Intelligence and Data Analytics concentration of the School's Master of S&T Intelligence (MSTI) degree program. Anthony's current research interests include testing the efficacy of cyber security awareness training and developing 21st century network analysis tools.

Walsingham's Entrapment of Mary Stuart:
The Modern Perspective of a Deception Analyst/Planner

by R. Kent Tiernan

Mary, Queen of Scots
Fotheringhay Castle, Midnight (12:01 a.m.), 8 February 1587

After months of defending herself against accusations that she had directly approved of and participated in traitorous activities designed by Thomas Morgan, John Ballard, and Anthony Babington to overthrow England's Protestant government and assassinate her royal cousin, Elizabeth I, Mary Stuart awaited her fast-approaching execution at Fotheringhay Castle. As the time quickly sped toward that fateful hour, she found that sleep eluded her. Using the time that was left before her day of atonement, the Scottish queen made peace with her God and prepared herself for the moment she would slip the surly bonds of earth. In so doing, she reflected on the recent events that eventually condemned her to the executioner's block scheduled for the early morning hours of 8 February 1587.

Looking back, she could not have realized that her escape from her rebellious Scottish nobles and request for sanctuary in England in 1568 would condemn her to years of house arrest and a growing sense of claustrophobic isolation. Mary realized that relations with Elizabeth had always been tenuous at best, and as a result she had attempted to negotiate an agreement that would safely return her to Scotland with her royal cousin's tacit support. However, it did not take long for the Scottish queen to discover that the greatest nemesis in blocking her freedom from English control were Elizabeth's two most influential advisors—William Cecil and Francis Walsingham.

Certainly, she opined that their hatred of her and what she represented to other Catholics in England and abroad justified her numerous attempts to support a growing flood of conspiratorial activities that would free her from the clutches of her heinous jailors. Granted, she understood that her approval or tacit consent (17 July 1586) to Babington's letter (written on 6 July 1586) suggesting Elizabeth must be physically removed from governance may have been ill-advised, but after more than 18 years of imprisonment, failing health, and dashed hopes (failures of the Ridolfi, Throckmorton, and Parry plots), Mary felt that her last chance of escape via the Babington conspirators had arrived. Perhaps, she thought, if she had not taken this one unfortunate, but obvious, fateful misstep she would have survived to fight another day for the return of Catholicism to England. However, she would never know that her trip to Fotheringhay Castle and rendezvous with the executioner's ax was not a result of a poor, "go for broke" decision on her part, but was instead the main objective of a skillfully planned, coordinated, and executed deception/influence operation developed by her two most formidable foes—Cecil and Walsingham—approximately six years earlier.

SUBJECT RELEVANCE

Several years ago, before embarking on writing a book on this subject, I asked myself who or why would anyone be interested in reading about a historical event focused on the death of a Scottish queen that occurred approximately 430 years ago. [Author's Note: *The Walsingham Gambit: Entrapment of Mary, Queen of Scots (1580-1587)* is scheduled for public release during

the late 2017 or early 2018 time frame.] After much thought about its relevance in today's global setting, and backdrop, the answer to my question seems quite simple.

First, it is a darned good story. That is especially true if one enjoys reading about espionage, conspiracies, a life or death struggle between two very talented, strong-willed women, and royal court intrigue and deceit all packaged within a larger backdrop of overt/covert religious activities between two implacable foes.

The Babington plot is a cautionary tale that can be used to enhance analytical methods and approaches focused on determining if an event is real or purposely distorted to protect or promote an opponent's military, political, economic, or psychosocial agenda.

Second, for those who are interested in contemporary intelligence issues or are simply fascinated with the subject of deception, the Babington plot offers a significant window into how the "art" of deception was applied to overcome a situation that threatened the very survival of a nation.

Third, to those who may be involved in planning or supporting manipulation-type activities, the Babington conspiracy provides some invaluable truths and insights into what is required to successfully conduct large-scale, strategically-focused deception/influence operations.

Fourth, for those committed to the search for truth, the Babington plot is a cautionary tale that can be used to enhance analytical methods and approaches focused on determining if an event is real or purposely distorted to protect or promote an opponent's military, political, economic, or psychosocial agenda.

Fifth, the subject is certainly topical with recent revelations that Russian intelligence overtly and covertly attempted to influence the 2016 U.S. Presidential election.

The fact remains that history is replete with examples of successful and failed denial and deception activities. Interestingly, the types of manipulative tactics, techniques, and procedures employed in the distant past are still being successfully used today. Referring to Edmund Burke's cautionary adage, we must never forget, "Those who do not know history are doomed to repeat it!"

THROUGH A DECEPTION ANALYSIS OPTIC

While volumes have been written on deception by myriad internationally renowned historians and interdisciplinary scholars and experts, relatively few have viewed the subject through a deception analysis lens. From those who have already applied some of these specific insights and perspectives to various issues associated with the Babington plot, this investigation has drawn heavily from the works of Charles Nicholl's *The Reckoning*; Alan Haynes' *Walsingham: Elizabethan Spymaster & Statesman* and *The Elizabethan Secret Services;* Stephen Budiansky's *Her Majesty's Spymaster*; Robert Hutchinson's, *Elizabeth's Spymaster*; John Cooper's *The Queens's Agent*; and Stephen Alford's *The Watchers*. As a consequence, these truly significant contributions in advancing research on the subject have provided an extremely valuable baseline of knowledge that contributes yet another alternative perspective on a conspiratorial event that finally rid Queen Elizabeth and Protestant England of "that devilish woman."

Regardless, the fact that events leading up to Mary Stuart's execution have been thoroughly scrutinized, studied, and analyzed by literally hundreds of Elizabethan Age experts and amateur historians alike, the tension-filled environment and sense of urgency enveloping Protestant England and predominately Catholic Europe from the late 1560s to mid-1580s provided Elizabeth's two most influential senior advisors the motive, opportunity, and means to develop and successfully execute a strategic deception/influence operation against England's mortal enemies. Developed as early as 1580, this audacious offensive-driven intelligence operation was formulated and led by the First Secretary and head of the English intelligence service, Sir Francis Walsingham, and approved and supported by his mentor, Sir William Cecil, Lord Burghley. In this article, I will summarize why and how the Babington conspirators, dedicated to freeing Mary Stuart from English control, were influenced by English agents of influence into taking actions that would paradoxically condemn the Scottish queen to the executioner's block on 8 February 1587. Additionally, the end result of this investigation has led me to conclude the following:

(1) The threat of reestablishing the Catholic faith and removing Elizabeth from the English throne increased steadily from the late 1560s to the mid-1580s, and created a heightened sense of urgency within her Privy Council to act aggressively against the threat both at home and abroad.

(2) England's very survival and ability to compete successfully against its Catholic opponents within its borders and abroad demanded an innovative change to its

national security policy and reorganization, plus centralization of its intelligence service, especially after the Northern Rebellion of 1568, Pope Pius V's excommunication of Queen Elizabeth in 1570, and the St. Bartholomew Day Massacre in 1572.

The reform of England's intelligence organization provided the means and capabilities required to develop, plan, and execute a complex, multi-level coordinated, strategic-focused intelligence deception/ influence operation.

(3) The reform of England's intelligence organization provided the means and capabilities required to develop, plan, and execute a complex, multi-level coordinated, strategic-focused intelligence deception/influence operation.

(4) By the late 1570s to early 1580s, Francis Walsingham and William Cecil had already accumulated a working knowledge of the Catholic opposition's conspiratorial *modus operandi*, discovered the opposition's focal points of activities or critical centers of gravity, and identified its key players and decision-makers both in England and abroad.

(5) Sir Francis Walsingham and Sir William Cecil were skilled, experienced intelligencers and administrators who were unequivocally dedicated to the protection of their queen, country, and religion. They were also ideally suited psychologically, emotionally, and intellectually to run a sensitive, high-risk/high-return clandestine intelligence-inspired deception/influence operation independently without the knowledge and approval of their queen.

(6) While concept development and planning phases of the offensive intelligence operation targeting the Catholic opposition began in the early 1580s, the implementation and execution phases of that plan were not put into play until 1584-85 using the Throckmorton and Parry plots as cover.

(7) The official enactment of the Bond of Association, isolation of Thomas Morgan in the Bastille, tightening of security by moving the Queen of Scots to Tutbury Castle, the irrevocable alienation of Mary from her son, James VI, and the successful control of her seemingly secure communications network at Chartley Hall by January 1586 were closely coordinated, deliberately pre-planned events specifically designed to entrap Mary Stuart in a plot to assassinate Elizabeth.

(8) Because Thomas Phelippes, Walsingham's "right-hand man," was the first person in the chain of custody to have access to encrypted communications between the Babington conspirators and Mary Stuart at Chartley Hall from January 1586 onward, Francis Walsingham had the capability to read and potentially manipulate everything that was passed through the Scottish queen's communications network.

ANALYSIS/INVESTIGATORY ROADMAP

During the process of developing and crafting the "Entrapment of Mary, Queen of Scots" hypothesis and then testing and evaluating its feasibility and plausibility within the scope and context of the Elizabethan historical period, I:

- Purposely addressed the historical events leading to the demise of the Scottish queen from a deception planner/analyst perspective.
- Highlighted assumptions from which subsequent conclusions were formulated. The conclusions are mine and mine alone. While some Elizabethan researchers, scholars, period experts, etc., may agree with these assumptions and conclusions, others may not.
- Discussed the evolution of Cecil's and Walsingham's deception/influence operation, and constructed a composite deception planning framework drawn from examples released to the public by the U.S. military services.
- Developed a realistic timetable as to when and how Cecil's and Walsingham's planning process progressed from concept development to operational execution, drawing from World War II historical examples (e.g., Operations FORTITUDE/BODYGUARD, the XX Committee's double agent program), and other deception activities that led up to the D-Day landing in Normandy.
- Focused on a number of hypothetical situations within the context of the Elizabethan environment through discussions with individuals familiar with the deception planning process. This approach provided best estimates as to the time it would take to transition from concept development to actual execution activities.
- Examined the political, religious, and economic environment which existed during the decades of the 1570s and 1580s—years in which Walsingham performed his duties as an apprentice to William Cecil (later Lord Burghley), English ambassador in Paris, and finally First Secretary and head of the English intelligence service.
- Determined that Walsingham and Cecil had the motive, opportunity, and means to conduct a

complex, interrelated strategic deception/ influence operation.

- Explained why such an aggressive, offensive-oriented intelligence operation was developed without the knowledge or approval of Elizabeth.
- Identified who specifically developed the plan, what the concept development and planning phases looked like, and then laid out the time frame in which these developmental activities took place.
- Addressed when, why, and how the implementation and execution phases of the plan evolved, particularly emphasizing how deception and influence techniques helped identify, track, penetrate, influence, control, and eventually manipulate the Morgan/Ballard/Babington-led conspirators from 1585 to the end of August 1586.

Assumption: Absence of evidence is not always evidence of absence.

Analysis best practices demand that when irrefutable facts are directly or circumstantially consistent in supporting more than one explanation of a historical event, the competing hypotheses require further in-depth investigatory scrutiny, inquiry, and consideration. The hypothesis that Mary was a fatal victim of a Cecil and Walsingham-inspired deception/influence operation fully meets this criterion.

FACTORS BEARING ON THE HYPOTHESIS: SITUATION ANALYSIS – 1568-1580

ENGLAND'S POSITION OF WEAKNESS

Very early in Elizabeth's reign it became undeniably apparent that her kingdom's national security status, when compared to that of her European competitors, was in no position to compete with them on a "one-to-one" basis. The new Queen had inherited from her half-sister a country which had lost its territorial foothold on the continent, was nearing economic bankruptcy, and was still reeling from the effects of Mary Tudor's attempts to reestablish Catholicism firmly as the state religion.

The problems facing the new Queen were summed up by a contemporary: "The Queen poor; the realm exhausted; the nobility poor and decayed; good captains and soldiers wanting; the people out of order; justice not executed; all things dear; excesses in meat, diet and apparel; division among ourselves; war with France; the French King bestriding the realm, having one foot in Calais and the other in Scotland; steadfast enemies, but no steadfast friends."[1]

Compounding Queen Elizabeth's problems was the fact that, of the approximately four million subjects living in England, an estimated 50% to 60% of them were adherents to the Catholic faith.[2] As a consequence, their reaction to the new reign of a Protestant-schooled daughter of Henry VIII and the disgraced Anne Boleyn was a highly problematic situation. Added to this concern was the fact that England was geographically isolated, surrounded by countries with larger populations and military forces, and militant in their allegiance to Rome. Without question, Elizabeth faced what appeared to be insurmountable problems that threatened her throne, her kingdom, and her religious orientation.

In 1566 William Cecil, Elizabeth's First Secretary and most influential advisor at the time, wrote:

> The succession not answered; the marriage not followed; a subsidy to be levied; the bill of religion stayed to comfort of the adversaries. Dangers ensuing: general discontentations; the slender execution of the subsidy; dangers of sedition in summer by persons discontented." Nor did things look better on the foreign front: earlier in the year Cecil had written in a confidential paper, "No prince ever had less alliance than the Queen of England hath." Elizabeth's friendless condition seemed all the more disturbing in view of the widespread fears that, on the continent, the major Catholic powers were coalescing, preparatory to mounting an offensive against Protestantism. "The Pope. . . and all his parties are watching adversaries to the Crown"… "We have heard and we hear daily of secret conspiracies and great confederacies, between the Pope, the French King, and other Princes of the Popish confederacy against all Princes Protestant and professors of the gospel, of which the Queen's Majesty is the chief patroness and protectrix at this day.[3]

A SENSE OF AN INCREASING THREAT

Assumption: Perceptions, if steadily reinforced, become realities. Sir Francis Bacon is reputed to have said that "people prefer to believe what they prefer to be true."

To make matters worse, the request of her cousin, Mary Stuart, for political protection and asylum further aggravated an already bleak situation.

On the morning of Sunday, 16 May 1568, with the possible exception of Elizabeth and her chief advisor William Cecil, many Englishmen did not understand the long-term implications of Mary's request for protection from her rebellious Protestant nobility. Even though the

"Queen of Scots most likely was not seeking permanent political asylum, she did need a resting place to rally her forces and therefore called on her cousin Elizabeth to provide her a temporary safe haven."[4] Much to the chagrin of both Mary and Elizabeth, what they hoped would be only a short respite on English soil would instead evolve into a permanent incarceration that would plague the Protestant-controlled kingdom for the next two decades.

While scholars differ over why Mary chose England as her place of refuge, rather than more sympathetic Catholic safe-havens in France, Spain, or Rome, it became an undeniable reality that the moment she crossed the English border she brought with her political and religious "baggage" that would only magnify, increasingly aggravate, and finally create irreconcilable differences between the two cousins. Mary herself quickly realized that her choice of seeking England as her temporary sanctuary was probably not a good one. In a letter dated 26 June 1568 sent from Carlyle to King Charles IX of France, she opined that "the injustices of Elizabeth or at least her Council is preparing for her a much longer sojourn in England than she would wish."[5]

From the English Catholic perspective, the Scottish queen was immediately considered a magnet and lightning rod for those committed to restoring "the old faith" to England. Not long after Mary Stuart's arrival on English shores, a substantial group of dissatisfied Catholic aristocrats in England's five northern-most counties revolted against the crown—a disturbing harbinger of more challenging threats to come.

While the northern uprising was ruthlessly put down by an enraged English queen, the precedence was indelibly set and acted as a catalyst for future, more aggressive conspiratorial activities similarly designed to overthrow Protestant rule and return Catholic orthodoxy to England. In the future, the English monarchy would face Catholic challenges at home and abroad that would prove to be even more effectively coordinated, better organized, better planned, and more lethal in intent. "The northern rising had revealed that beneath the fragile crust of religious uniformity, divisive passions bubbled."6 For the next two decades, the Catholic threat to Elizabeth's throne would significantly escalate as Mary, Queen of Scots became more involved in conspiratorial activities both in Europe and England—plots that were designed to extirpate Protestantism and the English queen from her island kingdom.

PAPAL/SECULAR THREAT ACCELERANTS EXCOMMUNICATION OF ELIZABETH – 1570

Pope Pius V

Indeed, the cruelly misjudged action of the saintly but hot-tempered Pope Pius V provided further evidence (albeit lately revealed in England) of Mary's disastrously provoking presence. Late in February 1570 came the paternal admonition, *Regnans in excelsis,* a bull of excommunication and deposition, woefully mistimed by a man who for a long time had personally admired Elizabeth. . . he told distant English Catholics that rebellion was actually a duty and obeying Elizabeth was a sin. The pontiff took on the mantle of aggressor and, in Elizabeth's mind as well as Cecil's, the bull identified the religion of perhaps half her subjects with covert treachery.[7]

In 1570 Pius V seriously complicated matters for the Protestant queen, her senior advisors, and especially Catholic-practicing English subjects by delivering a papal bull excommunicating Elizabeth from the protective arms of Rome. The impact of the Pope's edict immediately disrupted and destabilized a large segment of English society that for the previous ten years had complied with the Queen's policy of religious tolerance and compromise.

THE QUESTION OF REGICIDE

On the secular front, the question as to what lengths Catholics would go to in order to remove Protestantism from England evolved over time from guarded discussions of how Elizabeth could be removed by non-lethal means to actual planning for her assassination. While the act of regicide was already being hinted at or implicitly suggested by Mary Stuart, as her frustrations regarding the length of her incarceration grew from months into years, the uncovering of the Ridolfi plot, and later the Throckmorton and Parry plots, likewise attested to the fact that serious consideration for removing Elizabeth by non-lethal to lethal means was significantly increasing over time. (Author's Note: In varying degrees, each of these plots to destabilize Protestant control of England was supported by Catholic Spain, France, and the Pope. All three plots were also focused on removing Elizabeth from the throne of England and replacing her with Mary, Queen of Scots.)

ST. BARTHOLOMEW DAY MASSACRE – 1572

Assumption: A person who experiences an extremely traumatic or catastrophic situation will invariably remember that situation in detail for years after the event. Not only will the vividly horrendous event be permanently embedded in the person's memory, but the experience will also reinforce and strengthen any psychological biases that existed before the event.

The atrocities committed by Catholics on Protestants in Paris on St. Bartholomew's Day, 24 August 1572, undoubtedly qualify as a catastrophic event. The number of deaths resulting from the massacre in Paris was estimated at 3,000 to 4,000. For the rest of France, estimates range from 10,000 to 70,000 victims.

The long-term impact that the St. Bartholomew Day Massacre had on the English Protestant psyche was indeed profound. That event alone would remain a vivid reminder that the return of Catholicism to the kingdom could unleash the same fury and slaughter experienced under the reign of Elizabeth's sister, Mary. The horror and vividness of this horrendous example of human hatred run amok was carefully recorded by the resident ambassador in Paris at the time, Francis Walsingham. The impression left by his unsettling experience alerted his peers, many of whom sat on the Privy Council, to the future danger that awaited England should apostles of the "old faith" return.

Neville Williams wrote that "the St. Bartholomew Massacre was a grim moment for Protestantism in Europe, for the news from France was interpreted as an evil conspiracy by the powers of the Counter-Reformation and yet, before long, it provoked greater solidarity among Protestants of different persuasions and countries than any other single event.[8] Seconding Williams in his sentiments, G.J. Meyer stated: "What matters here is that the massacre of 1572 horrified the Protestants of England, [and] seemed to provide rich justification for their insistence that Catholicism had to be extinguished . . ."[9]

JESUIT "FIFTH COLUMN" INFILTRATION – 1577-1580

While Jesuit infiltration from France into England was identified as early as 1574, by 1577 the Bishop of London warned Francis Walsingham of the rising threat caused by returning Catholic missionaries. Based on numerous reports from other peers all over England, the Bishop reported that "the Papists marvelously increase both in numbers and in obstinate withdrawing of themselves from Church (Protestant-supported) and service of God." He was adamant that the only way of countering this disturbing trend was to formulate legislation which would make the Catholics' lot more unpleasant.[10] As a result of the Bishop's concerns, the English Privy Council imposed more stringent laws that heavily penalized subjects found supporting and protecting Catholic missionaries from Europe. In 1580 a second wave, encompassing the most dynamic, effective, and troublesome group of approximately 100 Jesuit "Soldiers of God," began infiltrating into England from abroad.[11/12]

By the years 1580-83, the process of political and religious polarization in England was quickly reaching a breaking point. Sir Francis Walsingham and his mentor Lord Burghley were convinced that the time had come to recapture the initiative from adversaries dedicated to their destruction. Consequently, they boldly set forth to develop an innovative high-risk/high-return, offensively-focused course of action that would take the fight to the enemy. Interestingly, Mary Stuart, the constant rallying point for anti-Protestant activities, would be used as a "stalking horse" and centerpiece of that plan.

MOTIVE TO DECEIVE/REDRESS THE POWER IMBALANCE

Given the fragile status of the Queen, country, and Protestantism, and the growing threat posed primarily by the Catholic forces of Spain, France, and the Papacy, Cecil and Walsingham were faced with a challenge that required a radical change in national security policy direction. The First Secretary and Lord Treasurer needed to buy more time to develop new, innovative courses of action that would eventually redress the power imbalance which existed between England and its powerful adversaries. In so doing, they would eventually place their country on an equal footing with revenge-seeking competitors.

RIGHT MEN, RIGHT TIME

Assumption: William Cecil, Lord Burghley, and Francis Walsingham were familiar with the writings of Thomas More and Niccolo Machiavelli and applied the principles espoused in *Utopia* and *The Prince* in their government duties.

Left: William Cecil; Right: Francis Walsingham

Key to the development and future success of the plan was the recruitment of Francis Walsingham. Like Cecil, Walsingham was an extremely talented, well-educated and -traveled man who shared the First Secretary's appreciation of the Renaissance and its new political philosophies embodied in the works of More and Machiavelli. While more doctrinaire than his mentor, Walsingham also shared a deep distrust of anything that smacked of the Romish religion which was further enflamed by the physical presence of Mary Queen of Scots on English soil.

Working with a unity of purpose, while at the same time complying with their Queen's national security priorities, the two men struck a more indirect, less visible, and non-confrontational path vis-à-vis their adversaries on the continent. Consequently, their new strategy (an indirect preemption approach) provided them the space, time, and opportunity to rebuild and revitalize what at that point was becoming an outdated, ineffective, and counterproductive national defense structure.

MEANS TO DECEIVE

One key initiative in advancing this low-profile, indirect, preemptive strategic approach focused on the restructuring, reorganization, and centralization of the English intelligence arm of government. Steeped in the principles of the Renaissance, Cecil and Walsingham adhered to the dictum that "Knowledge is Power," and believed that a reformed, revitalized, expanded, and more effective, offensive-oriented information-gathering institution would in the future play a significant role in leveling the international religious, economic, military, and political playing field.

To their way of thinking, intelligence, if properly applied, would become not only the means of determining enemy military capabilities and intentions but, if utilized to its fullest, would become a silent offensive weapon eroding from within the very foundation of future Catholic conspiratorial activities. Both men would pin their hopes, careers, and even lives on using deception and influence activities as the key to their queen's and country's ultimate survival.

DECEPTION FRAMEWORK

The increased infiltration of Jesuits and other orders of Catholic-inspired missionaries from the continent into England threw even more fire on fear that Elizabeth's kingdom would break out into an uncontrollable religious conflagration. The urgency to counter the Catholic threat and the sense that something had to be done became palpable within the English court.

Circa 1580, Walsingham, with Cecil's full cooperation and support, created a newly restructured intelligence organization that now possessed a greater capability to take the fight to its implacable Catholic foes. Given the renewed Catholic infiltrations into England, both men feared that their religion's, queen's, and country's survival was being put at greater risk. Knowing the import and sensitivity of what they were about to do, and taking into consideration their Queen's past unpredictable behavior, Cecil and Walsingham, without Elizabeth's knowledge, commenced to develop a rudimentary deception/influence plan specifically designed to counter and defeat future Catholic conspiratorial activities.

During this formative period in their planning process, broad goals and objectives were discussed and a general "concept of operations" framework developed. Also at this early conceptual stage, they considered and assessed the potential risks, costs, benefits, and unintended consequences (the what if's) that could arise should the plan actually be put into play.

CHRONOLOGY OF CATHOLIC AND PROTESTANT EVENTS

Red/Bold – Catholic Actions/Blue – Protestant Actions/
Black – Deception Planning Evolution

1560s

- **Spain suppresses Protestants in the Low Countries**
- England provides financial support to Scottish Protestants
- **Mary seeks asylum in England (1568)**
- **English nobles in northern England revolt (1569)**
- Elizabeth brutally "puts down" the northern uprising (1569-70)

1570s

- **Pope excommunicates Elizabeth (1570)**
- **Ridolfi Plot supported by Pope, Spain, and France (1571-72)**
- Ridolfi Plot defeated
- **St. Bartholomew Day Massacre (1572)**
- English intelligence (Robert Beale) produces a dire assessment of future Catholic threat
- Cecil becomes Lord Treasurer; Walsingham becomes First Secretary (1573)
- **First wave of Jesuit infiltration into England (1575)**
- Cecil/Walsingham develop indirect preemption strategy; intelligence reorganization begins
- **Desmond uprising in Ireland (1579)**

- **Second wave of Jesuit infiltration into England (1579)**
- **Increasing reports of Spain preparing to invade England**

1582-1584
OPPORTUNITY TO MOVE FORWARD

The opportunity to add flesh to the skeletal deception/influence concept arrived in mid- to late 1582 when the Catholic-inspired Throckmorton plot was uncovered. Using their queen's outrage and demands for immediate aggressive countermeasures against her Catholic plotters, Cecil and Walsingham used the situation to cover or hide "in plain sight" the more detailed planning and implementation activities required to make their secret and extremely sensitive offensive deception/influence operation a future reality.

It was during this critical 2-year period that Elizabeth's two most trusted advisors were able to anticipate more clearly what the follow-on threat would look like once the Throckmorton conspirators were successfully defeated. This invaluable insight also permitted them the ability to focus their efforts more intensely on the resources required to target specific individuals and Catholic conspiratorial centers of gravity in England and France.

1585
PHASE ONE: DECEPTION EXECUTIONS BEGIN

The assassination of William of Orange in July 1584 was quickly followed by two more abortive attempts to violently replace Elizabeth with Mary and her Catholic sympathizers. These acts alone fortuitously provided Cecil and Walsingham the justification and *raison d'etre* to put into motion finally a series of carefully pre-planned, coordinated, interrelated, and mutually supporting deception-focused initiatives that would specifically target key adversary "centers of gravity."

As a result of their efforts, by the end of the year the legal justification to execute Mary was enacted; Mary and her chief intelligence officer had been physically isolated from their support systems; key conspiracy centers of gravity had been successfully penetrated; key personnel in England and in Paris had been identified and were being closely watched and influenced by English intelligence agents; the Scottish queen's hope to share with her son the governance of Scotland was irrevocably dashed; and Mary's means of communication with her Catholic supporters was totally under Walsingham's control.

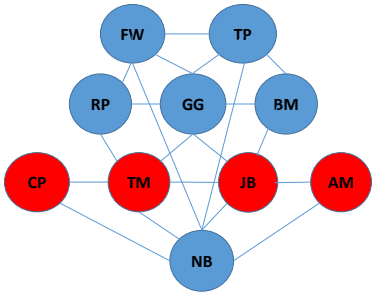
ENGLISH INFILTRATION OF CATHOLIC CENTERS OF GRAVITY

The core planning cell in Paris supporting the Babington plot had been penetrated by Walsingham's agents no later than June 1585. In all likelihood, Thomas Rogers (alias Nicholas Berden) was already reporting on English exile activities before Robert Poley gained access. Gilbert Gifford and Bernard Maude infiltrated the cell no later than 1585 and early 1586, respectively.

Infiltration of the Catholic Paris Planning Group (Center of Gravity) - Diagram 1

Conspirators
CP – Charles Paget
TM – Thomas Morgan
JB – John Ballard
AM – Amb. Mendoza

Agents/Agents of Influence
FW – Francis Walsingham
TP – Thomas Phelippes
RP – Robert Poley
GG – Gilbert Gifford
BM – Bernard Maude
NB – Nicholas Berden* (befriended Ballard (1581); with Ballard in Rome (1584) who sought approval to assassinate Elizabeth; reported activities surrounding Morgan and English exiles in Paris; recalled to London and continued work (1585))

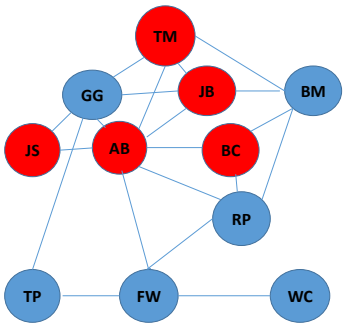


By the time Mary and her entourage were moved to Chartley Hall from Tutbury Castle on 24 December 1585, Walsingham's newly developed communications intercept system was already in place. By mid-January 1586, Mary was convinced that this newly acquired means to communicate with her supporters in England and abroad was secure from Protestant eavesdropping. From that point onward, Walsingham had total access to all message traffic flowing into and out of Chartley Hall.

Infiltration of the Babington Group (Center of Gravity) - Diagram 2

Conspirators
TM – Thomas Morgan
JB – John Ballard
JS – John Savage
AB – Anthony Babington
BC – Babington Cadre

Agents/Agents of Influence
GG – Gilbert Gifford
BM – Bernard Maude
RP – Robert Poley
TP – Thomas Phelippes
FW – Francis Walsingham
WC – William Cecil

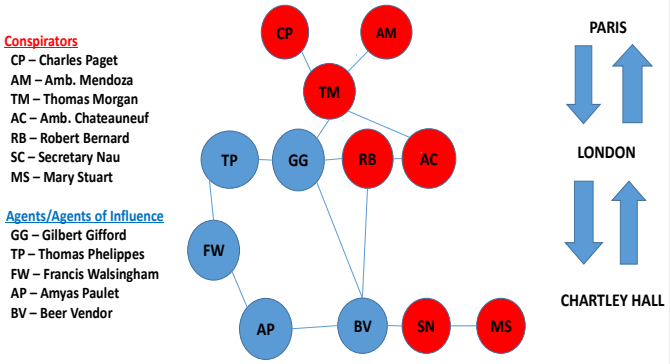


1586
PHASE TWO: INFLUENCE EXECUTIONS BEGIN

To secure his last turn of the screw, Walsingham now devoted his best energies. Therewith began one of the most incredible, though documentarily attested, acts of perfidy known to history—the "frame-up by which Walsingham made Mary Stuart privy to a plot of his own manufacture, the so-called Babington conspiracy, which was in reality a Walsingham conspiracy."[13]

Walsingham and Cecil now faced the most critical phase of the operation—that of causing the Catholic conspirators to assist them unwittingly in directly implicating Mary Stuart in the plan to kill her royal cousin Elizabeth Tudor. The success or failure of Elizabeth's two most senior and influential advisors was totally dependent upon their leadership skills and Sir Francis' field agents' ability to encourage, influence, or manipulate the key plotters' decisions, behaviors, and actions within the three Catholic decision-making centers of gravity. By that time, John Ballard had met with Anthony Babington and his supporters in March 1586. Walsingham's agents of influence—Gifford, Poley, and Maude—had already successfully infiltrated this critical Catholic center of gravity based in London.

Infiltration of Mary's Communication Net (Paris/French Embassy/Chartley Hall) - Diagram 3



For the next nine months, Walsingham with his group of intelligencers, watchers, and agents of influence would unswervingly work with singleness of purpose to successfully accomplish what had started as just an idea approximately six years before—how to eliminate from the world stage England's nemesis, Mary, Queen of Scots. In successful pursuit of that objective, Walsingham through his intelligence mechanism promoted a number of themes or stories designed specifically to influence the Babington conspirators' and the Scottish queen's actions. With Walsingham's support and direction, Gifford, Poley, and Maude focused their attention on encouraging conspirator beliefs, behaviors, and activities that would:

- Convince John Ballard and Thomas Morgan that English Catholic support for the plot was much greater than actually existed.
- Ensure that Babington's fellow conspirators in London remained committed to the objectives of the plot—invasion of England and assassination of Elizabeth.
- Delay John Ballard's escape from England to France after he learned that English Catholic support was much less than expected and Bernard Maude was discovered to be an English spy.
- Improve and expand Walsingham's capability to conduct damage control measures after Maude's cover as a loyal Catholic and confidant of Ballard was compromised.
- Place Robert Poley in a position that would significantly influence Babington's decisions and actions.
- Directly involve and implicate Mary, Queen of Scots in the plot.
- Buy time for the plot to fully develop by surrounding Babington with ambiguous situations in order to maximize the number of plotter arrests.
- Reinsert Gilbert Gifford back into the Catholic center of gravity in Paris once the Babington conspiracy was successfully defeated and Mary was executed.

The successful accomplishment of Walsingham's primary objective—the elimination of Mary, Queen of Scots—was finally realized at Fotheringhay Castle on 8 February 1587.

CHRONOLOGY OF CATHOLIC AND PROTESTANT EVENTS

Red/Bold – Catholic Actions/Blue – Protestant Actions/
Black – Deception Planning Evolution

1580s

- **Pope excommunicates William of Orange (1580)**
- **Second wave of Jesuit infiltration into England (1580)**

- Deception/influence planning begins—concept development phase (1580)
- **Catholic seminary established at Rheims for English adherents (1581)**
- **Throckmorton plot active (late 1582-84)**
- **Somerville incident focused on assassinating Elizabeth uncovered (1583)**
- **William of Orange assassinated (1584)**
- Deception/influence plan transitions to implementation phase (1583-84)
- Domestic surveillance and military preparedness activities in England significantly increase
- **Parry plot to assassinate Elizabeth uncovered (1584-85)**
- England provides financial and manpower support to Protestant rebellion in the Low Countries (1585)
- **Spain declares war on England (1585)**
- **New Catholic plot begins to develop in Paris (1585)**
- Deception/influence plan transitions from implementation to execution phase 1 – identification/penetration of new (Babington) plot (1585)
- **Babington plot becomes active**
- Deception/influence plan transitions from execution phase 1 to phase 2 – influence activities against plotters (1586)
- Mary, Queen of Scots executed at Fotheringhay Castle (February 1587)

1587-1603
THE QUEEN IS DEAD, LONG LIVE THE FUTURE KING

Consequently, what positive gains were attained by such an audacious, unprecedented, and controversial act of premeditated violence that Walsingham and Cecil perpetrated against an internationally-recognized royal queen?

First, it physically removed the symbol of Catholic resistance both in England and on the continent. Granted, the execution would potentially increase the likelihood that Catholic initiatives to replace Elizabeth and return the old faith to the English shores could accelerate. However, given intelligence reports about significant delays encountered with the building and provisioning of the Armada, and the lack of the Catholic opposition's interest in using tangible force in retaliation for such an act, the First Secretary and Lord Treasurer determined that the benefits of executing the Scottish queen far outweighed the potential negative consequences of such an action. They were not disappointed in their decision.

Second, eliminating Mary from the scene bought England the much needed time required to concentrate solely and focus its attention on improving its military force structure, readiness posture, and defensive/offensive capabilities in anticipation of a Spanish invasion from its formidable fleet and ground forces located in the Low Countries. As a consequence, England's unity of effort to marshal and coordinate the limited resources available to the English crown, coupled with the dilatory indecisiveness of Spain's leadership and just plain bad luck, were significant factors in the surprising defeat of the Spanish Armada in 1588.

The removal of Mary and the successful defense of England against the "English Enterprise" ensured in the short term that Elizabeth would sit secure on her throne and that Protestantism would remain the official state religion throughout the land. Yet, the apparent success surrounding the execution of Mary and the defeat of the Spanish Armada would turn out not as sweet as Elizabeth had hoped it would be. Little did she know that her counselors in negotiations with the King of Scotland (James VI) had already agreed that, at her death, Elizabeth would be succeeded by the son of the very woman she had spent so many years expending time, resources, and energy in keeping under "lock and key.'"

Mary and young son, James VI

The irony of that eventuality would certainly have been grudgingly understood by the rapidly failing Virgin Queen had she known about the "backroom dealings" that would bring Mary's son, officially recognized as King James I, to the English throne in 1603. However, perhaps ignorance of events swirling around her mercifully spared Elizabeth the ultimate

humiliation. She would never know that with her demise the Tudor dynasty would pass into history and be replaced by her hated cousin Mary Stuart's ancestral line. In a way, perhaps Mary Stuart, Queen of Scots, did reign victorious after all.

A FINAL POINT

> *There is a principle which is a bar against all information, which is proof against all arguments and which cannot fail to keep a man in everlasting ignorance—that principle is contempt prior to investigation.*
>
> - Herbert Spencer

When viewed from a deception planner/analyst perspective, what first appears to be a series of seemingly independent, random, and coincidental events in 1585 (e.g., Mary's move to Tutbury Castle, enactment of the Bond of Association, relief of Shrewsbury and replacement of Paulet as Mary's custodian, Morgan's incarceration in the Bastille, James VI's alienation from his mother, development of a new intercept system of the Scottish queen's communications network, and the relocation of Mary to Chartley Hall) can just as easily be explained as a sequential series of preplanned, coherent, mutually supporting events that were purposely designed to eliminate Mary Stuart from the anti-Protestant equation. Adding even more credibility to this little explored hypothesis is the fact that England was indeed fortunate to have in place two men of great genius and talent who possessed the motive, opportunity, and means to develop and unleash such an unprecedented, truly momentous, trailblazing anti-Catholic undertaking.

Hopefully, my "search for truth" will further spur future academic, intelligence, and military interest and inquiry into a subject area that continues to be a long-standing contentious, historical event—an event that unquestionably provides important lessons and insights for both current and future students interested in the "art" of deception. At the very least, I hope my conclusions have provided the reader additional "food for thought."

NOTES

[1] Luke, Mary M., *Gloriana: The Years of Elizabeth I*, pp. 32-33.
[2] Ibid., p. 473.
[3] Somerset, Anne, *Elizabeth I*, p. 191.
[4] Cooper, John, *The Queen's Agent: Sir Francis Walsingham and the Rise of Espionage in Elizabethan England*, pp. 50-51.
[5] *Letters of Mary, Queen of Scots*, Vol. 1, p. 85.
[6] Somerset, Anne, *Elizabeth I*, pp. 240-241.
[7] Haynes, Alan, *The Elizabethan Secret Services*, p. xxi.
[8] Williams, Neville, *The Life and Times of Elizabeth I*, p. 117.
[9] Meyer, G.J., *The Tudors: The Complete Story of England's Most Notorious Dynasty*, p. 498.
[10] Somerset, Anne, *Elizabeth I*, p. 385.
[11] Alford, Stephen, *The Watchers: A Secret History of the Reign of Elizabeth I*, p. 125. Stephen Alford estimates that by the end of Elizabeth's reign approximately 470 missionaries had infiltrated England. Of that number, 116 were executed, 294 were sent to prison (17 died while incarcerated), and 91 were banished from the kingdom.
[12] Cooper, John, *The Queen's Agent: Sir Francis Walsingham and the Rise of Espionage in Elizabethan England*, pp. 143-145. John Cooper estimates that by 1586 there were approximately 300 missionaries in England. Of that number, 33 had been executed, 50 were in prison, and 60 were banished from the kingdom.
[13] Zweig, Stefan, *Mary Queen of Scotland and the Isles*, pp. 310-312.

R. Kent Tiernan received a BA in History from Stanford University (1967) and an MA in Western European Area Studies from the University of Notre Dame (1971), after which he served 20 years in the U.S. Air Force. Before retiring from the military in 1987, he headed the Air Force Intelligence Service's Special Studies Division, which focused on foreign denial and deception tactics, techniques, and procedures. From 1989 to 2000, Kent was employed as a defense contractor and provided planning, analysis, and training support to the Joint Staff, DIA, NSA, and the U.S. Army and Air Force. In May 2000 he joined the CIA/NIC Foreign Denial and Deception Committee (FDDC) staff. In 2008 he was promoted to the Senior National Intelligence Service, where he held the position of FDDC Vice Chairman and Staff Director until his retirement in July 2014. His article, "Hiding in Plain Sight", originally published in the Defense Intelligence Journal *in 2006, was reprinted in* AIJ, *Vol. 32, No. 2, 2015, which explored the theme "Denial and Deception".*

NMIF Bookshelf

THE SPY WHO COULDN'T SPELL: A DYSLEXIC TRAITOR, AN UNBREAKABLE CODE, AND THE FBI'S HUNT FOR AMERICA'S STOLEN SECRETS.

Yudhijit Bhattacharjee.
New York, New American Library. 2016.
292 pages.

Reviewed by Mark W. Cleveland, a faculty member at National Intelligence University. He has served at the National Security Agency in various operational positions and is currently the NSA/SIGINT Chair at NIU.

Rocked by the recent actions of insiders like Edward Snowden and Chelsea Manning bent on divulging vast troves of sensitive information, the U.S. Intelligence Community faces a stark challenge in the digital age, when security breaches can include loss of secrets on an unprecedented scale. Against this backdrop, Yudhijit Bhattacharjee provides a well-crafted examination of a relatively obscure traitor—Brian Patrick Regan—who while working for the National Reconnaissance Office (NRO) in the years before 9/11 exploited his access to download over 20,000 classified documents and electronic media which he sought to sell to an array of hostile nations for millions of dollars. The author relates the absorbing tale of how the Federal Bureau of Investigation (FBI)—using computer forensics, cryptoanalysis, and extensive surveillance—was able to forge a case that led to Regan's arrest in August 2001 as he prepared to board a flight out of the country, halting his scheme before a foreign buyer could be found and ultimately resulting in his conviction and sentencing to life in prison.

Bhattacharjee, a former staff writer for the journal *Science*, is well-established as an award-winning essayist on topics ranging from astronomy and cybercrime to medicine. This, his first book, is based on an earlier article he wrote about Regan for *Wired* that appeared in 2010. Narrated in a fast-paced manner that showcases his ability to offer insightful and informative popularizations of technical issues, Bhattacharjee is able to weave an engaging and complex tapestry for the reader. The work includes effective elements of a who-done-it mystery, as the FBI pursues a tip that someone employing complex coded communications is attempting to sell secrets to Libya; a probing psychological portrait of a traitor, whose betrayal appears prompted by a lifelong sense of resentment coupled with the desire to escape debt; and, finally, a counterespionage thriller, detailing code systems, buried dead drops, anonymous communications, digital sleuthing, and old-fashioned detective work, leading to arrest and trial.

The book opens with a tantalizing description of a 2001 visit to a Long Island high school by a former student, who was returning years later on a surreptitious mission undertaken as part of an act of treason. According to Bhattacharjee's account, the early years had been difficult for this shadowy, unnamed former student who had come back to bury a laminated phone list outside the school. Lumbering, dyslexic, and socially awkward, as a youth he had been taunted and dismissed as dimwitted by classmates and teachers. Even after he had joined the military and embarked on a career within the IC, his intellect and ability were not accorded the respect by colleagues or supervisors that he felt was due. Underestimated throughout his life, he conceived of a cunningly complex plan to steal a huge store of classified information which he hoped to sell for millions of dollars, yielding a fortune that would erase financial debt and earn broader esteem. By withholding Regan's identity at the outset, and focusing on motives and elements of tradecraft, the author sets the stage for the first section of the book, which deals with a classic spy hunt.

The tip that began the search for the traitor came from an informant in the Libyan consulate. The material obtained by the FBI included coded messages from someone purporting to work for the CIA and samples of classified documents such as the most recent table of contents of the *Joint Tactical Exploitation of National Systems* (JTENS) manual, as well as satellite images and intelligence reports covering Middle East topics. The documents clearly indicated that the source had access to U.S. classified information. Bhattacharjee, in exploring the methodology used by the FBI and other agencies across the IC to narrow the range of suspects, offers an informative discussion of some basic principles of encryption and decipherment, including plaintext, keys, and brevity codes, to explain the nature of the encoded letters used by the spy. Meanwhile, the author also walks the reader through the fascinating work involved in identifying an active traitor by painstaking analysis of system audit data of the internal intelligence network known as INTELINK. Eventually the trail leads to the NRO and Brian Regan.

The author then offers a sketch of Regan's early years, underlying character, and motivations. Based on interviews with the forensic psychologist on Regan's legal defense team, as well as childhood friends, acquaintances, and

colleagues, the picture Bhattacharjee presents is disturbingly banal. Regan came from a large family with a working class background and grew up on Long Island. He was something of a social misfit whose dyslexia made reading and writing a challenge and school an embittering experience. Despite a rocky start, Regan's life seemed to improve after he joined the Air Force, received training in intelligence, married, and started a family. He enjoyed several overseas postings and later was selected to attend the Joint Military Intelligence College prior to being assigned to NRO in 1995. Although on the surface Regan appeared to be doing well—with a career and family—he felt under-appreciated at work and was living well beyond his means. Rather than curb expenses, Regan began to entertain the idea of committing espionage to transform his fortunes. [Editor's Note: The Joint Military Intelligence College (JMIC) became the National Defense Intelligence College in 2006 and since 2011 has been the National Intelligence University (NIU).]

Regan's access to INTELINK allowed him to search, download, photocopy, and then remove thousands of sensitive documents. He devised an elaborate scheme which involved burying caches of classified material and then contacting foreign governments using encrypted messages with the goal of trading coded coordinates of the sites in exchange for a massive payment. Once he put the plan into motion by contacting the Libyans, the narrative races between Regan's efforts to find a buyer and the FBI's investigation zeroing in on him as the prime suspect. This fast-paced section of the book offers a detailed view of the cat-and-mouse surveillance involved in confirming his role as a traitor—including hidden cameras in his office, network forensics, FBI tails at the public library, Foreign Intelligence Surveillance Act (FISA)-based monitoring of his home phone, and vehicle surveillance—all of which culminates in his arrest at Dulles International Airport.

The final portion of the book briskly explores more fully the details of Regan's complex plan, his coding systems, a convoluted attempted cover-up, his stubborn refusal to accept a plea bargain, and the trial itself. Finally, Bhattacharjee explains the critical effort to recover the lost material. As part of the sentencing arrangement, Regan agreed to explain his codes and help the government locate and dig up the hidden documents from a total of 19 sites in Pocahontas State Park in Virginia and Patapsco Valley State Park in Maryland. Even with his assistance, this was a frustrating challenge for the authorities as elements of the coding confounded even Regan, who had forgotten some of the techniques he had used. The description of the work involved in trying to crack the elaborate coding system may be too detailed for some, but is interesting for those readers drawn to intricate puzzles and code-related challenges.

In the closing section, Bhattacharjee grapples with the internal contradictions presented by this case. Regan's encryption systems are described as "unbreakable" but are so confusingly cumbersome that Regan himself lost track of the multilayered keys required to unravel them. His plan is characterized as brilliant but is marred by repeated blunders and amateurish tradecraft, such as renting a storage locker under the name Patrick Regan (dropping his first name) and being tossed out of the Libyan embassy in Bern, Switzerland, after naively visiting without any tangible material to prove his *bona fides*. Bhattacharjee's Regan comes across as somewhat pathetic, a crafty but self-destructive loser whose money problems and resentments prompt him to betray his country in an attempt to get rich. No ideologue, Regan is reminiscent of spies like Ronald Pelton and William Kampiles, motivated chiefly by personal frustration and greed. "My goal was never to bring harm to the United States... I just needed the money," Regan said years afterward in a prison interview.

Bhattacharjee has written a highly engrossing work that sheds light on a lesser- known spy whose downloading and theft of a huge volume of classified material foreshadowed the now well-understood risk presented by insider access to vast stores of classified digital records. Aimed at a general audience, the book unfortunately lacks citations and references and has a journalistic rather than a scholarly tone. Nevertheless, it is a worthwhile addition to the larger body of literature on counterespionage and offers a gripping tale of treachery, code-breaking, and investigative techniques that are blended in an effective and highly readable manner.

[Reviewer's Note: The views presented here are my own and do not represent those of NSA or NIU.]

• •

THE INTELLIGENCE WAR IN LATIN AMERICA, 1914-1922

Jamie Bisher.
Jefferson, NC, McFarland & Company, Inc. 2016.
418 pages.

Reviewed by Dr. Russell G. Swenson, retired, former Director of Research, National Intelligence University, and former analyst for both the U.S. Air Force and the Congressional Research Service. He holds master's and PhD degrees in geography from the University of Wisconsin-Milwaukee and is fluent in Spanish. He taught an elective on Latin America at NIU's predecessor institutions for several years.

The author of this absorbing exploration of World War I intelligence machinations in the Americas is a U.S. Air Force Academy graduate and USAF counterintelligence veteran

who has unearthed and synthesized the backstory of hundreds of declassified documents housed in National Archives and Records Administration (NARA) facilities. He complements the narrative with photos from the historical collections of NARA and the Library of Congress (LoC). His interest in the topic began when he accidentally stumbled across secret surveillance summaries originating in 1918 Buenos Aires. This archival discovery stimulated his multi-year combing through threads of information untapped by intelligence scholars, and perhaps never consolidated at all by contemporary intelligence analysts and agencies.

FORMAT AND APPROACH

The book's eight chronologically organized chapters cover each year from 1914 through 1921, and this sensible scheme extends to the bibliography where NARA and other archival documents are similarly listed chronologically. This approach offers scholars a means of readily tracking and appraising what would otherwise remain a jumbled list of primary sources. The large 8½ x 11-inch format lends itself to the three-column text used in the book's 400+ pages. The layout allows the word space for adequate attention to biographical details and character development for many of the numerous intelligence actors whose exploits require lengthy attention for a full accounting of multinational intelligence schemes and counterintelligence activities.

This reviewer is aware of only three books in English on topics related to Bisher's work that have been published since 2008: Charles Harris and Louis Sadler, *The Secret War in El Paso: Mexico Revolutionary Intrigue, 1906-1920* (University of New Mexico Press, 2009); Thomas Boghardt, *The Zimmermann Telegram: Intelligence, Diplomacy, and America's Entry into World War I* (Naval Institute Press, 2012); Howard Blum, *Dark Invasion: 1915 — Germany's Secret War and the Hunt for the First Terrorist Cell in America* (HarperCollins, 2014). Their narrow focus contrasts with the broad geopolitical sweep of Bisher's work. Only one other book approaches the meticulous attention to detail and import to intelligence history on display here: Colonel (USAF) Terrence J. Finnegan's *Shooting the Front: Allied Aerial Reconnaissance and Photographic Interpretation on the Western Front—World War I* (National Defense Intelligence College, 2006). [The reviewer was director of the NDIC Press at that time.] Bisher and Finnegan both document the signal importance of WWI as a testbed for the birth of a worldwide focus for U.S. intelligence efforts.

The extensive use of historical photos in *The Intelligence War in Latin America 1914-1922*, in conjunction with the document-based narrative, bring together and bring to life the espionage panorama in the Americas during and just after WWI. NARA and LoC records frequently provide evidence of multinational intrigue in declassified documents originally made available only to high-level U.S. government officials of the era. The author stitches together photographic and documentary evidence with reasoned inference in a manner reminiscent of a Ken Burns documentary. Bisher's integration of evidence for U.S. and foreign intelligence activity brings an internationalist or net assessment slant to this synthesis of WWI-era intelligence activity in the Americas.

CONTENT

By 1915, many of the tens of thousands of German immigrants in Chile supported the hemisphere-wide, German covert *Etappendienst* intelligence and logistics network. These fifth-columnists helped the surreptitious resupply of German merchant vessels which in turn provisioned German naval vessels in Pacific shipping lanes (pp. 35-38). German intelligence in the U.S., working out of offices in New York City under military attaché Franz von Papen, employed German immigrants from Latin America to carry out sabotage against U.S. commercial military infrastructure targets that could eventually hinder German war efforts (p. 34). A German intelligence objective was to promote political divisiveness in Mexico and thereby keep the U.S. more interested in this neighbor's affairs than those of the Central [European] Powers. William Jennings Bryan, briefly Secretary of State for President Wilson, disdained intelligence, but one of his political appointees, Zach Cobb, became a key intelligence figure as Collector of Customs in El Paso. In typically thorough fashion, Bisher develops a vignette of Cobb's energetic approach to information collection that allowed him to arrest Mexico's insurrectionist General Victoriano Huerta, a deposed former ruler of Mexico, as he tried to re-enter Mexico from the U.S. to stir up politically motivated violence, with clandestine German assistance (pp. 53-55).

1916 saw the confluence of political, diplomatic, economic, and military threads into a sharper U.S. strategic intelligence picture. Zach Cobb emerged as a conduit for transmitting frontline information to the Secretary of State and President Wilson. Cobb established and benefited from the development of a joint intelligence center in El Paso (p. 73) to coordinate information collection and operational support among the State Department, the Department of Justice's Bureau of Investigation, and military intelligence—a little-known precursor to today's El Paso Intelligence Center. German intelligence remained involved in the Americas by introducing biological warfare—coordinated out of the U.S. and Argentina—to sicken or kill livestock bound for the Allies in Europe.

Chapters covering 1917 and 1918 earn more pages of coverage than other years, as German intelligence agents and their local compatriots in Latin American countries encountered increasingly capable U.S. intelligence forces across the hemisphere in the contest for allegiance between the Allied and Central Powers. Bisher shows that the framework of a U.S. Foreign Intelligence Community emerged in 1917 with organic roles for a Censorship Board, the Secret Service, the Army's Military Intelligence Division (MID), the American Protective League (counterintelligence), the Office of Naval Intelligence, State Department Intelligence (Office of the Counselor), the Office of Investigation (Justice), the War Trade Board, the War Shipping Board and, not least, Allied intelligence (foreign intelligence liaison across the Americas). The Justice Department's Bureau of Investigation grew rapidly in these years, allowing a young J. Edgar Hoover to show his special skills. The Bureau posted agents in Mexico, Central America, and Cuba, in addition to tapping trusted travelers to report on conditions in South America (pp. 110-111).

The author's vignettes of U.S. agents and their targets often derive directly from primary archival documents. An engrossing example comes from the U.S. military intelligence effort to win the support of Central Americans for the Allied cause through propaganda. This effort became the chief concern of a 53-year-old, super-patriotic, downhome-style operator from Sundance, Wyoming, Charles Waite. Bisher tracks Waite's movements and actions, and interprets his thinking with the help of extensive records of his communication with MID headquarters. After a brief return to Washington, Waite became a State Department agent in Colombia, sent there to report on rumored German efforts to secure valuable metals like platinum from backwoods mining operations. Bisher includes extensive portions of one of Waite's colorful reports, in which he nonchalantly tells of using superior horsemanship to bump a mounted German intelligence operator off a 2,000-foot Colombian cliff while investigating a suspected enemy clandestine communications facility (pp. 232-233). Despite celebrations of the November 2018 Armistice among soldiers and sailors, intelligence organizations and their operators naturally had to continue fulfilling duties in the field and at home.

In 1919, within the shrinking intelligence bureaucracy, Herbert Yardley, the father of U.S. cryptography, preserved code-breaking capabilities in an interagency Cipher Bureau, employing holdover specialists and hidden funding from State and the Army's MID. It fell to the U.S. Coast Guard to ensure that intelligence collection and interagency coordination remained up to date in the inter-war period. For more details, see Eric Ensign, *Intelligence in the Rum War at Sea: 1920-1933* (Joint Military Intelligence College, 2001).

In 1920 Bisher finds evidence that Mexican, German, Japanese, Argentine, and Chilean intelligence officials acted in collusion, aiming to lead most of the major countries of Latin America into support of the upstart Latin League in a campaign against continued U.S. hemispheric initiatives. In Guatemala, Bisher recounts how the riotous end to a dictator's reign was assessed and reported by a stalwart military attaché, proving the peacetime value of maintaining attaches throughout the region.

In a chapter on espionage activities in 1921 and beyond, the author points out that the Office of Naval Intelligence, together with MID, predominated in tracking—but not otherwise countering—anti-U.S. plots fostered by a growing list of geopolitical enemies and sometime friends. The list widened to a Japanese-British-Chilean-German-Argentine-Mexican-Italian nexus and by 1922 incorporated Communist agents and sympathizers. The multilateral, espionage-abetted plotting came to an apparent end as a result of negotiations during the late 1921 Washington Naval Conference. Justice's Office of Investigation did not expand its Latin American surveillance beyond Central America in this time frame; it was not until WWII that J. Edgar Hoover's FBI embarked on a wholesale counterintelligence program across the hemisphere.

The final chapter of the book, "Epilog — Destiny, Doom, and Legacy," ties up biographical threads intermittently detailed in earlier chapters, bringing a career-long narrative perspective to the life story of numerous Latin American, North American, Allied, German, and Japanese intelligence officials and operatives. The author points out that the intelligence contributions of some key figures in WWI were never recognized in their biographies or obituaries.

CONTRIBUTION AND CONTEXT

The author does accomplish the book's objective—"to bring to light and make sense of the intelligence war in Latin America during World War I." Further, he manages to maintain coherence through the long narrative. Vignettes of the activity of notable personalities, among them Zach Cobb and Charles Waite, appear in more than one chapter. This scheme brings welcome continuity to the book's chapters, and entices a reader into an appreciation of how individual as well as group motives and aspirations affected the intelligence war effort from one year to the next.

The narrative also benefits from detailed attention to the exploits of well-known intelligence figures. For example, Bisher describes the 1915 cross-country trek by the fugitive German spy, Navy Lieutenant Wilhelm Canaris (p. 61), along a trading path blazed in 1894 by a German immigrant to Chile, across the chain of lakes and low

Andean passes between Lake Llanquihue in Chile and Lake Nahuel Huapi in Argentina to the new village of Bariloche (the same route taken by Che Guevara on his motorcycle adventure across the mountains in 1952, and by thousands of tourists today). This is the same multilingual Wilhelm Canaris who was chief of German military intelligence during the period 1935-1944.

One wonders if the current haphazard archiving of government documents, especially from the intelligence arena, will make efforts like Bisher's not only more difficult, but impossible, for future scholars. The continuation of centralized electronic storage makes archival storage less certain than for the more palpable records from before the 1990s. Even a Wayback machine for IC agency sites would overlook unique target information and analysts' sensemaking efforts carried out through evanescent dialogue within collaborative electronic tools. These trends mean that much of the material required for inferring intelligence calculations will be denied future generations. An isolated, contrary example of how fugitive material can be captured to illuminate intelligence organizational history is Kevin Wirth, *The Coast Guard Intelligence Program Enters the Intelligence Community* (National Defense Intelligence College, 2006). Wirth captured deliberations among senior officials who were deciding whether to join the Intelligence Community after he gained permission to read and correlate various inter-office email chains. Across Latin America, as Bisher discovered, collections of government records associated with intelligence either do not exist or are unavailable to researchers. An alternative to government archiving in the region involves private collections of documents held by former officials. Even when participants remain alive, knowledge of their quiet collections remains restricted to trusted friends.

Bisher's admirable work raises additional questions that he or other scholars might consider addressing, using the material presented here and in future works like it. Among those questions: What repeating, observable, and explainable patterns of behavior emerge among intelligence services and intelligence officials in a wartime and post-war environment? What operational or analytic advantages come with intelligence personnel who have spent much of their life in civilian occupations, in comparison with those whose entire working life has been in intelligence?

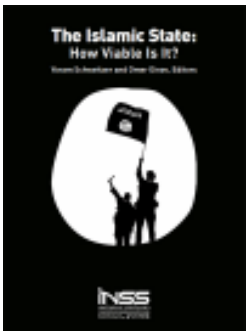
Although probably not the author's choice for this book's layout, the use of endnotes in place of footnotes makes the reader's job harder. For any reader who appreciates an author's careful documentation, bottom-of-page footnotes allow for instant indications of source quality. The salutary effect of footnotes increases when some notes feature content that goes beyond bibliographic basics, as in many of the endnotes here. On a positive note, the book remains remarkably free of typographical errors. The book also upholds high scholarly standards with a thorough index and detailed crediting of the numerous photos. Altogether, this seminal work stands out in the intelligence literature as a unique product that links information from declassified sources with the wider but still incomplete historical record of a world-altering conflict.

• •

THE ISLAMIC STATE: HOW VIABLE IS IT?

Edited by Yoram Schweitzer and Omer Einav.
Ramat Aviv, Israel, Institute for National Security Studies, Jafee Center for Strategic Studies, Tel Aviv University. 2016.
306 pages.

Reviewed by CDR (USN) Youssef Aboul-Enein, a Senior Counterterrorism Advisor for the Department of Defense and author of several books, most notably *Militant Islamist Ideology: Understanding the Global Threat* (Naval Institute Press, 2013). He is a former faculty member at the National Intelligence University, from which he earned an MSSI degree, and is currently Adjunct Military Professor and Islamic Studies Chair at the Dwight D. Eisenhower School for National Security and Resource Strategy, National Defense University. He previously published a review essay in *AIJ*, Vol. 30, No. 1, 2012, titled "Realism without Hysteria: Three Books that Aid in Critical Terrorism Analysis."



Israeli academics Yoram Schweitzer and Omer Einav have brought together a diverse set of scholars to contribute essays on the various facets of the Islamic State, or ISIS. The work is sure to generate debate and discussion on the nature of ISIS, and provides in some sections proposals to undermine the organization that has been a threat to Muslims and non-Muslims alike. This review will highlight some of the essays featured; readers need to appreciate that the cut-off period for the work is around the winter of 2015. I say that as it does not feature such progress as the defeat of ISIS in eastern Mosul, and recent operations threatening the group in Ar-Raqqa in Syria as well as the neutralizing of key ISIS leaders like Abu Muhammad al-Adnani.

Dr. Ofer Winter opens with his piece, "The Islamic Caliphate: Controversial Consensus," which is a rich discussion on the arguments between the Islamic State and the myriad of Muslim enemies it has acquired. Winter correctly assesses that when the ISIS caliphate was declared this denied the legitimacy of any other Islamic institutions, and that the announcement was aimed at the al-Qaida-associated group Nusrah Front, religious authorities which ISIS deems heretical, and Islamist political groups like the Muslim Brotherhood. Of note, ISIS refers to the Muslim Brotherhood as the *Murtadd* or apostate Brotherhood. One of Winter's more creative assessments is his organization of Salafi Jihadi-based critiques on the legitimacy of ISIS and its caliphate. This includes the declaring of a state without *ijma* (consensus), without *shura* (consultation), and that the circumstances were not ripe for a caliphate. Al-Qaida, according to the essay, demanded a retraction. What was not discussed by Winter is that this retraction by al-Qaida senior leadership goes back to 2007 when the then-leader of al-Qaida in Iraq, Abu Ayyub al-Masri, declared an Islamic State of Iraq, which collapsed a year later through the efforts of coalition forces and angry Sunni tribes hostile to the group's implementation of Islamic law in their image that was humiliating and resulted in the death of too many Sunnis. Other critiques highlighted by Winter include that the religious education of the caliph Abu Bakr al-Baghdadi is inadequate as he has not published a single religious text, and Salafi-Jihadis hostile to ISIS argue the group is undermining the Salafi-Jihadi project. These schisms among Salafi-Jihadis as a result of ISIS, and especially the animosity between ISIS and Al-Qaida, are crucial to understanding a key weakness of both groups.

Meir Litvak delves into radicalism and Islamic terror, and opens by attempting to place ISIS in the context of what he describes as Islamic fundamentalism. I disagree with this approach and feel that it is not useful analytically to conflate fundamentalists with militants. Instead, we should look at Salafis or Sunni Muslim fundamentalists as benign proselytizers, political activists, or violent jihadis in an effort to disaggregate ISIS, and contribute to the already hostile ecosystem ISIS has created through its targeting of Salafis who do not share its methodology and who question the very creation of the ISIS caliphate. Litvak does an excellent job providing a synopsis of the theories of Sayyid Qutb (died 1966), the most important theorist of modern militant Islamist ideology and discussing how the abject defeat of the Arabs in the 1967 Six Day War discredited pan-Arabism and invigorated Islamist movements. It was gratifying to see his reference to Abdullah Azzam, considered the spiritual founder of al-Qaida, and in particular his theory of the need to build a firm foundation or *al-Qaida al-Sulba*. He does, however, misspell the Islamic concept of *maslahah* (public good) on p. 38.

Yoram Schweitzer, who co-edited this book, contributes an exquisite essay on the internal conflict within the Global Jihadi camp, which takes readers into the polarization of violent Islamist groups brought about through ISIS's declaration of its caliphate. It is a struggle between and among these adversaries to adhere to the old leadership or pledge loyalty to the new caliph. Switching sides from al-Qaida to ISIS are such groups as Ansar Beit al-Maqdis (ABM) in the Sinai and Boko Haram in Nigeria. The ISIS dispute with al-Qaida is not about vision but strategy, Schweitzer reminds his readers.

David Simon-Tov and Yatom Hacohen immediately drew my attention as they focus on ISIS as an intelligence challenge. They correctly advocate looking at ISIS as part of an ecosystem, a term used by GEN (USA, Ret) Stanley McChrystal in his own fight with al-Qaida. The authors also propose that intelligence must internalize historical meaning, I cannot agree more, as ISIS in the mold of other Salafi-Jihadi groups spins narratives based on fragments of religion and history, weaving them into a modernist narrative that constantly changes. Simon-Tov and Hacohen discuss the term "dynamic disappearance," in which ISIS gains and relinquishes territory as circumstances permit. I am not sure I agree with this assessment, particularly in light of ISIS tenaciously fighting Iraqi forces currently for western Mosul. What I do agree with is their advocacy for the absolute need for cooperation among foreign intelligence organizations to build collective knowledge to defeat ISIS. [Editor's Note: It must be emphasized that both this book and the review of it were written prior to the huge battlefield setbacks suffered by ISIS in Iraq and Syria in late 2017.]

Gabi Siboni analyzes the military power of the Islamic State, and does an excellent job weaving together Abu Bakr al-Naji's book, *Management of Savagery*, with ISIS tactical, operational, and strategic approaches. The piece also appreciates the use of social media in command, control, and communications within the battlespace. The book continues to take a multidisciplinary approach to the study of ISIS, with essays focusing on the economics of the group and the approach of Russia versus the United States in combating ISIS. One of the more illuminating sentences came from Zvi Magen and his colleagues in their essay on Russia and the Islamic State challenge. They write that Moscow's policy is not to declare war on Salafism but Salafi-Jihadism. If accurate, this shows a highly nuanced and sophisticated isolation of the threat. The editors also provide a powerful argument at the conclusion that Salafi-Jihadi ideology strives to destroy all other ideologies, including that of both Sunni and Shia Muslim beliefs. The vilification of rivals has become a central policy of ISIS. This among other analytic observations helps readers train their mind to look analytically for weaknesses within ISIS, but also warns them not to think of al-Qaida as moderate or of Hezbollah as

redeemed. Those involved in countering terrorism in the post-Arab Spring ecosystem will find this book worth reading, and perhaps the best part is that it is sure to stimulate debate.

• •

INTO THE BLACK: THE EXTRAORDINARY UNTOLD STORY OF THE FIRST FLIGHT OF THE SPACE SHUTTLE COLUMBIA AND THE MEN WHO FLEW HER (with foreword by Astronaut Richard Truly)

Rowland White.
New York, Simon and Schuster. 2016.
480 pages.

Reviewed by MAJ (USA) Danielle Redmon, a Space Operations Officer (FA40) studying at the U.S. Army Command and General Staff College, Ft Leavenworth, KS. She enlisted in 1994 as an interrogator, was commissioned an MI officer in 2006, and is a graduate of the Army Space Operations Officer Qualification Course. She holds a BS degree in Psychology from Boston University and will receive an MEd in Continuing Adult Education from Kansas State University upon graduation in 2018. Dani is an avid aviation and space enthusiast; her hobbies include voraciously reading all things space-related, traveling, and acting as chief navigator for her pilot husband when flying the family's Cessna 172.

The public most remembers the space shuttle *Columbia* for its last flight. On that day, onlookers watched in horror as the space shuttle orbiter disintegrated upon reentry into the earth's atmosphere. Watching this disaster unfold on television, and the knowledge of the immediate deaths of seven astronauts, is not easily forgotten. *Into the Black* recounts the history of early manned space flight and the development of the Space Transportation System (STS), from its inception to its codification as a program of record. Rowland White's book does not dwell on the circumstances of the February 2003 shuttle disaster, however. Instead, it focuses on the people and events that brought *Columbia* into being and shaped the future of routine space travel.

The prologue opens with a poignant vignette from Dottie Lee, an aerothermodynamics engineer assigned to the shuttle program from the beginning. Anticipation builds as the reader is transported to the cockpit of *Columbia's* first launch in 1981, followed by the post-launch discovery of the shuttle's missing heat tiles as it races into orbit. Literary tension further intensifies the solemnity of the situation. Unless there is a fix, the life of the crew hangs in the balance. Will the astronauts be able to make it home?

The building suspense of the prologue quickly unfurls into a catalogue of biographical summaries pertinent to the future pilots of *Columbia*: John Young, Robert (Bob) Crippen, William (Bill) Engle, and Richard (Dick) Truly. Congruently, White portrays the astronaut pilots' early career progression against the backdrop of landmark events associated with the race to space. White's painstaking details surrounding Sputnik, the Apollo program, the Manned Orbiting Laboratory (MOL), and Skylab are familiar territory to most burgeoning aviation and space enthusiasts. In fact, it is not until readers reach the middle of the book that they are officially introduced to *Columbia*. The astronauts' narratives, world events, and the discourse of the ever-changing political climate are expertly interwoven and illustrate the 40-year space evolution that resulted in the construction of the STS.

Additionally, there are some surprising non sequitur passages interspersed throughout the book that add value and depth to the *Columbia* story. It is not until later that the reader realizes the interconnectedness of these seemingly disparate events. For instance, White segues into lengthy and detailed descriptions of the National Reconnaissance Office's (NRO) founding, its roles and responsibilities as pertaining to the Department of Defense (DoD) and the National Aeronautics and Space Administration (NASA), and the intelligence collection, retrieval, and dissemination of CORONA satellite imagery. It turns out that the NRO is an integral part of STS operations. In fact, it is due to CORONA's exceptional satellite imagery that the missing tiles on *Columbia's* first launch were identified, buying back precious time for the NASA team to engineer a solution for this emergency. Prior to CORONA, whenever something went wrong aboard a spacecraft during a mission, damage reports were confirmed by the limited abilities of an astronaut's direct observations, radio transmissions, and the thorough application of checklist procedures between mission control and the shuttle crew. At best, it could take a full day to diagnose an issue; however, with the benefit of CORONA's "eyes in the sky," the results of the imagery were accelerated to mere hours and eliminated the cloud of uncertainty.

This book is an absolute must read for anyone interested in the fields of aviation or space operations. White's vivid descriptions of shuttle operations, ground procedures, and historical context, coupled with his impressive arsenal of sources and supporting evidence, are a marvel to read and add instant credibility. Moreover, his careful historical research, detailed interviews, and unambiguous writing style and presentation are outstanding. By the time you finish the book, you almost feel like you could pilot an orbiter yourself! What is more, much of the material White used has only recently been declassified and is as illuminating to read as the shuttle narrative itself. For instance, this is the first time

in which I have read a thorough, understandable, clear, and concise description of the canister retrieval process of CORONA's imagery. The sheer magnitude of the skill and competence necessary to develop, analyze, and disseminate one satellite image is staggering—especially in an era before electronic mail and digitalized systems.

Into the Black sometimes reads like a checklist or a technical manual. The application of intimate, human emotions overlaid onto the storyline would have made the book faster-paced and more relatable to a wider audience. The dry, understated, sarcastic wisecracking so common in the aviator lexicon during an apocalyptic crisis is the only insight the reader gets regarding the emotional states of the personalities who make up the story. The irony is that the personification of *Columbia* by all who flew her consigns her memory to that of a long, lost friend. Crippen's beautiful and touching memorial speech at book's end enlightens the reader on the full scope of *Columbia's* contributions to space exploration and her unfading legacy.

[Reviewer's Note: I would like to give special thanks to David Matthews for his careful editing of this review.]

• •

THE PRESIDENT'S BOOK OF SECRETS: THE UNTOLD STORY OF INTELLIGENCE BRIEFINGS TO AMERICA'S PRESIDENTS FROM KENNEDY TO OBAMA (with foreword by President George H.W. Bush)

David Priess.
New York, Public Affairs. 2016.
384 pages.

Reviewed by Dr. Michael Douglas Smith, a retired CIA officer who wrote for the President's Daily Brief (PDB), managed the staff that produced it, served as a short-term briefer twice, helped reorganize the CIA PDB staff in the mid-1990s, and taught the PDB process to new IC officers for the Office of the Director of National Intelligence. He is currently a contractor supporting ODNI's National Counterterrorism Center.

The *President's Daily Brief*, usually referred to as the PDB, is surely the most famous of all "secret" publications. A dedicated staff within the Office of the Director of National Intelligence (ODNI) prepares the book's contents daily, but it is only delivered to the President and designated recipients six days a week unless the President requests a Sunday edition. The PDB staff contains briefers, editors, and a number of support positions. A senior officer oversees the staff.

Producing the PDB is a 24/7 process that may draw content from any information collected from Intelligence Community (IC) and non-IC sources. Analysts will develop assessments from this content during their normal working shifts or when alerted to information that needs to be evaluated immediately by their organization's operations center (or watch office). If an analyst believes the information should be dealt with, the analyst contacts the PDB staff and suggests an assessment be included in the next day's book. If the PDB staff agrees, the piece is submitted, the editorial process begins, and it will join the planned content, sometimes displacing a story already in line for publication. Occasionally the PDB staff will commission pieces directly based on its knowledge of senior policymakers' needs.

Most of the PDB's stories are written and edited during the day and fine-tuned in the evening as additional information is received and the briefing is put together. Special PDB support officers review incoming information that may affect the approved stories or interest the PDB recipients. These officers base their efforts on insights provided by the team of dedicated briefers who deliver the book to recipients each day. Each briefer receives a bundle of information when he/she arrives at work, usually around 2 or 3 a.m., and reviews it while preparing his/her own PDB package(s) for the recipient(s).

This early morning preparation is intense and guided by the choices that the President's briefer makes for inclusion in his briefing package. It is at this time that some tweaking to the PDB content may occur—either because the President's briefer decides that a story should not be used or new information makes one obsolete as offered. Occasionally a breaking story shakes up the planned flow of the briefing. Additional material is chosen by each briefer to customize the package for the individual interests of a policymaker. At some point during this time frame, analysts whose stories are scheduled to run will come in to answer questions. This gives the briefer an opportunity to clear up uncertainties or foreshadow a question by a policymaker. Most briefers have concluded their research, developed a course of presentation, and sorted projected handouts by the time they leave around 7-8 a.m. In the car, the briefer makes last-minute adjustments to the book and the delivery. After a briefer finishes the briefing, he/she makes the trip home to meet collectively with senior IC officers and the other briefers to compare notes and develop a tentative plan for the next day's book and supplementary items.

Until October 2014 the PDB was a paper publication and additional urgent material was either stapled in or provided as loose copy. However, technology developed sufficiently for a tablet version to be offered to the President and any other recipient who wanted one. This is now the norm, although a briefer may print a copy if a principal asks for one.

A morning meeting brings the briefers, analysts, and senior IC officers together to receive reaction to that day's PDB and learn what new material will be needed in the future. A notional PDB is scoped out and the system begins to fill the desired content. After the meeting, briefers will head to their offices to pass on individual comments to analysts and levy tasking based on the policymaker's comments and requests.

This is the process backdrop to David Priess' book that now constitutes the most up-to-date treatment of the PDB and the history of its reception in the Oval Office. It largely supersedes this author's history of the PDB published in the *Encyclopedia of U.S. Intelligence* (2014), though the emphasis is different. Priess explains his focus thusly: "The most fascinating issues about the PDB…revolve around the personalities of its producers and its readers, the process of its creation and delivery, and place it holds in the daily work of national security at the highest level" (p. xiii). This approach led him to interview all the living Presidents and many of the most important readers and overseers of the book to craft a coherent history of CIA's and later the Intelligence Community's entree to the counsels of the President and his most senior advisors.

.

It also moves John Helgerson's seminal study, *Getting to Know the President: Intelligence Briefings of Presidential Candidates, 1952-2004* (2nd edition, May 2012), into a support role for the study of daily intelligence inside the Oval Office. Future historians will start with these two books and, now that thousands of PDBs have been declassified and are available online, marry that background to an evaluation of the book's content.

Never static, the PDB has changed with each administration—always in the way it covers the world situation when the President's preferences are conveyed to the PDB staff, often in format and writing style. Nixon preferred his stories to start with a section containing facts and a concluding section with analysis, and was comfortable with legal-size paper. Clinton liked to write in the margin (on the left as he is left-handed). George H.W. Bush liked graphics on the back of the preceding page rather than inside the text. Obama wanted to read the book alone and then have a discussion with his national security team and the briefer (p. 121 et. seq.). With the election of the second President Bush, the official title changed to the *President's Daily Briefing*, to reflect that the rapidly changing intelligence stories meant that most bound PDBs were out of date before they were published and that it was just easier to make a coherent presentation using the flexibility of unbound stories in a three-ring binder. The binder has now become supplementary to the tablet for most readers. Recently, advisors to President Trump have told the PDB staff that the new President is a visual and auditory learner and has asked for more visual content and less text, according to a *Washington Post* story (April 2017). In the future, articles for the PDB will be structured to address these preferences. These changes and many others are embodied in the IC argument that the PDB belongs to the President and as such will be altered to reflect each President's personal preferences. The IC also uses this argument to deny access to the briefing—a position upheld by the courts.

One of the most important changes from administration to administration is the number of individuals the President designates as recipients. President John Kennedy, whose President's Intelligence Checklist was the PDB's immediate predecessor, initially restricted it to his brother Robert Kennedy, the Attorney General, and national security advisor McGeorge Bundy, and only belatedly allowed his Secretaries of State and Defense to receive the book. He never offered it to Vice President Lyndon Johnson. After succeeding Kennedy, Johnson kept the number of recipients small and it remained that way through the George H.W. Bush administration. After William Clinton entered office the number ultimately reached 24 readers (p. 211). George W. Bush initially reduced the number to six but increased it to 20 after 9/11 (pp. 231, 249). The continuing threats from terrorists led President Obama to merge the National Security Council with the Homeland Security Council and raise the number to over 30 (p. 282). The Trump administration's readership numbers so far have not been publicized.

Not everyone with access to the PDB has been impressed: Carter's national security advisor Zbigniew Bzrezinski remarked to Priess, "What struck me about the PDBs…was that they were informative specifically, but not enlightening generally" (p. 122). Years later Bzrezinski expressed more favorable opinions of the book's role during the Carter Presidency (p. 121). Former Secretary of State George Shultz was a frequent critic, and his first exposure during the Nixon administration while Director of the Bureau of the Budget left him cold: "I decided I was not reading anything useful to me" (p. 69). He might have used similar words during the Reagan administration (pp. 161-162). An even less charitable view, not cited in the book, was expressed by Tom Kean, co-chair of the 9/11 Commission, after reading the terrorist-related stories from the Clinton and Bush administrations: "They were garbage" (Philip Sheldon, *The Commission*, p. 220). Michael Leiter, Deputy General Counsel and Deputy Director of the WMD Commission who examined the analytic failure to correctly assess the demise of Iraq's WMD programs, noted how "poorly the analysts did conveying 'nuance and uncertainty'" (p. 266). [Editor's Note: Leiter was later Director of the National Counterterrorism Center.] During the history of the PDB, these views have not been shared by Presidents, who have repeatedly praised its usefulness. At the very least, most designated readers pay attention to the book precisely

because the President often uses the content to task his senior advisors or frame national security discussions with them. Examples of that abound in the book, and of the obverse, when designated recipients use their ability to call up stories for the book to bring issues to the President's attention (pp. 170-171, 243, 260-261).

The quality of this book is exhibited by the limited number of errors and omissions of relevant facts. On p. 20 Huntington "Ting" Sheldon is described as a career intelligence analyst, but he never worked as an analyst at CIA. He was hired to lead the Office of Current Intelligence by the Director of Intelligence (DI), Robert Amory. Thus, Sheldon was a manager of analysts, but not one of them. On p. 33 Russell Jack Smith is described as the "successor" to Amory even though Smith did not assume this position directly after Amory. Instead, Ray Cline did. The next sentence then mistakenly has Cline as Smith's deputy when it was the other way around. On p. 92 a reader without background on the "Family Jewels" might think DCI James Schlesinger compiled this farrago of facts, rumors, and speculations, when it was Executive Director William Colby acting on the DCI's instructions. Then, on p. 205 Leon Fuerth, Vice President Gore's national security advisor, is quoted as saying that "there was never a time in the transition and the administration that I did not get the PDB." This is a slight misremembering on Fuerth's part because this reviewer was one of Gore's PDB briefers during the first transition and I did not give the book to Fuerth on the days I briefed the Vice President-elect. Moreover, Fuerth was not in the room or in the car when I presented the brief to Gore. A bit of historical context that is not in the book would show that the Economic Intelligence Brief, "a new CIA product…to supplement the PDB" (p. 277), was imitating the DI's Economic Intelligence Daily developed for the Clinton administration. Another missing link is Robert Gates' early 1990s task force on electronic dissemination of CIA's products, including the PDB, which does not appear in the discussion "of a paperless PDB…" (p. 283).

Dr. Priess has done all students of the U.S. Intelligence Community a great service and laid the foundation for future historians to continue the story of the publication once described as "the only news not fit for anyone else to read" (Walter Pincus, *The Washington Post*, 1994).

Review Essay

The Church Committee Revisited: An Insider's Account

by LTC (USAR, Ret) Christopher E. Bailey

A Season of Inquiry Revisited: The Church Committee Confronts America's Spy Agencies.
Loch K. Johnson. Lawrence, University Press of Kansas. 2015. 345 pages.

The Threat on the Horizon: An Inside Account of America's Search for Security After the Cold War.
New York, Oxford University Press. 2011. 409 pages.

[Author's Note: The latter book was previously reviewed by me in *American Intelligence Journal*, Vol. 29, No. 2, 2011.]

Loch Johnson, a distinguished national security scholar and professor at the University of Georgia, has published a new edition of his 1985 study on the 1975 probe by the U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (more commonly known as the Church Committee), reminding the public of the continuing need for intelligence oversight and accountability in light of the more recent Iraqi WMD intelligence failures, the revelation by Edward Snowden of certain electronic surveillance activities of the National Security Agency (NSA), and the U.S. Senate Torture Report. This new edition is a useful companion to Johnson's 2011 insider's account of the Aspin-Brown Commission's 1995-96 inquiry into the activities of the U.S. Intelligence Community (*The Threat on the Horizon*). Indeed, Professor Johnson is well qualified to speak about both commissions. He served on the Church Committee as a special assistant to Senator Frank Church (D-ID) during his probe and later, during the Aspin-Brown Commission, as a special assistant to the chairman, making him well placed to record eyewitness impressions and daily Commission activities. In short, Johnson is the author of two companion, insider, political science studies on intelligence commissions (one Congressional and the other Presidential-Congressional), each having made a unique contribution to U.S. intelligence history.

This 2015 edition is a first-person chronological narrative of the work of the Church Committee's 16-month probe into the activities of the U.S. Intelligence Community

(IC).[1] In his own words, Dr. Johnson sought to provide an interim account—rather than a definitive study—that laid out the events of this inquiry, contributing "to the continuing national debate on intelligence policy."[2] He explains that his "observation post for these events was as a Senate staff assistant, on leave from university teaching. The investigation was a rare chance for me, as a political scientist, to compare the textbooks on Congress with the real thing."[3] The story unfolds with a brief history of executive-legislative relations in intelligence matters, followed by a chapter on the membership of the Church Committee, then proceeding through the investigation itself from its creation on January 21, 1975, by Senate Resolution 21 through May 1976 with the passage of Senate Resolution 400 and the establishment of the Senate Select Committee on Intelligence (SSCI), and finally concluding with a chapter that considers the aftermath of that Senate investigation. In the present edition, Johnson provides a postscript that considers the work of the Church Committee in comparison to more recent intelligence probes, and offers several useful appendices on the structure of the IC.

Professor Johnson provides the reader with a wealth of information about the people and the issues involving Senator Church's committee, first with respect to the committee's investigative work and later with respect to the use of that work in pushing a new oversight bill through the Senate. Initially, Johnson examines the creation of the committee, to include how people were recruited, organized into four task forces, and set about to do the work. He describes problems with the lack of an agenda,[4] in getting access to classified documents,[5] in pursuing varying research methodologies (i.e., historical, legal, and "soft" interviews) which caused a deep division in the staff,[6] in securing the cooperation of evasive or uncooperative witnesses,[7] and in preventing the unauthorized disclosure of classified information (i.e., leaks). He does not, however, discuss in any depth the various legal tools such as subpoenas, witness immunity, or possible contempt proceedings that were available to the committee; in part, this may be a reflection of the fact that Senator Church, unlike his House counterparts on the Pike Committee,[8] preferred taking a non-confrontational approach with the executive branch.[9]

Johnson raises many important legal issues for scholars. One interesting issue, abruptly dismissed by the committee but not explored by Johnson, was whether an executive official could be compelled to testify before Congress, but be barred from having a government attorney present to assist him.[10] Could that official refuse to testify under such conditions? In other words, could compelled testimony be later used against that official in a criminal proceeding? In one instance, Johnson does cite the decision of a federal district judge regarding the CIA's obligation to identify a certain intelligence officer associated with a questionable activity, but he fails to give us the case citation. Here, there is an important difference between knowing the name of a U.S. government employee who may have been involved in illegal activity and the name of a foreign source who has assisted the U.S. government. In the former case, a Congressional oversight committee has a valid legislative purpose in learning the person's name, while in the latter case the CIA Director would have a strong interest in protecting the Agency's "sources and methods."[11] Finally, while Johnson does discuss issues involving the release of classified information by a Congressional committee or the Senate as a whole (the Rule 36 issue),[12] he does not address the problem in constitutional terms: the President likely has Article II authority as the Commander-in-Chief to classify information under his control and does so by Executive Order, a problem that is complicated by the fact Congress has never passed legislation attempting to regulate the field. Still, tensions arise because Congress has constitutional oversight obligations with respect to its "power of the purse."[13]

Professor Johnson also provides the reader with many fine examples about how the executive branch mounted a "counterattack" against the Senate committee. He describes the stiffening resistance from the White House, to include the President's promulgation of Executive Order 11905 and the creation of the Intelligence Oversight Board (IOB),[14] the assertion of executive privilege to protect certain documents,[15] President Gerald Ford's 1975 reshuffling of national security officials (the so-called "Saturday Massacre"),[16] the misattribution of blame for the December 1975 murder of the CIA station chief in Athens to the Church Committee,[17] and the domestic investigative guidelines issued by Attorney General Edward H. Levi in March 1976.[18] Here, however, the reader would have benefited from an appendix providing the now out-of-date EO, a discussion about the roles and responsibilities of the IOB, and/or a clearer discussion about how the committee could have better handled press relations.[19] On many points, I found the book's index to be either inaccurate or incomplete.

As the Church Committee wrapped up the "active phase" of its investigation and prepared its final reports, it faced multiple obstacles to effecting reform of the Senate intelligence oversight structure. First, there was declining public interest in seeing reform of the IC. Aside from early, dramatic, but not necessarily significant exposures, such as the "dart gun," the "Cave of Bugs," or the never implemented Huston Plan, many people lacked an interest in restraining what they saw as a necessary, albeit misguided, effort to protect national security. Indeed, the

aborted nature of some of the CIA's work led some to question whether Senator Church's "rogue elephant" (the CIA) wasn't actually a "rogue mouse."[20] Also, from a political perspective, many senators had conflicting priorities, some of which were much more important to his/her constituents than arcane intelligence matters.[21] Finally, Senator Church was often absent from committee work in its later months, especially as he prepared his own bid for the 1976 Democratic nomination for President. Still, Senator Church and his committee managed to shepherd Senate Resolution 400 through the Senate's own processes, with many compromises made along the way.

This edition concludes with a 7-page postscript that judges the Church Committee investigation as "the high water mark for intelligence accountability in the United States,"[22] by comparison to subsequent congressional investigations (such as the 1987 Iran-Contra inquiry and the 2014 Senate Torture Report) as well as certain failures to investigate (e.g., a pre-9/11 probe into the nature of the FBI-CIA liaison relationship or a pre-March 2003 probe into the CIA assessments regarding the Iraqi WMD program). While Johnson concluded the original edition with an extended chronology of the Church investigation, he has added only an abbreviated update to the 2015 edition that omits numerous post-1976 oversight events/activities such as the 1995 scandal involving CIA operations in Guatemala,[23] the March 2003 creation of the position of Under Secretary of Defense for Intelligence,[24] and the 2007 creation of the President's Privacy and Civil Liberties Oversight Board.[25] Moreover, this section is marred by several errors, such as the erroneous citation to the "Agent" Identities Protection Act (p. 297)[26]; the repeated misspelling of former DNI John Negroponte's name (e.g., p. 299); and the erroneous inclusion of the entire Department of Homeland Security, the Department of the Treasury, and the Drug Enforcement Administration in the Intelligence Community (p. 301).[27] I did, however, appreciate the discussion of the two-model theory on Congressional oversight ("police patrolling" and "firefighting") offered by political scientists Matthew D. McCubbins and Thomas Schwartz.[28] In fact, I teach this useful theory to my own students in national security classes at the National Intelligence University.

The postscript could have benefited—greatly—from an examination of the recommendations made by the Kean-Hamilton 9/11 Commission.[29] Initially, the Kean-Hamilton Commission noted that "[f]ew things are more difficult to change in Washington than congressional committee jurisdiction and prerogatives,"[30] a point that certainly was amply demonstrated in Johnson's examination of the Church Committee's effort to bring about Senate Resolution 400 and the creation of the SSCI.[31] However, the Kean-Hamilton Commission found widespread dissatisfaction with the existing structure of Congressional oversight; the Commission recommended, therefore, that Congress address this problem either by a joint committee modeled on the old Joint Committee on Atomic Energy or by combining the authorizing and appropriating committees in each house. The 9/11 Commission then proceeded to make several recommendations about the structure and authorities of a new committee (or committees), with some familiar points (e.g., the committee should have subpoena powers and some members should have dual appointments on certain standing committees) and some new ideas (e.g., the committees should be smaller and members should serve without term limits).

Thus, the postscript could have usefully addressed the extent to which the oversight structure created after the probe of the Church Committee—while undoubtedly a much-needed overhaul in Congressional oversight—was still a work in progress that should have been revisited by Congress before, as well as after, the 9/11 attacks. Were the recommendations of the Kean-Hamilton 9/11 Commission valid? Do the same institutional issues which complicated the passage of Senate Resolution 400 still exist after the 9/11 attacks as an obstacle to further reform? How does the current Congressional oversight structure impact national security? In a like manner, the author could have usefully examined the role of the CIA Inspector General—originally conceived by Congress as a "long arm" oversight mechanism within the Agency—in promoting accountability with its audit and investigative authorities.[32] Has the IG served as an effective "watchdog" within the agency, identifying waste, fraud, and abuse in a timely manner, and with equally timely reporting to Congress? In other words, I would have liked a postscript assessing the Congressional oversight mechanisms created by Congress after the Church Committee inquiry, to include some review of the relative effectiveness of those mechanisms during the period leading up to the 9/11 attacks. Arguably, it would be much more difficult to effect major reform of the Congressional oversight structure now, absent another major catalytic event such as the Church Committee revelations or a 9/11-like attack.

Generally, this is an excellent book which provides the researcher with invaluable information about the problems faced by Senator Church and his committee staff in their commendable effort to investigate the U.S. Intelligence Community; to assess the strengths and weaknesses in its structure, processes, and authorities; and to recommend reform. I recommend this book to policymakers, scholars, and students interested in

understanding the difficult work involved in Congressional oversight. The book offers a gold mine of first-person experiences that could provide the basis for a deeper inquiry into the complex political-legal issues involved in Congressional investigations.

[Author's Note: All statements of fact, analysis, or opinion are the author's and do not reflect the official policy or position of the National Intelligence University, the Department of Defense or any of its components, or the U.S. government.]

Notes

[1] Fourteen published volumes of the Church Committee are available at the Assassination Archive and Research Center Public Library, URL: http://aarclibrary.org/publib/contents/church/contents_ church_reports.htm (accessed January 10, 2017).

[2] Loch K. Johnson, *A Season of Inquiry Revisited: The Church Committee Confronts America's Spy Agencies* (Lawrence, KS: University Press of Kansas, 2015), xx.

[3] *Id.*

[4] Johnson, *A Season of Inquiry Revisited*, at 87-88.

[5] *Id.* at 24.

[6] *Id.* at 29-31.

[7] *Id.* at 80-81.

[8] Representative Otis Pike (D-NY) was the chairman of the counterpart House Intelligence Committee. *Id.* at 75.

[9] *Id.* at 96.

[10] *Id.* at 39.

[11] Indeed, the CIA Director, as well as the now Director of National Intelligence, has a statutory obligation to protect intelligence sources and methods. 50 U.S. Code § 403 (g).

[12] Johnson, *A Season of Inquiry Revisited*, at 130-137.

[13] U.S. CONSTITUTION, Article I, § 9, cl. 7.

[14] President Gerald Ford signed EO 11905 on February 18, 1976; President Jimmy Carter later replaced it with EO 12036 issued on January 24, 1978. EO 11905 was an attempt to reform the IC, improve oversight of foreign intelligence activities, and ban political assassination. The IOB was conceived as a 3-person committee, possibly subordinate to the President's Foreign Intelligence Advisory Board (PFIAB), with the authority to consider reports by IC Inspectors General and General Counsels concerning questions of legality and propriety. Kenneth M. Absher, et al., *Privileged and Confidential: The Secret History of the President's Intelligence Advisory Board* (Lexington: University Press of Kentucky, 2012), at 192-194. *See also* Bartholomew Sparrow, *The Strategist: Brent Scowcroft and the Call of National Security* (New York: PublicAffairs, 2015), at 127.

[15] Johnson, *A Season of Inquiry Revisited*, at 122. See generally Mark J. Rozell, *Executive Privilege: Presidential Power, Secrecy, Accountability* (LawrenceS: University Press of Kansas, 2010), at 74-84.

[16] Johnson, *A Season of Inquiry Revisited*, at 106-109.

[17] *Id.* at 162-63.

[18] *Id.* at 154-55 and 208. The original guidelines have been revised many times and remain in force in the *FBI Domestic Investigations and Operations Guide* (DIOG). FBI, "FBI Records: The Vault," https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29 (accessed January 21, 2017).

[19] Johnson, *A Season of Inquiry Revisited*, at 54.

[20] *Id.* at 272.

[21] *Id.* at 161.

[22] *Id.* at 285.

[23] *See*, for example, James Risen, "2 CIA Officers Ousted over Guatemala Scandal," *The Los Angeles Times*, September 30, 1995, URL: http://articles.latimes.com/1995-09-30/news/mn-51610_1_cia-officials (accessed January 10, 2017).

[24] This position was created by the *National Defense Authorization Act for Fiscal Year 2003* in the aftermath of the 9/11 attacks to coordinate Department of Defense intelligence activities. 10 U.S.C. § 137. The USD(I) is the principal intelligence advisor to the Secretary of Defense; he provides executive oversight of the defense intelligence enterprise, to include the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), the National Reconnaissance Office (NRO), and the NSA. The USD(I) also serves as the Director of Defense Intelligence under the Director of National Intelligence (DNI). *See*, for example, Under Secretary of Defense for Intelligence (Biography), URL: https://www.defense.gov/About-DoD/Office-of-the-Secretary-of-Defense (accessed January 11, 2017).

[25] The President's Privacy and Civil Liberties Oversight Board (PCLOB), https://www.pclob.gov/. According to its website, the "Board is an independent, bipartisan agency within the executive branch established by the IMPLEMENTING RECOMMENDATIONS OF THE 9/11 COMMISSION ACT, Pub. L. 110-53, signed into law in August 2007." This oversight board—established by Congress in the executive branch—has recently prepared several important reports regarding electronic surveillance conducted by the NSA under Sections 215 (i.e., access to business records) and 702 (i.e., the targeting of non-U.S. persons reasonably believed to be located outside the United States) of the FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978. See, for example, PCLOB, "Report on the Surveillance Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," July 2, 2014, URL: https://www.pclob.gov/ library/702-Report.pdf (accessed Jan. 19, 2017).

[26] Former CIA officer Phillip Agee wrote several post-Vietnam books that gave detailed information about the identity and location of about 2,000 U.S. intelligence officers operating abroad, causing considerable damage and irreparable injury to U.S. interests. This led the U.S. Congress to pass the INTELLIGENCE IDENTITIES PROTECTION ACT OF 1982 (50 U.S.C. §§ 421–426). In fact, this bill was popularly known at the time as the "Anti-Agee Bill." See also Scott Shane, "Philip Agee, 72, Is Dead; Exposed Other C.I.A. Officers," *The New York Times*, January 10, 2008, http://www.nytimes.com/2008/01/10/obituaries/10agee.html?r=0 (accessed September 22, 2016).

[27] By statute, only elements of each department are part of the IC. 50 U.S.C. § 401a(4)(J) and (K). The DEA's Office of National Security Intelligence, but not the DEA itself, did not become a member of the IC until 2006. Office of the Inspector General, U.S. Department of Justice, "DEA's Use of Intelligence Analysts," Audit Report 08-23, May 2008. See also 50 U.S.C. § 401a(4)(L) (authorizing the President, or the

DNI and a department/agency head jointly, to designate other elements as part of the Community).

[28] Mathew D. McCubbins and Thomas Schwartz, "Congressional Oversight Overlooked: Police Patrols versus Fire Alarms," 28 *American Journal of Political Science*, 165-179 (1984).

[29] Thomas H. Kean and Lee H. Hamilton, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, DC: U.S. Government Printing Office, undated).

[30] *Id*. at 419.

[31] *See*, for example, Johnson, *A Season of Inquiry Revisited*, at 231-257.

[32] Ryan M. Check and Afsheen John Radsan, "One Lantern in the Darkest Night: The CIA's Inspector General." 4 J. OF NAT'L. SEC. LAW & POL'Y 247 (2010). While the INSPECTOR GENERAL ACT OF 1978 created 13 Inspectors General within the executive branch, the CIA IG did not become a "statutory IG," with enhanced authorities and reporting obligations to Congress, until the passage of the 1990 INTELLIGENCE AUTHORIZATION ACT. *Id*. at 255.

LTC (USAR, Ret) Christopher E. Bailey is an Associate Professor at the National Intelligence University specializing in national security law, processes, professional ethics, and strategy. He is a 2008 graduate of NIU's Denial & Deception Advanced Studies Program and the U.S. Army War College. He has an LLM degree in National Security & U.S. Foreign Relations Law from the George Washington University School of Law, where he is currently a candidate for the SJD degree. He is licensed to practice law in California and the District of Columbia, and is a member of the National Security Law Section, American Bar Association. Chris is a frequent and valued contributor to AIJ *and most recently volunteered to serve as co-editor for Vol. 33, No. 1, which explored the theme "Intelligence Ethics and Leadership."*