Perspective
EXPERT INSIGHTS ON A TIMELY POLICY ISSUE

September 2018

CORTNEY WEINBAUM, JOHN V. PARACHINI, RICHARD S. GIRVEN, MICHAEL H. DECKER, RICHARD C. BAFFA

Perspectives and Opportunities in Intelligence for U.S. Leaders

RAND CORPORATION

Contents

Cover image: AdobeStock

For more information on this publication, visit www.rand.org/t/PE287.

Chapter 1. Introduction

In December 2017, the White House's *National Security Strategy* described a vision for the U.S. Intelligence Community (IC):

> America's ability to identify and respond to geostrategic and regional shifts and their political, economic, military, and security implications requires that the U.S. Intelligence Community (IC) gather, analyze, discern, and operationalize information. In this information-dominant era, the IC must continuously pursue strategic intelligence to anticipate geostrategic shifts, as well as shorter-term intelligence so that the United States can respond to the actions and provocations of rivals. The ability of the United States to modernize our military forces to overmatch our adversaries requires intelligence support. Intelligence is needed to understand and anticipate foreign doctrine and the intent of foreign leaders, prevent tactical and operational surprise, and ensure that U.S. capabilities are not compromised before they are fielded. In addition, virtually all modern weapon systems depend upon data derived from scientific and technical intelligence.[1]

This vision encapsulates the current state of activities already underway in the IC, while simultaneously describing an aspirational state. In this vision, no bureaucracies or red tape are acknowledged as standing in the way of intelligence officers adapting to the global environment. In this vision, one might assume that the IC is a unified entity with no organizational structures, acquisition regulations, or security clearance backlogs that impede U.S. intelligence officers from hunting information anywhere it resides and creating actionable intelligence. This vision describes an IC that anticipates geostrategic shifts, pivots quickly to short-term crises, and utilizes all possible information and scientific advancements.

The White House's *National Security Strategy,* and the U.S. Department of Defense (DoD) *National Defense Strategy* that followed months later,[2] describe an increasingly complex global security environment and the reemergence of strategic competition among nations. These two strategy documents implicate China and Russia as revisionist states seeking to undermine an already weakening post–World War II international order,[3] while acknowledging that the United States must continue to defeat terrorism and counter rogue regimes such as North Korea and Iran. The *National Defense Strategy* argues that the United States now faces adversaries with the ability to contest U.S. dominance in all domains—air, land, sea, space, and cyberspace. In addition to this more lethal battlespace, the United

We believe that the IC has an opportunity to leap forward in helping to realize the *National Security Strategy*'s vision.

States faces threats short of war, including information operations, proxy warfare, intelligence operations, cyber attacks, and subversion. Finally, technological advances, such as artificial intelligence, autonomous vehicles, and hypersonics, to name just a few, are changing the character of war and undermining U.S. military superiority. While the strategy emphasizes that the United States aims for deterrence, it also acknowledges that the United States must be prepared to fight and win in a conflict with a near-peer competitor.[4]

This strategic environment—with emerging threats to the international order, rogue regimes, terrorists, the rise of near-peer competitors, and the proliferation of cyber weapons and weapons of mass destruction—presents the IC with a wide range of challenges. Indeed, an escalating crisis or conflict with a near-peer competitor will put enormous strain on the IC; the U.S. military and intelligence apparatus will come to the fight with what they have on hand and will almost certainly face rapid degradation. It is unclear whether the IC is prepared to provide decisionmakers and warfighters with the intelligence they need and expect for decision advantage and to ensure that U.S. forces can fight and win in this environment.

Our team convened a workshop in 2017 with fellow RAND researchers who are experienced across the IC, DoD, U.S. Department of State, and congressional committees to discuss the following questions: What are the most important intelligence enterprise topics that are not being addressed today? Which emerging changes is the IC ill-prepared to address? Where are the IC's blind spots? What issues are contrary to the IC's status quo and require a new way of thinking or doing business, particularly with the rise of near-peer competitors?[5]

This Perspective provides some answers to these questions by presenting discussion of five separate topics related to intelligence. Each chapter of this document provides analysis and recommendations on a separate topic that may be read, acted on, and implemented alone. But we believe that the IC has an opportunity to leap forward in helping to realize the *National Security Strategy*'s vision—by acting in a coordinated manner on all five of the topics together.

In Chapter Two, we describe how strategic warning warrants new investments and focus, including new tradecraft for the digital age and for complex global challenges, such as hybrid warfare. The warning mission is fraught with problems, not the least of which is denial, deception, and disinformation. The rise of near-peer competitors and the prospect of a major war inject a new sense of urgency into the warning discipline; early and accurate warning will be critical in preparing to surge for a major conflict.

In Chapter Three, we describe why a federated approach to tasking, collection, processing, exploitation, and dissemination (TCPED) architectures and processes could overcome stubborn stovepipes and yield new advancements. TCPED is the backbone of the IC, and unifying TCPED has the potential to reduce friction and increase speed, a critical capability in the context of a near-peer conflict, in which the volume and speed of information will quickly outstrip current capabilities.

In Chapter Four, we describe how several high-profile incidents have led to an environment in which most counterintelligence (CI) officers have been assigned insider threat responsibilities without commensurate additional resources or the ability to adequately cover both their CI and insider threat portfolios. Moreover, digital practices and processes can make security and CI more difficult. IC leaders are challenged to stop the leaks of sensitive information that threaten sources and methods, while attracting and retaining diverse talent with critical skills from a U.S. populace that appears to value transparency from its government more than at any time in American history. Getting the security mission and CI right should increase confidence in the analytic product.

In Chapter Five, we describe the value that publicly available information could provide to all-source analysis—if only all-source analysts could leverage this information to its fullest potential. The availability of credible open-source data is challenging the IC's bias toward secrets, but this must be balanced with the unique value that intelligence provides to policymakers and warfighters. Open-source information and academic expertise are already bolstering foundational intelligence and improving warning, both critical as the IC surges to a crisis. The use of open sources as part of the all-source product should increase confidence in analytic judgments, and perhaps speed the process as well, if the IC could settle on the tradecraft that governs its use.

In Chapter Six, we explain how the IC could surge resources strategically in times of crisis to posture itself for a world that is reliably unpredictable. Surging to crises is a perennial challenge, but will be exponentially more difficult in a crisis or conflict with a near-peer competitor. Organizational concepts that allow for the surge of analytic and collection capabilities in advance of a crisis—taking cues from open sources, warning, and a universal TCPED system—might help address crisis avoidance and crisis management capabilities.

This Perspective is intended to identify topics for intelligence leaders to tackle and to provide suggested approaches for how to do so as these leaders seek to posture the IC to meet its future demands. Future missions in this emerging global environment will likely demand high operational tempo and may even take place in a highly destructive battlespace with a near-peer military power. This type of scenario led us to focus slightly more on security, defense, and military issues than other types of intelligence topics. The analysis in this Perspective was conducted by the RAND National Defense Research Institute (NDRI) as an exploratory effort, rather than a comprehensive research endeavor. While we did not conduct new research, we did apply new perspectives and analysis to existing research and analysis. Though this work was funded by DoD, it was not directed by the U.S. government and does not reflect the views or opinions of the U.S. government.

Chapter Notes

[1] White House, *National Security Strategy of the United States of America*, Washington, D.C., December 2017, p. 32.

[2] U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, Washington, D.C., 2018.

[3] For more in-depth discussion about the international order, see RAND Corporation, "Building a Sustainable International Order," webpage, 2018.

[4] U.S. Department of Defense, 2018.

[5] We sincerely thank our colleagues (in alphabetical order) Stephen Flanagan, Bradley Knopp, David Luckey, and Heather Williams for participating. Together our combined experiences include roles of National Intelligence Officer, Defense Intelligence Officer, Defense Attaché, members of the National Security Council, professional staff members of the Senate Select Committee on Intelligence and Senate Committee on Homeland Security and Governmental Affairs, and other senior positions in DoD, the military, and the IC. Their biographies and our author biographies are provided at the end of this document.

Chapter 2. Reconstituting Strategic Warning for the Digital Age

Ever since the Japanese attack on Pearl Harbor, congressional and independent expert panels have investigated real or perceived failures of the IC to warn policymakers about strategic events. Many of these reviews have come up with similar diagnoses of the problems and recommendations to remedy them, including establishing, de-establishing, and re-establishing roles and responsibilities for the warning function.

Since 2014, events have raised questions about both the IC's strategic warning effectiveness and the policy community's understanding of warning and its ability to command action in response. Examples of recent strategic events include ISIS's establishment of a caliphate stretching from Syria to Iraq and including Mosul, Russia's invasion of Crimea and entry into the Syrian conflict, North Korea's aggressive testing of missiles and nuclear detonations, and China's construction activities in the South China Sea. In all these cases, IC elements asserted that they provided warning, and some IC officials complained that policymakers failed to heed the warning. At the same time, some policymakers lamented either that the warning did not come early enough to guide action or that possible actions the United States could take were not politically or operationally feasible or effective.

There have not yet been calls for more-extensive investigations into the executive branch's failure to detect and effectively react to strategic events, other than the investigations into Russian meddling in the 2016 U.S. election. However, Russian interference in the recent election is illustrative of the type of activity that the IC needs to warn about and policymakers need to address.[1] Re-imagining the strategic warning mission for the digital era and shaking off Cold War approaches to warning is a critical IC mission need. The Director of National Intelligence, the Under Secretary of Defense for Intelligence (DNI), and the senior leaders of the all-source intelligence organizations—the Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), and Federal Bureau of Investigation (FBI)—need to raise the priority of the warning mission, develop a new analytical tradecraft appropriate for the digital age, and invest in training the IC workforce such that it can meet the demands of the 21st century.

One would think that the nation's warning capabilities would be better, given the tremendous potential of sophisticated analytics on large volumes of data. Capabilities offered by companies such as Graphika and Recorded Futures and by the Intelligence Advance Research Project Activity (IARPA) may provide useful tactical warning of near-term events that warrant near-immediate response, but longer-term strategic events like those mentioned above are often difficult to recognize, because they evolve more slowly and frequently involve elements of intentional deception. Effectively leveraging the plethora of digital data can provide rich context for decisions, reveal hidden trends that may have exponential effects, and facilitate ways to explore a myriad of possibilities that are plausible but not consistent with current trends.

To provide strategic warning in the current era, some analysts are leveraging the power of data analytics to provide the contextual understanding of events with strategic implications, but this approach is not nearly as widespread in the IC as it is in the private sector. Hiring analysts with data science skills and training the current cadre to leverage big data community-wide and to draw on insights from big data as a normal practice is an essential evolutionary step for the analytic community. Much of these data may come from open sources, so a greater appreciation for how this flood of new information sources can usefully complement clandestinely acquired information is another important evolutionary step. There are important uses of open-source intelligence (OSINT) across the IC, but cultural and information technology (IT) infrastructure changes are needed to make it natural for all analysts to make it part of their daily take. Getting analysts to evolve in this fashion requires a push from senior IC officials and a pull from senior policymakers. Without leadership action, attention to the warning mission will drift until the next commonly perceived warning failure.

Without leadership action, attention to the warning mission will drift until the next commonly perceived warning failure.

Why Is Good Warning So Difficult?

When Robert Gates returned to CIA as Director of Central Intelligence in the early 1990s, he chartered a task force to examine the IC's capabilities in providing effective strategic warning. In the memo transmitting the task force's report to the National Foreign Intelligence Board, Gates described the warning mission as follows:

> Warning is not the same as the entire universe of contemporary intelligence. The term "warning," as it applies to intelligence means to sound an alarm, to give notice, to give admonishing advice to policymakers. It connotes urgency and implies the potential need for policy action in response. It is a different intelligence function than simply informing policymakers or enhancing their understanding of an issue or development. For the purposes of this decision memorandum, warning would include identifying or forecasting events that could cause the engagement of U.S. military forces (from the scale of embassy evacuations to larger military activities) and of events that would have a sudden deleterious effect on U.S. foreign policy and security (e.g., coups, third party wars, refugee surges, and so forth).[2]

Gates's characterization of warning focuses on threats that are liable to engage U.S. military forces, demand prompt policy action, and bear significant implications for American foreign and defense policy. He calls for warning of sudden danger and unexpected events, rather than of opportunities for policymakers to advance their policy objectives or the evolution of events that may have long-term ramifications. The digital age provides more data sources that may facilitate warning. However, the volume of data and the speed at which information can influence events have increased in ways that also complicate the warning mission.

The strategic warning mission is bedeviled by two inherent challenges. The first is how the IC identifies, categorizes, understands, and monitors key developments over time. These developments include enduring ones that are not "out of the blue," but rather slowly developing situations that may turn into opportunities for constructive action or threats that need countering; it is difficult to stimulate action in response to such situations precisely because they are slow to develop and do not seem to warrant urgent action. The second challenge is how to alert policymakers to something that has rarely, if ever, been seen before. How the IC communicates insights on threats and opportunities to policymakers is a fundamental aspect of the warning process: The best intelligence analysis has no value if it is not given to a policymaker in time for action. The inherent challenge in providing insight to policymakers about future developments is making sure that warning is heeded but does not cause undue alarm.

The inherent challenge in providing insight to policymakers about future developments is making sure that warning is heeded but does not cause undue alarm.

Structural Changes Will Not Solve the Warning Challenge

While the IC's structure has been modified over time to address a range of intelligence failures, no manner of structural changes can resolve the inherently difficult analytic task of strategic warning. Two alternative structural approaches to warning have been common in the history of the U.S. IC. One approach is to institute a central entity charged with the warning mission, staffed with personnel who have been trained on how to assess the unique aspects of warning analysis. Several commission and panel studies emphasize the importance of having a centralized entity or dedicated individual accountable for overseeing and coordinating the warning mission.[3] In 1979, the National Intelligence Council (NIC) established a National Intelligence Officer (NIO) for Warning. The mission of this

The decision to warn is rarely clear-cut.

NIO was to provide a dedicated intelligence official responsible for strategic warning to national policymakers.

The counterargument to centralizing the warning function in one office or one official is that doing so tends to make the mission personality-dependent and isolated in a single office as opposed to woven into the fabric of all regional and functional IC accounts. As a consequence, the warning function risks being orphaned and overlooked. Still others argue that all analysts are warning analysts, and that the fundamental task of intelligence analysis is to provide insights about the future. In 2011, the role of the NIO for Warning was discontinued, and the responsibility for warning was described as the mission of all analysts. In turn, this has led others to argue that if everyone is a warning analyst, then no one is accountable for a warning failure.

While it is true that any analyst or IC leader whose work supports a policymaker in any fashion—directly or derivatively—has warning as part of their job, some analytic missions have more of an explicit foresighting mission than others. Reasonable cases can be made for and against both structural approaches. Organizational structure is probably less important in the current digital age. What is more important is the types of data that are collected, sorted, interpreted, and communicated at a speed that policymakers can leverage to their advantage.

The challenge is to figure out how to provide policymakers with decision advantage about the likelihood and risk consequences of important developments. Jack Davis, a much-revered former CIA analyst, wrote that

> analysts must issue a strategic warning far enough in advance of the feared event for U.S. officials to have an opportunity to take protective action, yet with the credibility to motivate them to do so. . . . Waiting for evidence the enemy is at the gate usually fails the timeliness test; prediction of potential crises without hard evidence can fail the credibility test.[4]

This is fundamentally a problem of sense-making and communicating the insight to busy policymakers—an inherently difficult challenge.

The decision to warn is rarely clear-cut. At one end of the spectrum, failure may stem from a lack of clear understanding of U.S. policy interests and requirements. On the other, these complex situations may lead to constant warnings and the "cry wolf" syndrome. Again, Jack Davis insightfully noted, "[w]hen analysts are too cautious in estimative judgments on threats, they brook blame for failure to warn. When too aggressive in issuing warnings, they brook criticism for 'crying wolf.'"[5] Given the speed of narratives about evolving facts on the ground, the warning mission needs a new or revised tradecraft and training regime. Moreover, senior IC leaders need to evangelize the warning mission's importance much more than has been the case in recent years.

Policymakers take in information in a variety of means, but on balance spend most of their time getting and giving information verbally. Historically, intelligence analysts mainly produce written products, but this has been in the process of changing over the course of the past 30 years. Since the early 1990s, the relationship between intelligence officers, particularly analysts, and policymakers has evolved from that of a producer-consumer transactional interaction to one that also resembles a consultant-client relationship involving iterative interaction. After 9/11 and throughout the early 2000s, this relationship continued to become more interactive and iterative and not merely the production of materials to be read by a few senior leaders. Analytical organizations in the IC continue to generate important written products, but policy consumers are short on time and seek a deeper understanding than can be imparted in a static written product. In a landmark essay on the process of analysis, Robert S. Sinclair pointed out the contrast between the way "intelligence analysts typically do their work (linear, cerebral, mostly written) and the way policymakers do theirs (nonlinear, transactional, mostly oral and interactive).[6]

While the IC continues to produce mostly written reports and assessments, it increasingly conveys and also briefs its findings in new ways and via new mediums, responds to policymaker inquiries, and, as a result of this more interactive process with policymakers, provides a more nuanced contextual understanding of events. Digital-era policymakers want to get information via a variety of means and want to be able to interrogate information providers much more than was the case in the past. While written intelligence products will remain a bedrock intelligence community product, there is already interest in digital written products that convey information with greater visual content and interactivity. New ways to communicate that also allow for much faster means to exchange information can greatly aid the warning mission, because the IC is frequently confronting rapidly evolving situations that have never been seen before.

Policymakers want to take positive action to shape events, so they do not just want to be alerted to threats. They want to understand when there may be opportunities to take actions that further their policy interests. This new emphasis presents a challenge for intelligence professionals, who typically focus on *threats* to national security as opposed to *opportunities* to further national interest. (There is an old saying that when intelligence analysts see flowers, they think of funerals rather than weddings.) New approaches to warning that include opportunity analysis are another element of the anticipatory intelligence mission that can meet the needs of policymakers.

Improving Warning Analytical Tradecraft

To advance the warning analytical tradecraft beyond its current state, the IC needs to take at least three initiatives. First, the IC needs to identify and employ structured analytical techniques that improve analysts' ability to inform policymakers about emerging events that are either slowly evolving or seem to have come out of the blue.[7] Second, the IC needs to continue to leverage the revelatory power possible with digital analytics and digital collaboration. And third, the IC needs to proliferate these advancements in analytical techniques and the use of new technologies across the community. While there are encouraging developments in analytical tradecraft and the use of digital technologies for analysis, many of these advancements have not become a regular and common part of the workflow

Expertise needs to be complemented by a diversity of views.

of line analysts who often work through large volumes of information to meet daily deadlines.

In the past, when the IC had a designated warning function, the warning mission was driven by analysts using indicator lists to monitor important changes. An intrinsic difficulty with traditional warning indicators is that they are keyed to specific, imaginable outcomes. To compile indicators, one needs to know in advance what event or opportunity is under consideration. It is inherently difficult to compile indicators for an unknown event. Indicator lists provide a structured basis for warning analysis, but they do not provide nuanced context for making plausible forecasts of future events that may not exhibit indicators that are currently monitored or imagined. Another limitation of indicators is that they are generally based on precedent. This can be highly useful in relatively structured, linear situations. But the assumption that history will repeat itself is not always true, especially in situations marked by complexity and fundamental discontinuity. Even the best historical analogies are partial—past cases may resemble a current or future development in some respects but not others.

Warning about previously unseen events is dependent on much more than simply having experts who know the issues associated with the topic. Experts in a field tend to see trends based on what they have seen before, and they have difficulty imagining discontinuities that surprise.[8] Sinclair outlined how cognitive science explains how people perceive events and organize the information associated with them into narrative explanation.[9] We have implicit frameworks in our minds that we use to organize and associate new information with our past experience. Expert analysis and judgment are critical to understanding an issue but do not naturally lead to exploring discontinuities.[10] Experts frequently miss events that are discontinuous from what they had previously predicted, because the experts are naturally wedded to their previous assessments, barring new information that leads them to reevaluate those assessments.

Expertise needs to be complemented by a diversity of views. Analytical methods can help curb cognitive bias, facilitate consideration of alternative futures, and encourage structured ways to collaborate with others and harness the power of aggregated judgments. For example, outlining plausible futures, assumptions about them, and indications to look for to discern what future is emerging forces analysts to forecast futures in a way that can be inspected by policymakers.[11] The tradecraft primer for structured analytical techniques is a valuable tool for analysts, but only a few of the techniques are valuable to the warning mission. Guidance on which existing structured analytic techniques (SATs) should be used for the warning mission is important, as is developing new ones.

Important progress is being made in methods for eliciting and aggregating the predictions of many via crowdsourcing techniques and prediction markets. IARPA has advanced both crowdsourcing techniques and prediction markets to augment forecasting future developments, and the organization has made noteworthy advances. Its prediction market has moved from a developmental project into use by the NIC. The crowdsourcing project has sought to identify the characteristics that make certain people good at making probabilistic assessments of future trends and then aggregate the judgments of thousands of these people to get a cumulative probabilistic forecast. IARPA is exploring a variety of ways to leverage different crowdsourcing methods to produce better forecasts of future events and several of them are proving valuable. However, one critique of the approach focuses on the importance of selecting the right issue and crafting the right question to use with various expert elicitation and aggregation techniques.[12]

These good initiatives face challenges in scaling across the IC and getting analysts to incorporate them into their daily workflows. A few pockets of successful transition from research and development to actual use is good, but getting widespread use is much more difficult. Cognitive bias continues to be a vexing problem for analysts, even with the more widespread use of SATs and collaborative approaches to achieve cognitive diversity.[13] While new analytic techniques and new sources of information will help inform an understanding of a broader set of plausible futures, this will not solve a problem as old as the IC itself—too much information for analysts to digest. Here there is a role for computer data analytics to sift and sort quickly huge volumes of data, which can help but not solve the problem. Ultimately, the analyst must undertake the uniquely human task of sense-making that is inherent in analysis of social activities.

The 9/11 and Weapons of Mass Destruction (WMD) Commissions concluded that the IC needed to improve its analytic capabilities. The WMD commission specifically recommended greater use of SATs to improve analysis.[14] The use of SATs helps analysts to counter cognitive bias, encourage alternative explanation for future possibilities, forecast events, outline the plausible implications of forecasted events, and foster an analytical culture that is more systematic and transparent. But these analytical techniques are good only if they are used—and analysts do not always use them because they take more time and effort. Moreover, not all the SATs are relevant for warning analysis. Those that are relevant, such as alternative futures analysis, will become more powerful as they harness the power of data science. Even if intelligence analysts employ SATs and leverage data science and novel collaborative tools, the challenge remains to effectively inform policymakers, who may struggle with their own cognitive bias problems. Policymakers tend to be bedeviled by time constraints, stick to a point of view in hopes that their previous policy choices will change circumstances, and deliberate when they perceive few policy options. Returning to the strategic events listed at the outset of this chapter, many IC officials have argued that there was abundant warning about them, but that policymakers failed to act on the warnings. In the policymakers' defense, as Henry Kissinger is reported to have once said, "You warned me, but you did not persuade me."[15] Put a slightly different way, "Warning conveyed does not always result in warning received." The

Warning conveyed does not always result in warning received.

The IC needs to develop a warning analytical tradecraft that draws on the potential of new data sources and new methods to extract insight from them.

business of strategic warning is difficult on both sides of the IC-policymaker equation. The speed of events in the digital age makes this conundrum even more challenging.

Boosting the Warning Mission for the Digital Age

In the DNI's strategic plan issued in 2008, the depiction of the global complexity and the nature of the warning mission are elegantly described:

> Strategic warning and predictive estimates were standard art forms in the less dynamic Cold War period. Our anticipated strategic environment models closely on chaos theory: initial conditions are key, trends are nonlinear, and challenges emerge suddenly due to unpredictable systems behavior. . . . We believe our customers will seek our inputs on what may surprise them, if we are capable of placing such inputs in a larger context and demonstrating rigor in our analytic approaches to complexity.[16]

While this message from 2008 was well articulated, implementing a new way to address the challenges described has been difficult to achieve. To effect the cultural change, the IC leadership must issue multiple messages to the IC workforce, develop new tradecraft, and train a new generation of intelligence professionals on how to meet the warning challenge.

The DNI's 2014 *National Intelligence Strategy* states that anticipatory intelligence remains one of the IC's three mission objectives that are "foundational intelligence missions the IC must accomplish." The function of anticipatory intelligence is to "detect, identify, and warn of emerging issues and discontinuities."[17] But this is the only mention of the warning mission in the entire document. Again, the words on strategic warning, although fewer than in the 2008 DNI strategic plan, are good. The problem is that this is not enough. IC leaders need to issue repeated statements about the importance of the warning mission and then follow up to push for change. In addition to IC senior leaders "foot stomping" the importance of the warning mission, the IC needs to develop a warning analytical tradecraft that draws on the potential of new data sources and new methods to extract insight from them.[18] Across the IC, there are encouraging signs that the importance of data science to the analytical mission is recognized, as the community has established positions for chief data officers, hired a cadre of data scientists, and, in the case of CIA, stood up the Directorate for Digital Innovation. Charging these new organizational elements to make warning a priority is an easy measure for senior IC leaders to mandate.

The types of problems that capture policymaker attention have evolved with the changing international security environment, and the IC warning mission has not adequately kept pace. To its credit, the NIC has, since 1997, produced a *Global Trends* report outlining global trends 10 to 20 years in the future.[19] The most recent version of the report attempted to provide 5-year and 20-year looks into the future, the former being more relevant for current policymakers and the latter putting trends in a longer historical context.[20] As valuable as this document series is, it is extremely difficult to describe developments that clearly reveal threats and opportunities that policymakers understand as warranting policy action now. The NIC has also been experimenting with new analytic products to alert policymakers about warning events, as well as testing whether a special warning adviser is warranted for various NIO missions. While the special adviser function seems different from the NIO for Warning that was eliminated in 2011, the intent of interjecting a warning component into the NIC portfolio of intelligence products seems like a return to a previous era but with a different organizational construct. These recent attempts at innovation are good, but their ultimate value is still a work in progress.

The priority of the mission needs to be captured in an Intelligence Community Directive (ICD) that provides the basis for developing new approaches to warning analysis and that will be employed by analysts using the full range of intelligence sources used in analysis. ICD 203 describes analytical quality and standards in detail, but it never mentions how these structured approaches to analysis can aid the warning mission.[21] These analytic standards are relevant to a new strategic warning analytical tradecraft, even though they do not explicitly state how they relate to warning. Outlining how they are relevant for the warning mission is just one modest step toward infusing strategic warning in the IC's analytical tradecraft.

A new warning tradecraft drawing on past processes that emphasize indicators is necessary, but many more techniques are also needed to fashion new approaches to warning that take advantage of the potential new digital data sources that can help anticipate abrupt changes in the international system. Lists of indicators of military attack or national instability must be put into a broader context, and the use of structured analytical techniques can help analysts do this. Point predictions of strategic events are rarely possible and frequently either wrong or wrong-headed. A new warning tradecraft that combines indicators with techniques to test assumptions, identify event drivers, consider plausible alternative explanations and outcomes, and aggregate expert forecasts provides a good foundation, but it must be applied throughout the community to achieve a fundamental change in approach to warning.

The Way Forward

In a future DNI *National Intelligence Strategy*, much greater emphasis should be given to strategic warning as an intelligence mission. Beyond underscoring the importance of "anticipatory intelligence" as one of three mission objectives, the 2014 *National Intelligence Strategy* does not go to the next level of granularity to define strategic, operational, or tactical warning. It does not even provide an overarching concept for how this critical function should be carried out. Given the importance of warning, it warrants higher priority than a passing mention. Future documents and directives guiding U.S. intelligence need to directly and

Future documents and directives guiding U.S. intelligence need to directly and forcefully underscore the importance of strategic warning to most intelligence missions.

forcefully underscore the importance of strategic warning to most intelligence missions. The warning mission warrants more prominence and regular reiteration in IC leadership strategy statements, directives, management guidance, and budgetary investments. The analytical workforce needs to hear from IC leaders that the warning mission is a high priority for the IC, and this commitment needs to be realized in the form of investments in the development of new tools and techniques, training in their use, and application of these new tools and techniques to the analytical workflow. Exhortation alone will not be enough.

Advanced notice on evolving strategic situations gives policymakers a chance to evaluate options and take actions that might forestall or expedite the warned-of events. The leadership challenge that senior IC leaders currently face is how to support analysts with tools, techniques, training, and a requirement to apply them to the warning mission.

Chapter Notes

[1] Dana Priest, “Russia’s Election Meddling IS Another Intelligence Failure,” *The New Yorker*, November 13, 2017.

[2] Director of Central Intelligence, memorandum for National Foreign Intelligence Board, “Subject: Warning,” July 17, 1992.

[3] For two of the most prominent historical examples, see Director of Central Intelligence, *DCI Task Force Report: Improving Intelligence Warning*, Washington, D.C., May 29, 1992, p. 4, approved for public release April 25, 2012; and U.S. Senate, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities: Foreign and Military Intelligence Book I*, Washington, D.C.: U.S. Government Printing Office, 1976.

[4] Jack Davis, *Improving CIA Analytic Performance: Strategic Warning*, Washington, D.C.: Central Intelligence Agency, Sherman Kent Center for Intelligence Analysis, Occasional Papers, Vol. 1, No. 1, September 2002a.

[5] Davis, 2002a.

[6] Robert S. Sinclair, *Thinking and Writing: Cognitive Science and Intelligence Analysis,* Center for the Study of Intelligence, February 2010.

[7] U.S. Government, *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*, March 2009.

[8] Louis Menand, “Everybody’s An Expert: Putting Predicts to the Test,” *The New Yorker*, December 5, 2005. See also *The Economist*, “Predicting the Future: Unclouded Vision,” September 26, 2015.

[9] Sinclair, 2010.

[10] Menand, 2005.

[11] For a good example of the application of this process, see James B. Bruce and Jeffrey Martini, *Whither Al-Anbar Province: Five Scenarios Through 2011*, Santa Monica, Calif.: RAND Corporation, OP-278-MCIA, 2010.

[12] Alexander Halman, “Before and Beyond Anticipatory Intelligence: Assessing the Potential for Crowdsourcing and Intelligence Studies,” *Journal of Strategic Security*, Vol. 8, No. 5, Fall 2015.

[13] Stephen Artner, Richard S. Girven, and James B. Bruce, *Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community*, Santa Monica, Calif.: RAND Corporation, RR-1408-OSD, 2016.

[14] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States*, March 31, 2005.

[15] Henry Kissinger, as quoted in Roger Z. George and James B. Bruce, eds., *Analyzing Intelligence: Origins, Obstacles, and Innovations*, Washington, D.C.: Georgetown University Press, 2008, p. 113.

[16] Director of National Intelligence, *Vision 2015: A Globally Networked and Integrated Intelligence Enterprise*, undated.

[17] Office of the Director of National Intelligence, *The National Intelligence Strategy of the United States of America: 2014*, Washington, D.C., 2014.

[18] Bradley M. Knopp, Sina Beaghley, Aaron Frank, Rebeca Orrie, and Michael Watson, *Defining the Roles, Responsibilities, and Functions for Data Science Within the Defense Intelligence Agency*, Santa Monica, Calif.: RAND Corporation, RR-1582-DIA, 2016.

[19] Office of Director of National Intelligence, National Intelligence Council, “Global Trends,” webpage, undated.

[20] Office of Director of National Intelligence, National Intelligence Council, “Global Trends: Paradox of Progress,” 2016.

[21] Intelligence Community Directive 203, *Analytic Standards*, Washington, D.C.: Office of the Director of National Intelligence, January 2, 2015.

Chapter 3. Unifying Tasking, Collection, Processing, Exploitation, and Dissemination (TCPED) Across the U.S. Intelligence Community

The IC's topline budget amount for fiscal year (FY) 2016, including both base and supplemental budgets, totaled $70.7 billion.[1] According to some experts, the United States spends more on collection, analysis, and dissemination of intelligence than the rest of the world's intelligence organizations combined.[2] In addition to vast financial resources, the U.S. government has access to the most-sophisticated intelligence collection technologies in the world; recruits, trains, and sustains a highly educated, motivated, and talented workforce; and currently functions at a higher level of sharing, transparency, and cooperation than at any previous time in U.S. history. With that said, a limiting factor in our nation's ability to realize the full potential of its combined intelligence strengths and resources resides in the disaggregated and nonfederated tasking, collection, processing, exploitation, and dissemination (TCPED) architectures and processes used.[3] TCPED is the backbone of the IC, the framework on which all intelligence rests. It should be the aggregate of foundational systems and processes that allow leaders to seek intelligence answers to questions, allocate resources, direct analysis and production of finished intelligence, and deliver it to the appropriate end users at the appropriate time.

Prioritization of intelligence-gathering resources is only loosely associated with the National Intelligence Priorities Framework (NIPF), the Office of the Director of National Intelligence's (ODNI's) "primary mechanism to establish, disestablish, manage, and communicate national intelligence priorities."[4] Tasking for collection across the various intelligence-gathering disciplines is stovepiped within individual agencies and integrated only loosely at the national level. Processing and exploitation of collected data remain largely disaggregated, while access to "raw" collection remains limited at best. In practice, the intelligence-gathering disciplines, or "INTs," are not resourced in direct accordance with the NIPF. The NIPF serves as a rough set of guidelines to be cited when useful, but it is only loosely associated with the day-to-day budget priorities of the IC. The NIPF only marginally impacts the routine tasking of individual INTs within their silos by INT functional managers at the agencies who have that authority—human intelligence (HUMINT) and OSINT at CIA, signals intelligence (SIGINT) at the National Security Agency (NSA), geospatial intelligence (GEOINT) at the National Geospatial-Intelligence Agency (NGA), and measurement and signature intelligence (MASINT) at DIA—or by National Intelligence Managers at the national level (who can look into their own regional or functional silo but have little impact on resources or TCPED decisions across the entire enterprise). Decentralized acquisition and disconnected operations of TCPED architectures further limit processing, exploitation, and dissemination across the community. For example, sensors flown on unmanned aerial vehicles acquired and operated by the military services often do not connect to existing national-level IC architectures, preventing analysts across the IC from benefiting from all data sources. In addition, the U.S. space and ground architecture includes too few nodes where satellite data can be received, processed, and transmitted to global users in a timely manner. Meanwhile, disconnects across classified domains prevent warfighters on ships, in cockpits, and at forward operating bases from accessing the most current intelligence in real time.

Discussions of what is required to improve intelligence often focus on increasing topline resources. IC officials have historically argued that the IC budget is too small, considering that the IC cannot or struggles to answer many policymaker questions on a timely basis.[5] Other experts argue that additional dollars do not necessarily translate directly into improved intelligence. In a progress review of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Richard Best of the Congressional Research Service cautioned members of Congress to temper their expectations: “It should be remembered that intelligence analysis is an intellectual exercise; it is not possible to increase budgets by 50 percent and receive 50 percent better analysis in the next fiscal year.”[6]

One of the things required to improve intelligence is neither growth nor diminution of the IC’s budget but rather a federating and unifying of the collective and individual components within the TCPED processes of the 17 organizations of the IC,[7] as well as an expanded understanding of how TCPED applies to every INT in the IC at both the operational warfighting and strategic decisionmaking levels.[8] The IC could develop a federated approach to TCPED that manages centrally but allows for decentralized execution of all resources across the community. Such an approach would task and integrate across all collection platforms; make use of all available resources in the community; and allow streamlined access to raw, processed, and analyzed data across the entire intelligence enterprise. Below, we explore how such a process might work, and how it might address some of the problems with the current approach to TCPED.

Federated Tasking?

Joint Publication 2.0 describes how TCPED supports, or should support, the Joint Force Commander’s (JFC’s) ability to achieve operational success over an adversary:

> To prevail, the JFC’s decision and execution cycles must be consistently faster than the adversary’s and be based on better information. Being faster and better requires having unfettered access to the tasking, collection, processing, analysis, and dissemination of information derived from all available sources.[9]

Similarly, the availability of intelligence information can be crucial to strategic decisionmaking at the national and operational levels.

Unfortunately, tasking for either collection or analytic production across the intelligence enterprise is far from federated, and commanders and decisionmakers seldom have access to “all available sources.” On any given day, IC analysts from one organization may be seeking the answers to an intelligence question that was answered by collection or analysis conducted in another organization days, weeks, or even months earlier. This duplication of effort occurs because responses to ad hoc collection or production tasks are generally not cataloged or codified inside a single organization, let alone across the entire IC, and thus are not discoverable. Improving such discoverability might be accomplished by improving technological systems or operational processes, but it might also be improved by reconsidering the actual organization and individual missions of the component agencies of the IC.

While duplication of effort is itself a problem, an equally serious issue is the possibility that different answers might be provided to the same question. Although in some cases multiple analyses of the same data by separate organizations can provide alternative analyses for consideration by commanders and policymakers, decisionmakers are often frustrated by duplicative, repetitive, or contradictory intelligence analyses that make their consideration and decisionmaking more time-consuming and sometimes more difficult.[10]

The same system that results in duplicative analyses could also prevent analysis from reaching those who need it.

The same system that results in duplicative analyses could also prevent analysis from reaching those who need it. There are many reasons that access to information might be blocked: Some information remains stovepiped because of real or perceived requirements to protect sources and to ensure continued access to the information, some analytic products are created in-house for organizational leaders only and never shared beyond the organization’s walls, and other information is marginalized or relegated to long-term internal storage by the originating organization because it is perceived as not germane to other organizations’ missions.

Theoretically, in a “perfect universe,” all collection and production tasking could be federated at the national level and passed to the organization with the most efficient and effective means of collecting or producing against the task. The results of all analyses would be made available to all with a need to know, such that decisionmakers would have access to “all available sources.”

In the real world, however, where intelligence resources are limited, the volume and variety of sources of information are nearly infinite, and the ability to determine which organization’s collection methods, assets, sources, or analysts are best suited to a particular task, federation remains beyond the IC’s grasp except in limited circumstances where IC-wide surges or task forces divide the labor across multiple organizations. Some federation occurs among functional managers within the INTs, national intelligence managers within regions and functions, and IC organizations at the macro level; true federation, however, remains elusive.

Too Much Collection?

Some experts express concerns that the IC collects too much information—more than it can process, translate, or analyze, and certainly more than it can effectively utilize. Leaving aside recent arguments about excessive intelligence collection being a threat to civil liberties and privacy, collecting more information than the IC enterprise can reasonably process may be a waste of precious resources and likely adds to the burden of analysts and analytic tools that are already overtaxed trying to process and make sense of the volume of data pouring in daily.[11]

While it is true that the volume of information now available in the world exceeds the IC's capability to collect and process, it does not necessarily follow that there needs to be a reduction in collection. If you are looking for a needle in a haystack, you need to collect the entire stack of hay to find the needle. It does not matter how many people or tools you use to sift through a half-stack—if the needle is in the other half, you will never find it. In the case of the IC, analysts are looking for tens of thousands of needles every day in billions of incomplete haystacks across 17 organizations and within hundreds, potentially thousands, of internal silos of information.[12] Collecting only the information required is much more difficult than collecting it all and sifting through it after the fact. The answer to the reputed problem of "too much collection" resides not in reducing information intake, but in federating and expanding the capabilities, tools, and processes used to manage and task searches within the various "haystacks," and to exploit and disseminate the "needles" as they are found.

Collecting only the information required is much more difficult than collecting it all and sifting through it after the fact.

Stovepiped Processing and Exploitation?

Federating the stovepipes of collection and processing within the IC is not a new idea. The House Permanent Select Committee on Intelligence (HPSCI) released a staff study in April 1996 titled IC21 that spoke directly to this issue:

> The most common criticism of the current collection management process, and one in which we concur, is that it is dominated by "stovepipes," i.e., types of collection that are managed so as to be largely distinct from one another. There are several net results. First, the collection disciplines become competitors for resources driven as much by bureaucratic imperatives as by a broader national need. Second, it also becomes much more difficult to make educated IC-wide decisions about overall collection needs and the resources required to implement them.[13]

Some improvements have been made across the IC in discoverability and access to information since the promulgation of ICD 501,[14] but processing and exploitation of data remain largely stovepiped, both in storage location and accesses through "stewards" and in the capabilities and tools used to process the available information.[15] What the HPSCI observed more than two decades ago as a problem involving increasing collection management and analysis has expanded into a larger issue of stovepiped processing and exploitation.

ICD 501 requires, with some exceptions, that IC elements use "automated means" to make "discoverable" to authorized IC users all intelligence and intelligence-related information that they are authorized to "acquire, collect, hold, or obtain," or analysis that an IC element is authorized to produce.[16] This directive was promulgated in response to congressional mandates in the IRTPA to "strengthen the sharing, integration, and management of information within the Intelligence Community." However, realities within the IC suggest that discoverability is far from perfect, access and processing in real time is all but nonexistent, and automated means of discovering another agency's most closely held or originator-controlled secrets are still hampered by a system of stewards, gatekeepers, and internal processing decisions.

Consider SIGINT collected by NSA from a foreign source and in a foreign language. NSA possesses processing tools, language analysts, and analytic capabilities to locate, translate, process, and disseminate in English the information that it collects for use by analysts in the rest of the IC. But despite NSA's exquisite capabilities, only a fraction of the SIGINT it collects ever gets processed, translated, or disseminated.[17] While analysts in other agencies might have language skills that would allow them to help process and analyze the data NSA collects, most have very limited access to NSA's "raw" collection. Increasingly, advanced machine reading capabilities, search algorithms, automated translation, image detection, and the like are making human first-looks less important, but until we get to a point where the machine tells us when it has collected something we are interested in, we should use all the human capability we have at our disposal.

Similarly, while new tools and applications have allowed NGA to exploit and disseminate increased amounts of imagery for use in the IC, the volume of imagery collected each day far exceeds the capacity of NGA analysts to view, analyze, or comment on all but the most critical, time-sensitive images. All-source analysts in other IC agencies continue to have limited access to unprocessed or not-yet-released imagery collected by NGA, and even less access to images or data collected elsewhere by U.S. intelligence, surveillance, and reconnaissance (ISR) assets.

Add to the volume of data collected by national technical means the even greater volume of data available through commercial ISR platforms and openly available on the internet, or crowdsourced and uploaded as needed by billions of smartphones and other sensors around the planet—and it becomes even more obvious that analysts, let alone commanders and decisionmakers, do not have access to all available sources of information.

Absence of a Central Dissemination Clearinghouse

The 1996 HPSCI IC21 Staff Study suggested that the lines between single-source analysis (such as SIGINT and IMINT) and all-source analysis were beginning to blur and that there needed to be greater clarity in analytic roles for each of the INTs and "in relationship to one another."[18] Today, the problem still exists but might be better described as a need to refine the roles that individual analysts must play regardless of where they sit in the IC's organizational chart.

Many of the unique skills and missions that were once the purview of individual agencies have begun to blend together. NGA is responsible for providing GEOINT, "the exploitation and analysis of imagery and geospatial information that describes, assesses and visually depicts physical features and geographically referenced activities on the Earth."[19] NSA provides SIGINT, "foreign intelligence from communications and information systems," for use by decisionmakers across the U.S. government.[20] Given this division of responsibilities, is a geo-rectified digital feed that includes foreign language narration and launch video at a foreign missile installation the purview of NGA, NSA, or both? And if an analyst at CIA or DIA has the tools and language capability to process and analyze the information before NSA or NGA can get to it, should that information not be made available for exploitation and dissemination sooner rather than later?

ODNI was created to oversee the 17-organization IC and "improve information sharing, promote a strategic, unified direction, and ensure integration across the nation's IC."[21] Yet, apart from long-term assessments produced by the NIC, which falls under the purview of ODNI, the IC lacks truly centralized mechanisms for disseminating the nation's most timely and relevant assessments. Policymakers and warfighters must sift through and sort hundreds of daily assessments and determine on a continuous, individual basis which assessments to believe and which to set aside as "alternative."

The IC lacks truly centralized mechanisms for disseminating the nation's most timely and relevant assessments.

Unified TCPED: The Future of Intelligence

As new technologies emerge and improvements are made—in machine learning and machine translation, artificial intelligence, big data sorting and processing capabilities, still image and video facial recognition, change detection algorithms and other processing, and exploitation and analytic tools not yet imagined—analysts could become ever more capable of working with, exploiting, processing, and analyzing even greater volumes of information and producing and disseminating higher-quality and more-timely intelligence analyses. In an IC of the future—fully networked and connected to all available sources of information—individual analysts and analytic teams might have the flexibility to use the skills and tools at their disposal to respond to decisionmakers' most critical intelligence needs.

In the interconnected, "internet-of-things" 21st century, it might be time to question why geographic location or agency designations should matter at all. In the black-and-white analog IC of the not-too-distant past, imagery analysts squinted through lenses at backlit photographs to interpret imagery nuances that would be missed by the untrained eye of an all-source analyst. Similarly, cryptologic language analysts would hit replay repeatedly as they struggled to differentiate foreign language and nuanced meaning from background noise in voice recordings. Today, however, nearly all data are digital; exploitable; capable of being processed by myriad tools, techniques, and technologies; and easily shareable with allies and friends around the world as needed.

While individual IC agencies continue to believe that what they collect and the sources and methods they use should be protected from wide dissemination, the IC should be as agnostic about where data are processed or exploited as decisionmakers of the future are likely to be about the individual agency provenance of their intelligence feeds. Decisionmakers require relevant, timely, and accurate intelligence to make informed decisions, but they should not have to use their limited time to ponder which agency seal to revere above others when presented with alternatives.

> The IC should be as agnostic about where data are processed or exploited as decisionmakers of the future are likely to be about the individual agency provenance of their intelligence feeds.

Jack Davis, in his occasional papers on the "founder" of modern U.S. intelligence analysis, Sherman Kent, suggested that Kent would say that it is the first responsibility of IC analysts to accommodate clients by producing assessments timed to their decision cycle and focused on their learning curve.[22] Kent would also urge, Davis asserts, that analysts "allow time for Directorate, Agency, and, when appropriate, Community coordination" to permit challenges to and refinement of data and to accommodate "collective responsibility" in the IC.[23] Within these two thoughts lies the notion that it is the first responsibility of the IC, writ large, to accommodate clients by producing collective assessments, where appropriate, timed to their decision cycles.

The highest order of intelligence produced for U.S. decisionmakers has been collective in nature. National Intelligence Estimates, IC memoranda, and Sense of the Community memoranda all benefit from the collective assessment of the IC. In recent years, the President's Daily Brief (PDB) evolved for a time to include assessments produced by analysts across the IC, coordinated with multiple agencies, and edited and polished by a single, national-level PDB staff. The highest-ranking decisionmakers in the nation have traditionally been given the same collective wisdom of the IC in its entirety, even as many below the level of Department Secretary or Joint Chiefs of Staff have received daily books filled with individual agency assessments and predictions.

Imagine an IC of the future collectively working against a living and ever-evolving set of intelligence requirements; collecting and providing unclassified and classified data in a single, unified system accessible to analysts with appropriate clearance and need-to-know; and working through intelligence problems with other U.S. and possibly allied analysts, wherever they are in the world, to produce intelligence information that is easily accessible and discoverable by analysts, warfighters, and decisionmakers around the globe. For such a fantasy to ever become reality, agency seals and stovepipes would have to be permanently replaced with national interest and collective enterprise in a unified IC TCPED construct.

Concluding Thoughts

Unified TCPED would combine centralized tasking across multiple subordinate collection organizations with collection management systems that would be "aware" of other complementary collection efforts without revealing sources. A greater volume of collected data would be discoverable and available for processing and exploitation by analysts and warfighters regardless of their geographic location or agency affiliation, if such affiliations were even to remain necessary. This might require creation of an entity at ODNI enabled with "super user" access to all sources and methods and empowered to direct unification of TCPED across the IC. Creation of a TCPED ombudsman role to adjudicate inevitable conflicts might also be considered. Dissemination of analysis would be centralized to provide the collective best efforts of the IC, but would continue to include alternative analysis or dissenting views for consideration without prejudice.

Eventually, even the concept of individual INTs, which currently compete for limited resources within the IC, might give way to a larger concept of intelligence dominance through unified TCPED, focused more on finding needles than building and storing haystacks.

Chapter Notes

[1] Office of the Director of National Intelligence, "U.S. Intelligence Community Budget," 2018.

[2] Anne Daugherty Miles, *Intelligence Community Spending: Trends and Issues*, Washington, D.C.: Congressional Research Service, November 8, 2016. See also Bernd Debusmann, "U.S. Intelligence Spending—Value for Money?" Reuters, July 16, 2010.

[3] The use of the term *federated* here refers to a number of organizations being formed into a single centralized unit, within which each organization keeps some internal autonomy.

[4] Intelligence Community Directive 204, *National Intelligence Priorities Framework*, Washington, D.C.: Office of the Director of National Intelligence, January 2, 2015.

[5] The FY 2018 National Intelligence Program budget request is 7.5 percent higher than the budget requested for FY 2017.

[6] Richard A. Best, *Intelligence Reform After Five Years: The Role of the Director of National Intelligence*, Washington, D.C.: Congressional Research Service, June 22, 2010.

[7] Executive Order 12333, *United States Intelligence Activities*, Washington, D.C.: The White House, December 4, 1981, amended July 30, 2008.

[8] The major intelligence disciplines considered in this chapter are HUMINT, SIGINT, GEOINT, MASINT, and OSINT. (Other or sub-INTs include electronic intelligence [ELINT], technical intelligence [TECHINT], cyber intelligence [CYBINT], financial intelligence [FININT], and imagery intelligence [IMINT], but these are not specifically discussed in this chapter.)

[9] Joint Publication 2.0, *Joint Intelligence*, Washington, D.C.: Chairman of the Joint Chiefs of Staff, October 22, 2013.

[10] Concerns over contradictory and duplicative analyses predate the IC and the National Security Act of 1947 as amended. For CIA's account of President Harry S. Truman's frustrations on these matters in 1946, see Central Intelligence Agency, "The Beginning of Intelligence Analysis in CIA," undated.

[11] Gary Sullivan, "Too Much of a Good Thing," *Baltimore Sun*, August 27, 2014. See also Alex Young, "Too Much Information," *Harvard International Review*, August 20, 2013.

[12] Hundreds of internal databases and silos exist within the IC at the national level, thousands likely exist across the military services and other subcomponents of the Departments of Defense, State, Homeland Security, Treasury, etc.

[13] U.S. House of Representatives Permanent Select Committee on Intelligence, 104th Congress, *IC21: The Intelligence Community in the 21st Century*, June 5, 1996.

[14] Intelligence Community Directive 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*, Washington, D.C.: Office of the Director of National Intelligence, January 21, 2009.

[15] Analysts at IC agencies have more ability than ever to discover information related to their work that may be protected by another agency, and they have some capability to request release of details from the originating agency, but much information that does not need to be highly protected remains inaccessible. Raw SIGINT or unprocessed IMINT, for example, is mostly not accessible to analysts throughout the community except through specific requests.

[16] Intelligence Community Directive 501, 2009.

[17] Barton Gellman, Dafna Linzer, and Carol D. Leonnig, "Surveillance Net Yields Few Suspects," *Washington Post*, February 5, 2006.

[18] U.S. House of Representatives Permanent Select Committee on Intelligence, 1996.

[19] National Geospatial-Intelligence Agency, "About NGA," undated.

[20] National Security Agency, "Frequently Asked Questions: Signals Intelligence (SIGINT)," last modified May 3, 2016.

[21] Office of the Director of National Intelligence, "ODNI Fact Sheet," October 2011.

[22] Jack Davis, *Sherman Kent and the Profession of Intelligence Analysis*, Washington, D.C.: Central Intelligence Agency, Sherman Kent Center for Intelligence Analysis, Occasional Papers, Vol. 1, No. 5, November 2002b.

[23] Jack Davis, 2002b.

Chapter 4. Managing Security as an Enterprise

Recent years have seen several high-profile incidents involving insider threats to employees and information—notably the Fort Hood shooting in 2009, Chelsea Manning's release of classified material to WikiLeaks in 2009, the Navy Yard shooting in 2013, Edward Snowden's theft of classified material from NSA in 2013, and a data breach of security clearance records from the U.S. Office of Personnel Management (OPM) in 2015. These events led to executive orders addressing insider threats and to a renewed government-wide emphasis on security. Unfortunately, the need for personnel to address the risk of insider threats has, in many cases, meant that counterintelligence (CI) officers are designated as "insider threat officials" or are even assigned a broader security portfolio—without being given commensurate additional resources.

CI is defined by the DoD dictionary of military terms as "information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, 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."[1] While CI has an important role to play in countering insider threats and supporting security more generally, saddling CI executives with these added roles often serves simply to get the issue off leadership's plate while adversely affecting CI officers' main function of catching spies and terrorists. Worse, if CI officers are given responsibility for countering insider threats without being given the resources and authorities to do so, there can be a false perception that security is being managed as a unified, interconnected enterprise. It may be hoped that the IC should be effective enough to both do CI right and manage security as an enterprise, but this cannot happen without adequate resources or authorities to cover both portfolios.

In this chapter, we discuss how insider threats have created an environment in which many CI officers have been assigned insider threat and security or suitability clearance responsibilities in addition to their traditional responsibilities. We examine the challenges posed by these new responsibilities, and we suggest options for moving forward to address these challenges. While this is an issue for the entire executive branch, this discussion will focus on the 17 elements of the IC and the executive departments in which they reside.

Responses to recent events have led to an expansion in the security portfolio and a corresponding challenge in determining who is responsible for addressing security concerns.

An Expanding Security Portfolio

Responses to recent events have led to an expansion in the security portfolio and a corresponding challenge in determining who is responsible for addressing security concerns. The concept of the "insider threat" rose to special prominence following events such as the Fort Hood shooting, in which a U.S. Army major killed 13 people and injured more than 30 others, and the revelation of major compromises of classified information that same year by Sgt. Bradley Manning (now known as Chelsea Manning). In 2011, President Barack Obama signed Executive Order (EO) 13587,*Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, which created the National Insider Threat Task Force.[2] EO 13587 was focused on information security and especially on classified national security information.

The Washington Navy Yard shooting in 2013 brought renewed emphasis to another aspect of the security portfolio, which was also raised after the Fort Hood shooting: personnel security. On September 16, 2013, a cleared and badged contract employee at the Washington Navy Yard shot and killed 12 personnel and wounded four others.[3] An independent review of this event resulted in six major findings and recommendations, including a recommendation to

> centralize authority, accountability, and programmatic integration. Authorities and accountability for physical and personnel security matters are fractured within DOD and across many government agencies. DOD should assume responsibility for personnel security investigations from the Office of Personnel Management, and consolidate a single authority within the Department for security policies, budgets and implementation.[4]

The reasoning behind this proposed solution is understandable, although the recommendation for a single authority to handle personnel security might not be the best approach, particularly regarding the role of CI.

In October 2016, following a series of problems at OPM, including a major breach of the security investigations database, the National Background Investigations Bureau (NBIB) was established as the primary service provider of government-wide background investigations for the federal government.[5] Although NBIB remains a part of OPM, NBIB's IT infrastructure was removed from OPM and placed under DoD management because of security concerns. However, OPM retained the role of

Suitability Executive Agent (SuitEA) to implement EO 13467's mandate to reform the processes related to suitability for government employment.[6] Suitability clearances authorize government employees and contractors to enter government buildings and handle unclassified government information. The increased emphasis on suitability processes has greatly broadened the scope of today's security portfolio: For small IC elements in large executive departments, the vast majority of the departmental workforce is likely being granted access to facilities, information, and even other employees through suitability processes, not the more rigorous background investigation process required for granting access to classified material and facilities. The number of employees with suitability clearances presents an additional challenge for managers of insider threats, who are trying to balance security regarding people, information, and facilities.

In sum, the expansion of the security function, including the growing need for suitability processes, raises questions about how the security function should be managed and what the appropriate role of CI should be.

Managing the Security Function

Across the IC and, more importantly, across the executive departments that host IC elements, the security function is currently managed in a piecemeal fashion and governed by various types of committees. As an example, DoD has a directive titled Management of the Defense Security Enterprise (DSE) that designates the Under Secretary of Defense for Intelligence as the Defense Senior Security Official, with a primary function of chairing a Defense Security Enterprise Executive Committee (DSE ExComm) with 15 voting members.[7]

Each executive department understands the concept of security in a different way.

However, each executive department understands the concept of security in a different way. DoD defines *security* as "proactive measures adopted to safeguard personnel, information, operations, resources, technologies, facilities, and foreign relations against harm, loss, or hostile acts and influences."[8] The U.S. Department of Homeland Security (DHS) defines *security* as a "condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences."[9] But what constitutes the security portfolio? The portfolio includes security for people, security for information, and security for facilities, but is the IC making the appropriate distinctions among those aspects of the portfolio?

Continuing with the DoD example, the defense security framework includes "personnel, physical, industrial, information, and operations security, as well as special access program (SAP) security policy, critical program information protection policy, and security training." While that is challenging, DoD also desires the framework to

> align with and be informed by other DOD security and security-related functions (e.g., counterintelligence, information assurance, nuclear physical security, chemical and biological agent security, foreign disclosure, security cooperation, technology transfer, export control, cyber security, anti-terrorism, force protection, mission assurance, critical infrastructure, and insider threat policy).[10]

Other executive departments similarly aspire to be part of a unified security enterprise. It is especially interesting to look at the 17 elements of the IC, which are scattered across six executive departments. DNI has assigned the IC security portfolio to the National Counterintelligence Executive (NCIX), giving the executive dual responsibilities as the director of the National Counterintelligence and Security Center (NCSC). Handing responsibility for the security portfolio to IC elements in executive departments provides an example of how an already busy CI official can be given security as an additional duty. Further, as will be discussed below, the IC element has effectively been given the responsibility for security without having true departmental authority.

This practice also raises questions about the role of CI. Should CI officials willingly accept the added responsibility of managing the entire security portfolio, or should they maintain their focus on catching spies and terrorists?

Is CI taking on security and insider threat missions at the expense of higher-priority missions?

And, regarding suitability clearances, current executive branch policy is that ODNI is the government-wide lead for security clearances and OPM is the lead for suitability clearances.[11] Setting aside that this policy is emblematic of the jumbled personnel security authorities across the executive branch, it raises another question. If offered the option, should the head of an element of the IC (HEIC) pursue ownership of a larger department-wide insider threat and security portfolio and assign that role to the HEIC's senior CI official, or should the HEIC carve out a supporting role in the areas of personnel security clearance and protection of classified information and facilities?

The Challenge for CI

The expansion of the security portfolio raises questions about how CI's mission—catching spies and terrorists—is being affected by these additional responsibilities. Is CI taking on security and insider threat missions at the expense of higher-priority missions? ODNI has assigned the security portfolio to NCIX, making that executive dual-hatted as the director of both CI and security through the NCSC.[12] This seems to be taking the easy route of handing the CI community the additional complex tasks of security and insider threat so that IC leadership (i.e., HEIC) can check the box as "complete."

CI also must contend with the problem of coordinating with law enforcement—as opposed to conducting law enforcement functions with intelligence resources. Intelligence supports policy- and decisionmakers, while law enforcement supports prosecutions. Although espionage is a crime and the successful prosecution of spies requires CI agents to follow necessary rules of evidence, if a CI agent is dual-tasked with the responsibility of serving as a law enforcement agent, it is likely that the agent will develop a criminal case file and see the case through to prosecution, which also distracts from CI's main mission of catching spies and terrorists. The problem of interaction or coordination between intelligence and law enforcement rates an entire chapter in HPSCI's IC21 report, leading to the conclusion that it is the responsibility of the executive branch to determine how CI and law enforcement should work together:

> There is no need to further clarify the National Security Act of 1947, as amended, or the subsequent Executive Orders. There is a flexibility in these laws that permits a reasonable, but well-bounded, range of interpretation that will allow for improved cooperation and coordination between law enforcement and intelligence without blurring important demarcations between the missions and authorities of the two communities.[13]

There is an added burden on the busy CI officials in IC elements that conduct high-risk operations. This applies, of course, to the elements of the IC in DoD, but also to smaller IC elements, such as the Drug Enforcement Administration (DEA) and FBI, as well as operational entities within DHS. While CI and security can have a "common superior," the top official focused solely on CI in these elements must have an operational focus.

Both CI and law enforcement support security, and security is the *sine qua non* of intelligence and law enforcement operations. However, security is not necessarily something either can do effectively part-time. If one looks at "intelligence as a clandestine quest for competitive advantage,"[14] the need to separate CI from security generally and law enforcement becomes more apparent. At the same time, the IC has a commendable desire to manage security as an IC enterprise, even if the rest of the executive branch cannot.

The Way Forward

Managing security as an enterprise offers opportunities for standardization and improved effectiveness and efficiency, but security should be the responsibility of separate senior officials and not simply handed to busy CI officials as an additional duty. The IC needs a process for letting CI contribute to security as all INTs do, without distracting CI from its focus of catching spies and terrorists.

The specifics of how this might be done should be the subject of further study. There are 17 elements in the IC, and each has a different relationship with its parent executive department (except for CIA). In smaller executive departments, IC elements may need to have CI and security under one senior official. However, larger executive departments should be able to separate the functions while still establishing a management mechanism that allows security to be managed as an enterprise. DNI can set an example by removing the dual role of the NCIX. Once this "higher headquarters" split has occurred in ODNI, each of the subordinate IC elements will be able to look at its enterprise security management structures using a clean-slate approach.

Chapter Notes

[1] Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, April 2018.

[2] Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, Washington, D.C.: The White House, October 7, 2011.

[3] Admiral John M. Richardson, letter to the Secretary of the Navy regarding the Washington Naval Yard shooting, November 8, 2013.

[4] Secretary of Defense Independent Review of the Washington Navy Yard Shooting, *Security from Within: Independent Review of the Washington Navy Yard Shooting*, November 2013.

[5] U.S. Office of Personnel Management, National Background Investigations Bureau, "About Us: Safeguarding Integrity and Transparency," undated.

[6] U.S. Office of Personnel Management, "Suitability Executive Agent," undated.

[7] Department of Defense Directive No. 5200.43, *Management of the Defense Security Enterprise*, Washington, D.C.: U.S. Department of Defense, October 1, 2012, Incorporating Change 2, August 15, 2017.

[8] Department of Defense Directive No. 5200.43, 2017.

[9] George Katsos, Jerome Conrad, Frank Disimino, Ted Liddy, Anna Necheles, Charles Oliver, Christina Pham, and Basil White, eds., *United States Government Glossary of Interagency and Associated Terms*, Washington, D.C., July 2017.

[10] Department of Defense Directive No. 5200.43, 2017.

[11] Michelle D. Christensen, *Security Clearance Process: Answers to Frequently Asked Questions*, Washington, D.C.: Congressional Research Service, R43216, October 7, 2016.

[12] U.S. Code, Title 50, Section 3383, National Counterintelligence and Security Center.

[13] U.S. House of Representatives Permanent Select Committee on Intelligence, 1996.

[14] Vincent H. Bridgeman, "Defense Counterintelligence Reconceptualized," in Jennifer E. Simms and Burton Gerber, eds., *Vaults, Mirrors, and Masks*, Washington, D.C.: Georgetown University Press, 2009, pp. 125–148.

Chapter 5. Better Utilizing Publicly Available Information

Intelligence analysts have access to greater quantities of openly available data from public and commercial sources than at any time in history. This growth has produced a commensurate increase in the information available to decisionmakers and policymakers—who can also access the same publicly available information as the IC without waiting to receive a finished intelligence product.[1] This wide availability of data has changed the information paradigm to an environment where open-source information, also known as publicly available information (PAI), is widely available on most topics.

Yet this abundant PAI is not always accurate nor reliable. Policymakers will continue to rely on intelligence analysts to analyze all sources of information—classified and unclassified—to determine each source's credibility, accuracy, and relevance to specific topics. This abundance of information stresses the intelligence cycle. The speed of reporting available in the media, social media, and on the internet provides policymakers with access to open-source analysis faster than intelligence analysts can synthesize, analyze, and report on all available sources.

All-source analysts and their leaders have not yet embraced either PAI or its synthesized and analyzed result, open-source intelligence (OSINT),[2] with the same force as have policymakers. As a result, IC organizations often treat both PAI and OSINT as another stovepipe, similar to other INTs, rather than a resource for foundational use in all analytic products.

Leaders could continue the evolution of all-source analysis by answering questions such as the following: What are the procedures for using PAI—including crowd-sourced information—in foundational intelligence and targeting databases? How should all-source intelligence be peer reviewed to identify biases, weaknesses, and flaws in the analytic process? What tradecraft standards can be developed to determine the credibility and accuracy of big data analytics and data science, the methodologies often used to synthesize large data sets from unclassified sources?

For many all-source analysts, including those at CIA and DIA, these questions are straightforward for social media data. Those agencies both have groups who mine, synthesize, analyze, and rate for credibility information from social media. And yet these questions are more difficult for analysts to answer for information collected by unclassified sensors. In this chapter, we discuss how IC leaders might make broader use of PAI and OSINT in all-source analysis with revisions to existing policies, training, and evaluation mechanisms.

What Is the Intelligence Value of Publicly Available Information?

A sometimes-heard sentiment among the IC is that "if it's not classified, then it's not intelligence." This viewpoint suggests that classification is a differentiator, and that what makes the IC special is its access to classified sources and methods that are not available to organizations and individuals outside of government.[3]

However, this argument becomes less convincing as more—and more high-value—sources and methods become available on the unclassified open markets. New technologies, approaches, and media are making information-gathering and analytic capabilities accessible to the masses. Technologies to collect intelligence are more prevalent in the public domain,[4] and, as a result, nongovernmental users now have greater access to information sources and methods than at any time in the modern era. Further, unclassified and publicly available sources and methods can often produce intelligence value significantly faster than traditional all-source processes that rely on classified sources, and without classification hurdles that prevent sharing with uncleared stakeholders and foreign partners.

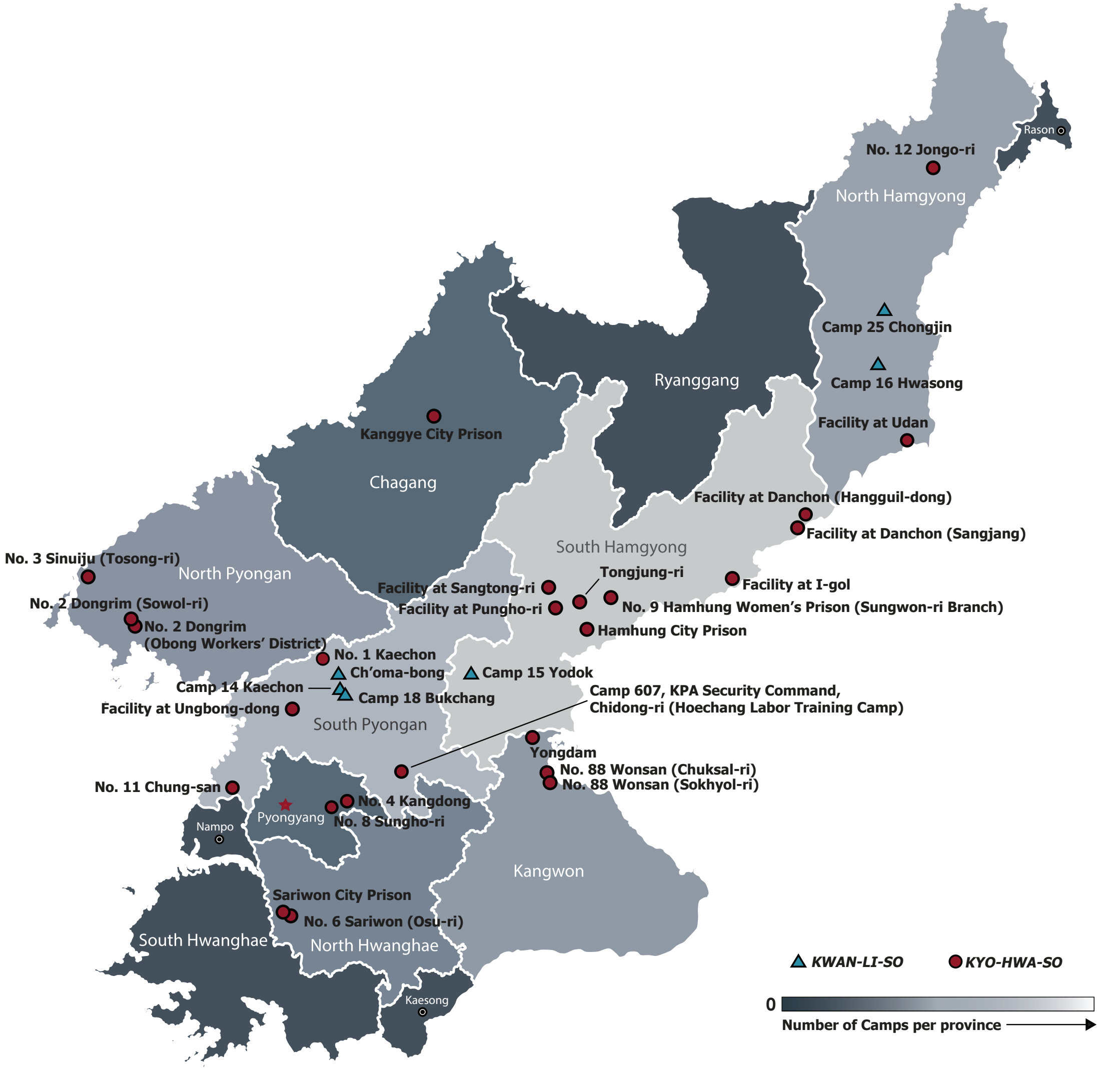
The open-source commercial imagery market is booming. Every smartphone user can view commercial imagery for free through Google Maps. For a fee, governments, corporations, nonprofit organizations, and private individuals can buy higher-resolution imagery or more-current imagery through Google. By one estimate, the size of the commercial imagery market will be $6.8 billion by 2023.[5]

As more commercial providers are launching commercial imagery satellites, NGA has changed its business model to include unclassified commercial imagery in its product lines. Unclassified imagery includes panchromatic (grayscale) imagery,[6] multispectral imagery that provides more information[7] in multiple spectral bands of varying wavelengths,[8] and even synthetic aperture radar (SAR)[9] for nighttime and all-weather images.

Unclassified information available on social media and through unclassified ubiquitous sensors located around the world also provides new value to analysts, who historically did not have access to such diverse and high-quality sources. For example, the Committee for Human Rights in North Korea is a nonprofit organization that has manually analyzed unclassified imagery, prisoner testimony, and a translation of the 2012 North Korean Criminal Code to meticulously detail the differences between North Korea's arbitrary detention system (designed to sow fear and oppress the populace) and its political prison camps (designed to separate dissidents from the population and punish them and "up to three generations of family members"). Their analyses have detailed where these camps are located, as shown in Figure 5.1, how they are operated, and how prisoners are treated.[10]

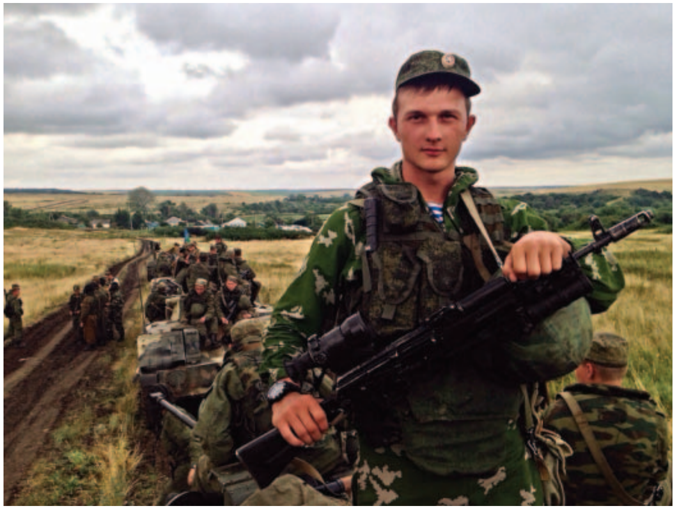
Researchers at Bellingcat, which publishes online the findings of citizen journalist investigations into war and the criminal underground, use a different approach. For example, they have merged overhead satellite imagery with open-source social media posts to track Russian troop movements.[11] Bellingcat used open-source images (such as the photo shown in Figure 5.2 that a Russian soldier posted of himself online), metadata from the images, and imagery from other unclassified sources to locate Russian troop positions and movements. In 2017, Bellingcat used a Ukrainian Twitter user's photos, as shown in Figure 5.3,

Figure 5.1. Map of Prison Camps in North Korea



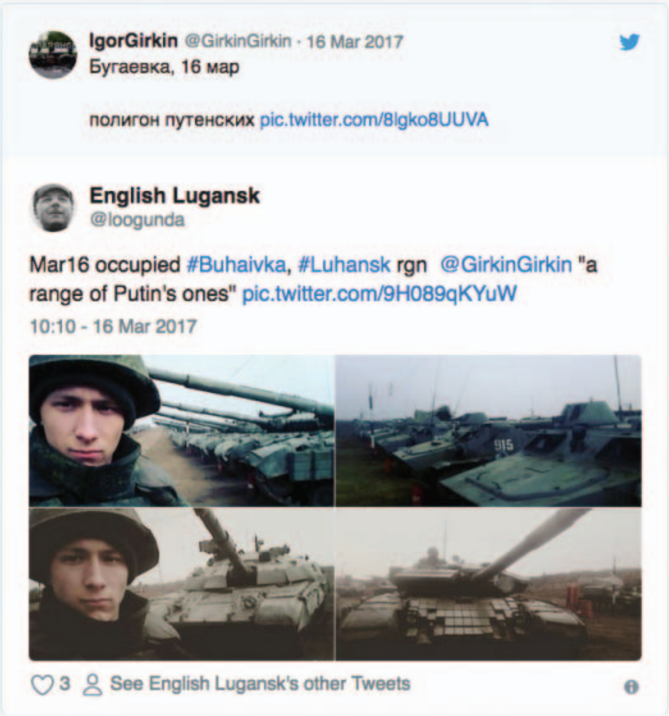
SOURCE: Hawk, 2017. Used with permission.
NOTE: kwan-li-so = political prison camps; kyo-hwa-so = labor reeducation camps.

Figure 5.2. Photo of Russian Soldier Stanislav Tarasov Posted to Instagram and Geomapped to 47°56'10.33" N 39°50'2.55" E (Pavlovka, Russia) Using Google Earth



SOURCE: Via Toler, 2015.

Figure 5.3. Tweets from @GirkinGirkin and @loogunda



IgorGirkin @GirkinGirkin · 16 Mar 2017
Бугаевка, 16 мар

полигон путенских pic.twitter.com/8lgko8UUVA

English Lugansk
@loogunda

Mar16 occupied #Buhaivka, #Luhansk rgn @GirkinGirkin "a range of Putin's ones" pic.twitter.com/9H089qKYuW
10:10 - 16 Mar 2017

♡ 3 See English Lugansk's other Tweets

SOURCE: Via Bellingcat Investigation Team, 2017.

and satellite imagery to demonstrate that Russia was violating a heavy weapon withdrawal agreement.[12] Analytic approaches that rely on social media data without merging that information with other sources would be unable to come to the analytic conclusions Bellingcat has reached.

The approaches just described can be used to understand WMD programs and foreign missile technology, some of the highest-priority threats the IC addresses. Bellingcat has used social media photos and posts, videos posted on YouTube, witness interviews, chemical analysis, and other open-source reporting streams to document chemical weapon attacks inside Syria by the Assad regime,[13] chemical weapon use by ISIS against Kurds,[14] and Russian activities related to chemical attacks.[15] Inside the IC, these sources would be considered HUMINT or MASINT if they were classified, but when publicly available, all-source analysts are left to verify the reports' credibility and accuracy, often without the time or tools to do either.

When NGA asked researchers at the University of Missouri's Center for Geospatial Intelligence to develop machine learning and artificial intelligence tools to speed up and automate functions traditionally performed by human analysts, the new approach was capable of finding missiles spread across wide geographic areas:

> Researchers . . . used a deep learning neural network to assist human analysts in visual searches for surface-to-air missile sites over a large area in southeastern China. The results showed that the computer performed an average search time of only 42 minutes for an area of approximately 90,000 square kilometers. By comparison, North Korea is about 120,000 square kilometers.[16]

The University of Missouri team reported that its results were "more than 80 times more efficient than a traditional human visual search" and "achieved the same overall statistical accuracy as human analysts—90 percent—for correctly locating the missile sites."[17]

Other nongovernmental organizations are deploying their own unclassified sensors, rather than relying solely on publicly available ones. NORSAR is a Norwegian nonprofit research organization with seismic detection stations that detect and measure the strength of seismic events, determine whether an event was man-made (such as a nuclear or conventional explosion) or naturally occurring (such as an earthquake), and calculate events' locations and magnitudes. On September 3, 2017, NORSAR detected a seismic event in North Korea and reported the following:

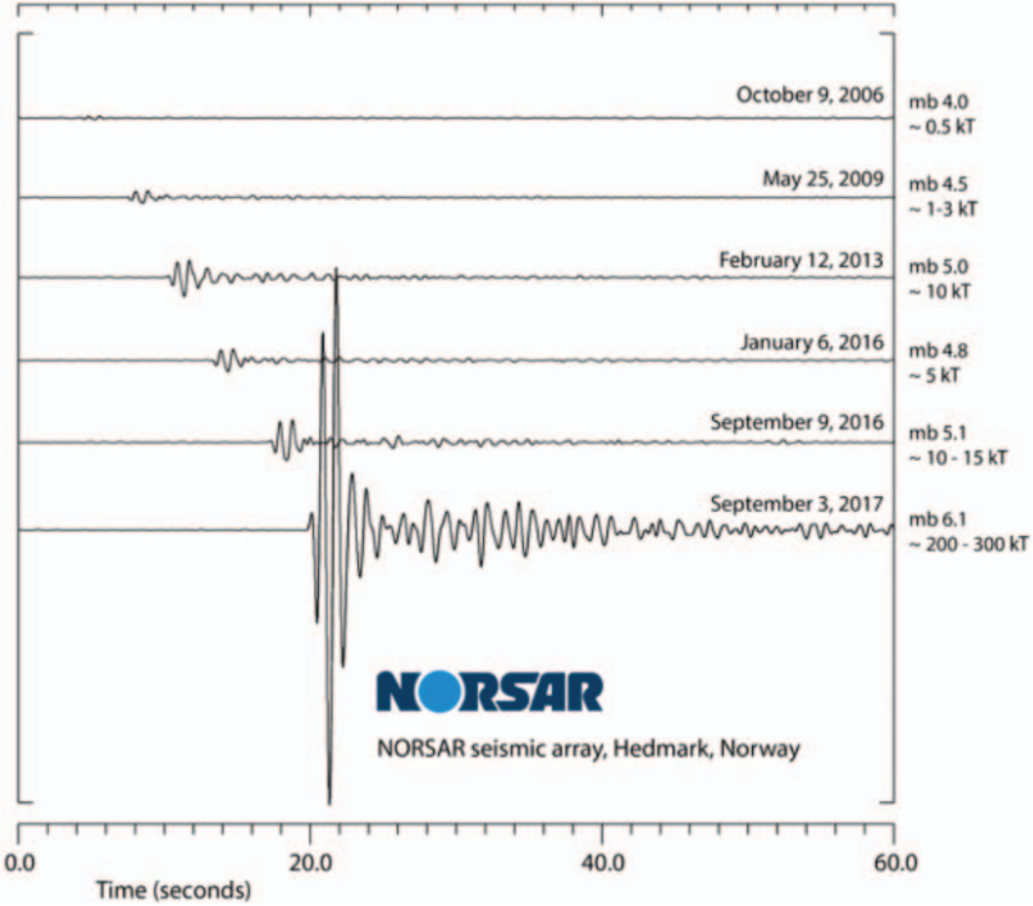
> NORSAR recorded the signals from the underground nuclear test explosion on our seismic stations some 7360 km from the test site. The signal took 11 minutes to travel the distance from North Korea to Norway, showing up at our instruments at 05.41 Norwegian time. We have worked thoroughly with the explosion signals to assess the seismic magnitude of this nuclear test and its explosive yield. Our assessment points to a magnitude 6.1 and an estimated yield of 250 kT. This is by far the largest of the tests performed by North Korea.[18]

These data, shown in Figure 5.4, led analysts to conclude that North Korean claims of a hydrogen bomb test were plausible, though they still doubted the regime's technical abilities to achieve that accomplishment.[19] Unclassified technical collection—if verified by intelligence analysts—provides policymakers the ability to bring definitive evidence to international debates over United Nations resolutions, sanctions, and coalition operations without needing to request declassification.

Nongovernmental organizations have used technical collection together with unclassified analytic approaches to analyze North Korean missile tests and trajectories. Analysts compared three North Korean missile launches in 2017 to calculate how the regime's missile program has advanced by increasing the missiles' strike range from less than 3,000 miles to almost 6,800 miles.[20] Figure 5.5 shows that these new ranges are far enough to reach Chicago and beyond.

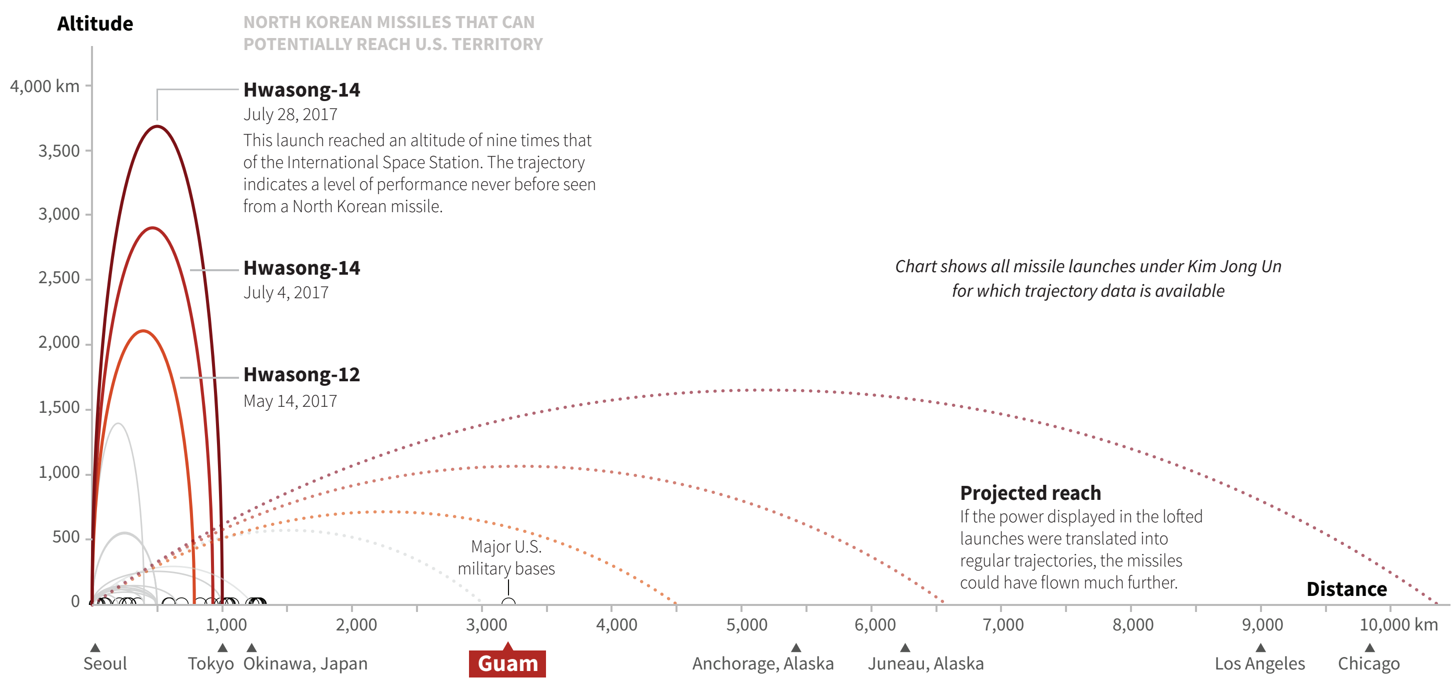
In October 2017, Martyn Williams, an expert on North Korea, and Doug Madory, an expert on internet technologies, identified a new internet connection between the Russian telecommunications company TransTeleCom (TTK) and North Korea. Previously, the only connection North Korea had to the internet was through China; when that connection was briefly severed in 2014, it left North Korea without internet access.[21]

Figure 5.4. NORSAR Seismic Readings from North Korean Missile Tests



SOURCE: NORSAR, "Summing Up the Nuclear Test in North Korea on 3 September 2017," September 22, 2017. Used with permission.

Figure 5.5. Calculated and Projected Trajectories of North Korean Missiles Based on Three Tests



SOURCE: Adapted from Reuters / S. Scarr, J. Wu, W. Cai. The CNS North Korea Missile Test Database, Nuclear Threat Initiative (NTI); David Wright, Global Security Program at Union of Concerned Scientists. Used with permission.

Williams and Madory published the network usage and transfer speeds of this connection in the Dyn Corporation's blog. Their finding led the Russian company TTK to issue a statement in which the firm neither confirmed nor denied the existence of such a connection to North Korea.[22] In the IC, this type of information would be considered SIGINT, it would likely be highly classified, and policymakers would likely have been unable to use it publicly to prove this link between Russia and North Korea.

Changing How All-Source Analysts Think About Open Source

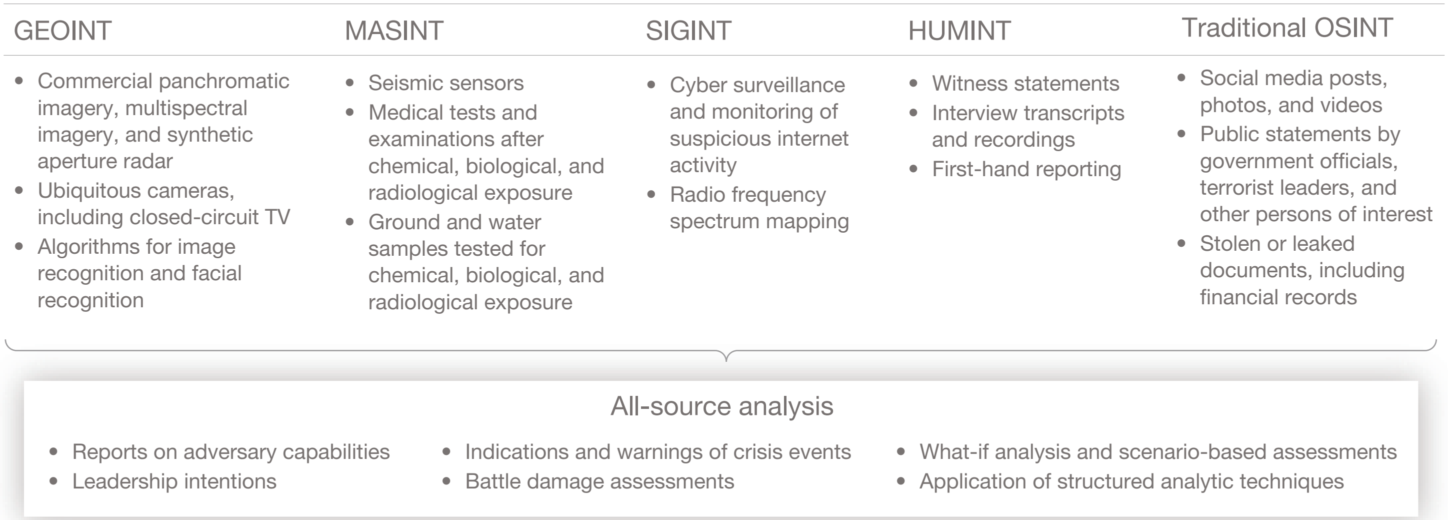
Many of these examples demonstrate the use of open sources and methods to describe activities, capabilities, and intentions within the closed so-called "hermit kingdom" of North Korea. If open source can work there—where internet connections, social media, and ground sensors are extremely limited—then the value of open source to other intelligence topics could be even greater.

We categorized open-source capabilities in terms of the intelligence disciplines and arrived at the grouping shown in Figure 5.6.

All-source analysts at nongovernmental organizations such as 38 North (which specializes on analysis of North Korea) and Bellingcat conduct each of the types of all-source activities listed in the right-most column of Figure 5.6. The value for intelligence analysts with access to classified sources, therefore, could be to add classified sources to these unclassified sources to create all-source products that are more robust than either classified or unclassified all-source products could be on their own.

However, to take advantage of the full range of information sources, the analysts within each discipline need to perceive the value of open-source data and methods *and* they need the ability to use them. Such an approach is not typical within the IC today, where all unclassified sources

Figure 5.6. Publicly Available Sources and Methods, Categorized by Relevant Intelligence Discipline



GEOINT	MASINT	SIGINT	HUMINT	Traditional OSINT
• Commercial panchromatic imagery, multispectral imagery, and synthetic aperture radar • Ubiquitous cameras, including closed-circuit TV • Algorithms for image recognition and facial recognition	• Seismic sensors • Medical tests and examinations after chemical, biological, and radiological exposure • Ground and water samples tested for chemical, biological, and radiological exposure	• Cyber surveillance and monitoring of suspicious internet activity • Radio frequency spectrum mapping	• Witness statements • Interview transcripts and recordings • First-hand reporting	• Social media posts, photos, and videos • Public statements by government officials, terrorist leaders, and other persons of interest • Stolen or leaked documents, including financial records

All-source analysis

- Reports on adversary capabilities
- Leadership intentions
- Indications and warnings of crisis events
- Battle damage assessments
- What-if analysis and scenario-based assessments
- Application of structured analytic techniques

tend to be lumped together as OSINT and are considered to be collectively the responsibility of OSINT officers and offices. Without experts in each intelligence discipline, collection phenomenology, technology, and country team looking for unclassified sources to help their work, analysts are all able to ignore troves of potentially valuable data as "not my responsibility."

The barriers that prevent analysts from embracing PAI to its full extent are not new, and neither are the solutions to overcome them. But that does not mean they are easy to overcome. The barriers include, but are not limited to:

Cognitive Biases

"Not invented here syndrome" describes the cognitive bias to exclude information and methods that originate outside a trusted organization.[23] This bias leads some intelligence officers to believe—consciously or not—that sources and methods from outside the IC cannot be as high-quality or dependable as the sources and methods analysts are familiar with and that were generated by their own colleagues.

An extension of "not invented here" is a belief that, "We can't trust it if we didn't collect it." This mentality describes the inability to trust sources collected by people who have not been vetted by agency personnel: Those "outside" collectors may have fudged or outright fabricated data, leading to a conclusion that, if all the data cannot be trusted all the time, then none of the data can be trusted any of the time.

Both of these cognitive biases serve analysts' risk-reward models. Analysts who trust sources that are later revealed to be fraudulent are punished, either through formal channels or by being embarrassed among their peers. Alternatively, analysts who ignore open sources from outside of traditional channels are rarely—if ever—punished or humiliated.

The barriers that prevent analysts from embracing PAI to its full extent are not new, and neither are the solutions to overcome them. But that does not mean they are easy to overcome.

These biases can be lessened or neutralized by giving analysts more exposure to PAI and to techniques for evaluating the credibility of unclassified sources. Analysts should be required to use PAI and those tradecraft tools on a regular basis in teams, similar to how agencies describe using SATs. A previous RAND study described the benefits of SATs and how to implement them:

> SATs provide analysts with clear, often step-by-step, guidance for conducting analysis of intelligence issues. By providing greater structure to the analytic process, they reduce subjectivity and add both rigor and transparency to analysis. A key part of reducing

subjectivity in analysis requires identifying cognitive bias and reducing it.[24]

This change would build and strengthen the analytic muscles needed to use PAI on a regular basis with confidence and analytic integrity. By addressing these solutions in teams, analysts can learn from each other's work without individually needing to take risks associated with being the only analyst citing PAI sources.

Big Data, Big Challenges

A challenge with open sources is that even if analysts want to use them, there is simply too much open-source data to analyze, the information exists in too many formats, and analysts lack the analytic tools to fully interpret it. This challenge is daunting but not insurmountable: Analysts need approaches for data processing and analysis to make sense of open sources, as well as new policies to work with data where they reside, rather than having to move all the data onto government systems.

Open-source organizations help greatly with this challenge by collecting, synthesizing, and analyzing OSINT, but these organizations usually address specific subsets of open-source data, and all-source analysts may be undertrained on how to effectively utilize these capabilities and product lines. All-source analysts need access to more data science techniques and to better understand the techniques already offered by brethren in their agencies.

Behavioral Economics in Action

Over the past 30 years, the field of behavioral economics—which lies at the intersection between economics and psychology—has studied human decisionmaking and rational choice, finding explanations for why people are likely to choose the path they believe is easiest rather than the path that will lead to the better outcome.[25] This field of study explains, for example, why so few people exercise and eat healthy foods, despite knowing the benefits.[26] Behavioral economics can also explain why analysts are less likely to switch from their classified computer system to their unclassified computer, even when they know how much useful data may be found on the internet.

Barriers that may appear to be surmountable annoyances—such as working across classified and unclassified computing domains—can become roadblocks to intelligence reform. When business communications, business processes, data, and data processing tools reside predominantly on classified computing systems, intelligence personnel are less likely to conduct significant chunks of work on unclassified systems. In addition to the inconvenience and annoyance these computing barriers create, any behavior change by analysts includes the risk of data spills (classified data being spilled onto unclassified computer systems), which carry severe repercussions. The efforts and risks involved in switching networks and moving data and analysis between IT systems become too large, while the payoffs—higher-quality intelligence—are too small to the individual.

Agencies can overcome this challenge by increasing the number and quality of applications available on unclassified computing systems and the magnitude of IT support to users. In a project for NGA, RAND found that, in order for NGA employees to conduct more work on unclassified systems, they needed a clearer understanding of what types of information can safely be used on unclassified computing systems, and they needed the data transfer capabilities and other technology tools to work with those data safely.[27]

Concluding Thoughts

As the amount of data available in the public domain continues to increase, all-source analysts risk ignoring this information at policymakers' peril. In the policy arena, intelligence needs to be discussed and debated as quickly as possible—often while events are unfolding, and often in unclassified settings with persons who lack security clearances or access to classified computing systems.[28] When classified sources provide insights that are not available in PAI, the merger of classified and unclassified sources provides the opportunity to create intelligence assessments—finished analysis—at lower classification levels for policymakers to act on.

At the time of the writing of this Perspective, intelligence agencies and congressional committees are investigating past and ongoing Russian covert influence campaigns within the United States.[29] A recent article in *The New Yorker* described the IC's lack of open-source analysis on this topic as an "intelligence failure":

> Unlike 9/11, the Russian campaign did not occur without warning on a quiet fall day. Rather, it unfolded over at least six months on Americans' social-media accounts—hardly the stuff of spy novels. Kremlin leaders had signalled their plans years in advance. The Russian playbook wasn't a secret, either. It had been well documented by European governments, researchers, and journalists after the Kremlin's information operations to destabilize Estonia, in 2007; Georgia, in 2008; Ukraine, in 2014; and Britain, in the leadup to the 2016 Brexit vote.[30]

The information that would have revealed Russia's tactics and intentions for meddling in democratic processes was in open sources. While classified sources could have revealed Russian activities, the IC's lack of classified collection on this topic does not excuse this intelligence failure; the evidence was available in PAI, if only analysts had looked.

On the topic of terrorism analysis, the House Permanent Select Committee on Intelligence, stated the following in 2015:

> The Committee believes that the U.S. Government as a whole, and in particular the Intelligence Community, must improve its efforts to understand the full scope of terrorist groups' messaging campaigns and communications methods online. These efforts should not be confined solely to intelligence analysts; operational personnel, including intelligence and defense officials, must be aware of how terrorist groups make use of open source messaging.[31]

For topic after topic, information in the public domain could provide high intelligence value—if all-source analysts seek these data out and use them in their analyses.

Open sources often provide earlier indications of events than classified sources, can be layered with classified sources to provide a more complete and nuanced understanding, and offer information that can be shared and discussed with foreign partners and uncleared U.S. partners. Robert Cardillo, director of NGA, said, "We [intelligence professionals] owe them [policymakers] time and space: time to make the decision, and space to take the action."[32] Open sources provide useful intelligence that policymakers can receive, digest, and react to faster and more easily than many classified sources. The potential value of PAI is clear; the IC's current challenge is to overcome the barriers that prevent all-source analysts from fully exploiting these troves of intelligence.

Chapter Notes

[1] Department of Defense Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, Washington, D.C.: U.S. Department of Defense, August 8, 2016, defines *publicly available information* as "Information 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, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public."

[2] The *DOD Dictionary of Military and Associated Terms* (Joint Chiefs of Staff, 2018) defines *open-source intelligence (OSINT)* as "Relevant information derived from the systematic collection, processing, and analysis of publicly available information in response to known or anticipated intelligence requirements."

[3] Brett Miller, "Evolution of Intel: How Valuable Is OSINT?" *In Public Safety*, July 24, 2015.

[4] Cortney Weinbaum, Steven Berner, and Bruce McClintock, *SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain*, Santa Monica, Calif.: RAND Corporation, PE-273-OSD, 2017.

[5] PR Newswire, "Global Commercial Satellite Imaging Market Size, Share, Development, Growth and Demand Forecast to 2023—Industry Insights by Application, and by End-User," October 10, 2017.

[6] Esri, "Panchromatic Image," GIS Dictionary, undated-b.

[7] Esri, "Multispectral," GIS Dictionary, undated-a.

[8] Debra Werner, "Raytheon Moves Into Commercial Imaging Market with DigitalGlobe Camera Order," *Space News*, October 11, 2017.

[9] David S. Germroth, "Commercial SAR Comes to the U.S. (Finally!)," *Apogeo Spatial*, May 9, 2016.

[10] David Hawk, with Amanda Mortwedt Oh, *The Parallel Gulag: North Korea's "An-jeon-bu" Prison Camps*, Washington, D.C.: Committee for Human Rights in North Korea, 2017.

[11] Aric Toler, "Geolocating Stanislav Tarasov," Bellingcat, May 28, 2015.

[12] Bellingcat Investigation Team, "Tanks of Buhaivka: A Training Facility in Eastern Ukraine," Bellingcat, March 17, 2017.

[13] Hady Al-Khatib, "Examining the Chemical Attack in Sukkari District in Aleppo, September 6th 2016," Bellingcat, September 23, 2016.

[14] Eliot Higgins, "Signs of Mustard Gas Use in September ISIS Chemical Attacks," Bellingcat, September 21, 2016.

[15] Christiaan Triebert, "The Khan Sheikhoun Chemical Attack—Who Bombed What and When?" Bellingcat, April 10, 2017.

[16] Sandra Erwin, "With Commercial Satellite Imagery, Computer Learns to Quickly Find Missile Sites in China," *Space News*, October 19, 2017.

[17] Erwin, 2017.

[18] NORSAR, "Summing Up the Nuclear Test in North Korea on 3 September 2017," September 22, 2017.

[19] Anna Fifield, "In Latest Test, North Korea Detonates Its Most Powerful Nuclear Device Yet," *Washington Post*, September 3, 2017.

[20] Bonnie Berkowitz, Laris Karklis, and Kevin Schaul, "How Three Recent Launches Signaled New Leaps in North Korea's Missile Capabilities," *Washington Post*, September 3, 2017.

[21] Doug Madory, "North Korea Gets New Internet Link via Russia," *Dyn*, October 2, 2017.

[22] Martyn Williams, "Russia Provides New Internet Connection to North Korea," *38 North*, October 1, 2017.

[23] Dan Woods, "Do You Suffer from the Data Not Invented Here Syndrome?" *Forbes*, November 15, 2012.

[24] Artner, Girven, and Bruce, 2016.

[25] Shahram Heshmat, "What Is Behavioral Economics?" *Psychology Today*, May 3, 2017.

[26] One such example is Christopher Gustafson, "Health, Obesity, and Behavioral Economics," *Cornhusker Economics*, University of Nebraska Institute of Agriculture and Natural Resources, January 7, 2015.

[27] Cortney Weinbaum, Richard Girven, and Arthur Chan, *Roadmap to Succeed in the Open: For the National Geospatial-Intelligence Agency's Human Development Directorate*, Santa Monica, Calif.: RAND Corporation, TL-251-NGA, 2017.

[28] Derek Grossman, "Keeping Up with the Policymakers: The Unclassified Tearline," *War on the Rocks*, July 28, 2016.

[29] Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, Washington, D.C., January 6, 2017.

[30] Priest, 2017.

[31] U.S. House of Representatives, H. Rept. 114-144, Intelligence Authorization Act for Fiscal Year 2016, 114th Congress, June 9, 2015.

[32] Michael Morell, "Robert Cardillo on the NGA's Role in the Raid on Osama bin Laden's Compound," *Intelligence Matters*, podcast of the "The Cipher Brief" website, November 7, 2017.

Chapter 6. Surging Intelligence in an Unpredictable World

The IC, operating in an environment of ever-changing and unexpected developments, has labored for decades to find the best way to *surge* to meet the requirements of crises and conflict. This challenge has only been exacerbated in the past several decades by the collapse of the Soviet Union and the end of a world order dominated by two major powers. The rapid expansion of social media and attendant velocity with which information moves around the globe has increased the speed of change. As a result, the IC is left facing a more diverse set of global problems and an increasingly complex prioritization challenge than ever before. In his February 2016 congressional testimony, then–Director of National Intelligence James Clapper noted that the United States is facing the most "diverse global threat environment" in 55 years.[1]

Indeed, today the United States is facing myriad crises and a wide array of threats, including ongoing instability and conflict in the Middle East, sophisticated and growing cyber threats, a North Korea on the verge of obtaining a deliverable nuclear weapon capability, the proliferation of WMD, violent extremism and terrorism, migrant and refugee crises, and technological innovation among adversaries (including cyber, the growing capabilities of nonstate actors, and information warfare)—just to name a few.[2] Taken together, these challenges present the IC with a daunting task and underscore the need for persistence in collection, global analytic coverage, and more-agile intelligence organizations that can seamlessly and rapidly surge to crises.

With this as a backdrop, the 2018 *National Defense Strategy* raises the specter of a new challenge: the reemergence of strategic competition among great powers, namely a resurgent Russia with its challenge to the post–Cold War order in Europe, and an increasingly assertive China. The strategy argues that both Moscow and Beijing can now contest U.S. dominance on the battlefield, while advances in technology are changing the character of war. While acknowledging that the United States must continue to fight terrorism and counter rogue regimes such as North Korea and Iran, the strategy is clear that the United States must be prepared to fight and win in a conflict with a near-peer competitor.[3] An escalating crisis or conflict with Russia or China would put far greater strain on the IC than current crises and conflicts, and significantly compound the surge problem.

The IC's structure—with its analyst-to-task ratios and standard set of dissemination mechanisms and product lines—is well suited to peacetime operations utilizing routinized procedures and staff organized to the routine tasks at hand. In stable regions of the world, the IC uses such an approach to fulfill its missions of providing foundational intelligence, topical updates, and predictive analysis. However, during emerging crises and conflict, the demands for intelligence—from the tactical to the strategic—and the speed at which it is needed increase dramatically, necessitating a surge of resources, for both analysis and collection, to ensure that policymakers and warfighters have the intelligence they need for decision advantage.

The wide array of global challenges facing the IC, combined with insufficient global coverage, makes warning of pending crises and the ability to surge to the crisis more difficult while also increasing the likelihood of a major intelligence failure. We discuss these issues further below and also recommend some measures that IC leaders might consider in seeking to build a more sustainable approach to crisis response.

A Global Power with Insufficient Global Coverage

The United States is a global power with global interests, and its policymakers and warfighters expect near-global coverage from the IC. In a world awash in information, the IC's relevancy is predicated in large part on its ability to provide actionable, insightful knowledge to decisionmakers in a timely fashion. Many senior leaders outside the IC believe that the IC has persistent global coverage in peacetime, that there is sufficient collection and analytic coverage everywhere and on every issue, and that, in the event of an unforeseen crisis, the IC is able to provide insight and understanding with only minimal augmentation and organizational disruption. When policymakers and warfighters pose an intelligence-related question, they expect that the IC can deliver an answer with unique insight in a reasonable period of time.

> The IC has insufficient collection and analytic coverage in many areas, because the majority of its resources are devoted, by design, to China, Russia, North Korea, Iran, and transnational violent extremism.

However, the IC has insufficient collection and analytic coverage in many areas,[4] because the majority of its resources are devoted, by design, to the "four plus one" problem sets: China, Russia, North Korea, Iran, and transnational violent extremism.[5] This level of effort is derived from the *National Intelligence Priorities Framework*, which in turn is driven by White House priorities.[6] The Defense Intelligence Enterprise (DIE) then further refines the IC's priorities based on the requirements of the Secretary of

When crises arise in unexpected places, the IC has to surge its analytic and collection resources to meet the increase in decisionmaker requirements.

Defense, the Chairman of the Joint Chiefs of Staff, and the combatant commands.[7] The DIE apportions the work for its constituent elements through the Defense Intelligence Analysis Program (DIAP), the seminal document governing who does what in the enterprise.[8] Each defense intelligence organization is responsible for analysis and production in its respective areas. This organizing principle can be effective in peacetime but is not designed for crises, conflict, or war, where the demands for integrated intelligence analysis rapidly skyrocket.

These prioritization schemes, while essential, result in a disproportionate investment in the top-priority issues and countries, which leaves much more limited collection and analytic resources devoted to other lower-priority issues and countries.[9] The wide array of challenges and the speed of change inevitably mean that there are unforeseen developments across the globe that the IC is ill-prepared to handle. The lack of foundational intelligence, collection, and analytic resources and expertise make surging to these crises much more difficult.

Shifting Priorities and Intelligence Needs During Crises

New administrations often bring new priorities and focus areas, while defense and command priorities also shift over time with global developments and as U.S. interests change, thus complicating the IC's resource allocation challenge. There is a time lag between an administration's change in priorities and the IC's ability to develop new sources, gain access, update foundational intelligence databases, and develop analytic expertise. Thus, while prioritization mechanisms provide the IC with authoritative guidance on where to direct resources, the need for prioritization points to limits in intelligence coverage, since there are insufficient resources to address all potential issues. When crises arise in unexpected places, the IC has to surge its analytic and collection resources to meet the increase in decisionmaker requirements.

Consumers of intelligence—from the President, the National Security Council, and national policymakers down to senior warfighters, including at the combatant commands and their components—expect high-quality intelligence to make informed decisions during crises and conflicts.[10] During crises, customer demands for intelligence rise dramatically, and, as long as intelligence is free at the point of delivery, these stakeholders will demand "all knowledge all the time," thus exacerbating the response times. The pace of events and increased collection lead to increased reporting, and these data need to be evaluated, analyzed and packaged for key consumers. The IC often requires 24/7 operations to keep pace with events and the creation of new product lines, such as situation reports or daily intelligence summaries, to cover the full range of developments. Providing this level of service requires enormous resources, which means that analysts and collectors with various levels of expertise are called on to surge to the problem. Many will have little to no familiarity with the new target set. In addition, surging personnel typically have to put aside their regular responsibilities, thus thinning out the coverage in lower-priority areas.

The IC's Typical Approach to a Surge

Surging to crisis is an IC-wide challenge, but it is particularly difficult for the DIE, because it is responsible for providing intelligence not only to policymakers but also to commanders and warfighters, who often require more-detailed, actionable intelligence. Crises usually involve DoD, the combatant commands, and some form of military action, which might range from deterrence operations to combat. Even unexpected natural catastrophes or humanitarian events often require the U.S. military to engage. This means increasing demands for order-of-battle data, targeting, and operational intelligence, such as force tracking, in addition to strategic analysis. This type of intelligence is time-consuming and requires substantial augmentation of personnel.

In the DIE, the approach to a surge has been for the various elements to establish crisis working groups or intelligence task forces to augment the analytic effort for the speed of war, a time-consuming and often disruptive endeavor. If a joint task force is established, the IC will surge resources to build out an analytic center to support the operational commander. Figure 6.1 shows the typical surge for a crisis where personnel within the existing workforce (shown by the dashed line ceiling) are reassigned or reallocated to the crisis.

The IC's ability to do predictive, anticipatory analysis and effective warning would help ease the transition into a surge, although improved warning alone is not the solution. First, there will always be unexpected developments and unanticipated crises, because the world is an unpredictable place. Second, the IC's prioritization schema means that there are probably insufficient analytic and collection resources, as well as a lack of depth and expertise in low-density areas in any case. As a result, the IC surges to unexpected threats or crises when they occur in an area of inadequate coverage, taking resources from across geographic regions or functional areas to the crisis at hand, often with analysts who have little knowledge of the country, region, or problem set, to meet demanding, high-paced requirements.

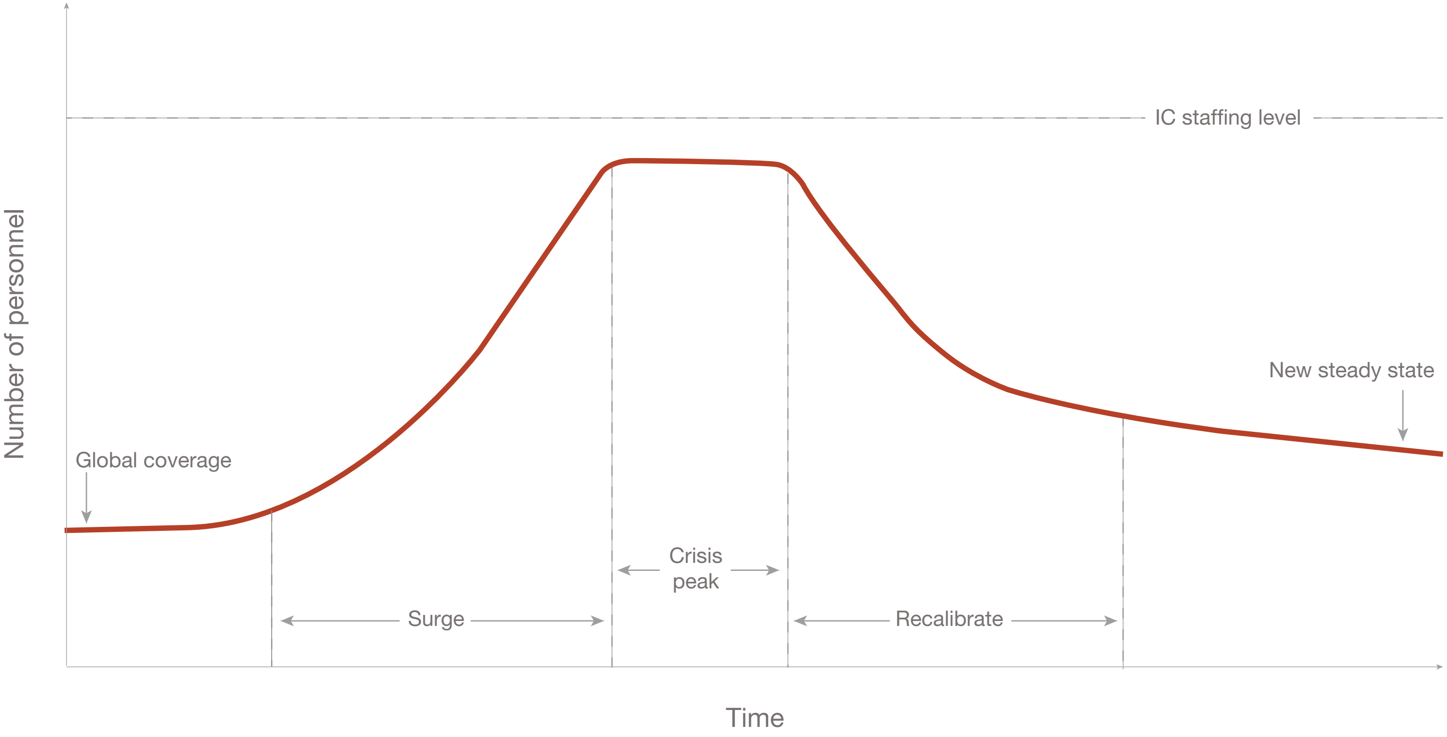
Examples of Surging During Crisis

There are numerous examples of DIE elements surging to a crisis to meet new mission demands. In most cases, the organizations were largely unprepared in terms of resources and expertise to address the emerging crisis or steady-state crisis operations. Some noteworthy examples:

Iraq in 2003

Following the 2003 invasion of Iraq, the IC established the Combined Intelligence-Operations Center (CIOC) in

Figure 6.1. Typical Surge



Baghdad to provide strategic and operational intelligence to the Multi-National Force–Iraq (MNF-I) Commander and his senior staff. The CIOC included more than 100 analysts, largely from DIA, but also small numbers of NGA, NSA, and allied intelligence officers.[11] In the aggregate, the IC had built great depth of expertise on Iraq and the region and developed substantial analytic resources and robust collection but, given the demands at the national level, was unable or unwilling to fully resource the organization with IC cadre. Instead, MNF-I turned to the reserves to fill out the ranks, most of whom deployed to Iraq for one-year tours but had little knowledge of Iraq and often marginal skills as intelligence analysts. This led to inefficiencies and a lack of depth and analytic capability, necessitating robust reachback to DIA and U.S. Central Command for expert analysis.

Israel/Gaza in 2014

In response to a barrage of rocket attacks, the Israeli Defense Forces (IDF) launched heavy air and artillery strikes against HAMAS in July 2014, followed by a ground incursion into the Gaza strip. Operation Protective Edge continued until late August, when a ceasefire was finally established.[12] Although the IC was following the escalating conflict, it did not anticipate the large-scale IDF ground incursion, which necessitated a significantly higher level of effort than past Israel-HAMAS conflicts. Meanwhile, higher-priority issues in the region, including the rise of ISIS and the conflicts in Syria and Iraq, resulted in the U.S. European Command Joint Intelligence Operations Center taking on the majority of the analytic responsibility for the DIE, necessitating a significant surge of resources to monitor the conflict and produce detailed daily intelligence reports.

Russia/Ukraine in 2014

Unrest and instability in Ukraine leading to the ousting of the pro-Russian government in Kiev sparked a Russian military intervention into Crimea and subsequently eastern Ukraine.[13] Russia's annexation of Crimea and military support to pro-Russian insurgents in the Donbas presented the IC with a significant challenge. With the collapse of the Soviet Union, the IC had allowed its collection and analytic capabilities to atrophy and was unprepared in terms of collection, analytic resources, and expertise for a resurgent Russia with possible further military designs on its near abroad. The IC surged to the crisis but also began a lengthy build of resources to address the long-term strategic shift.

> In most cases, building out a crisis team was a zero-sum game from a resource perspective, at least initially.

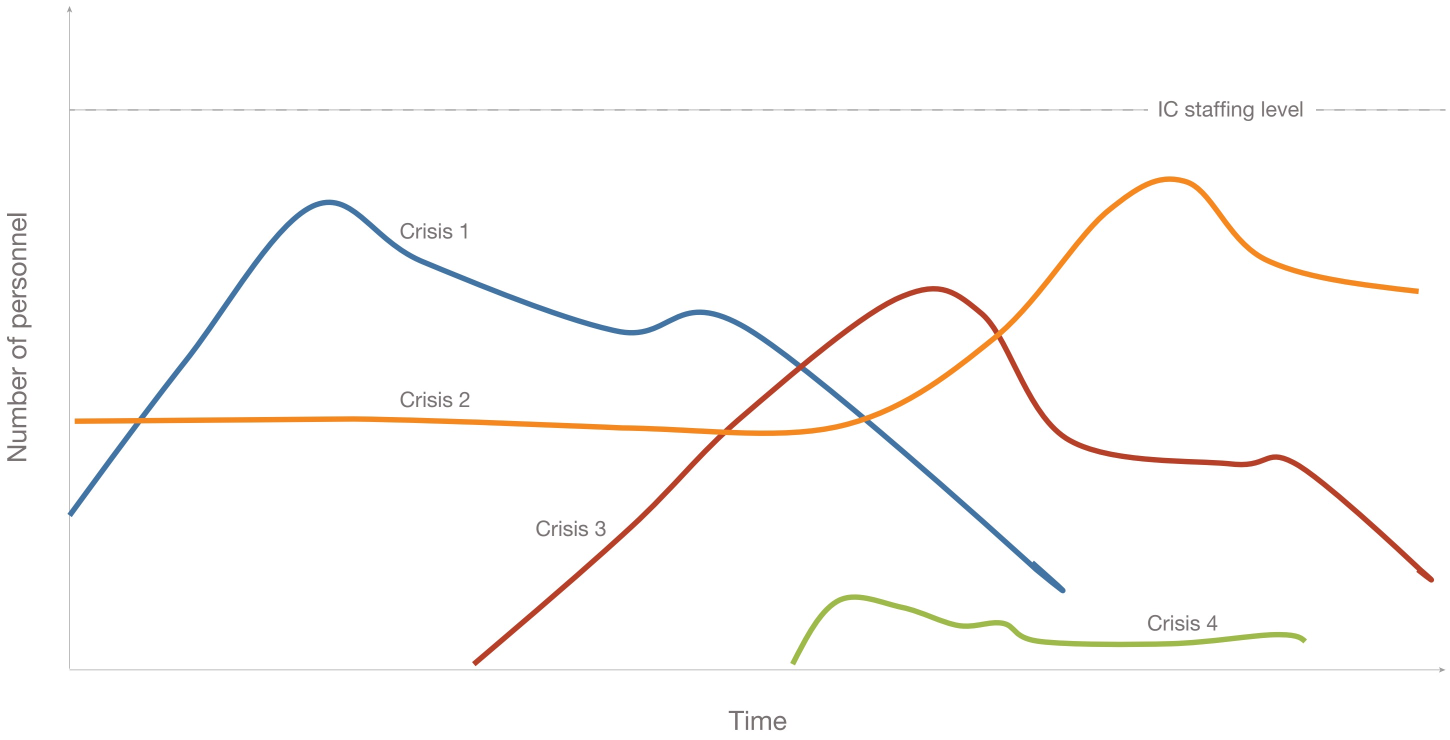
Russia/Syria in 2015

Russia militarily intervened in the Syrian civil war in late September 2015 to prop up Syrian leader Bashar al-Assad. Again, the IC was surprised by Russia's unprecedented expeditionary deployment and its subsequent broader effort to insert itself into the region, and the IC moved to quickly establish effective crisis operations.[14] The key DIE stakeholders leveraged technology and a federated approach to analysis and production to meet the mission requirements efficiently and with minimal organizational disruption. This virtual task force met daily via video teleconference and published a joint daily intelligence summary to which each element contributed, in accordance with its expertise and DIAP responsibilities.

Surging Has Meant Making Trade-Offs

There are many other examples, but in most cases, building out a crisis team was a zero-sum game from a resource perspective, at least initially. Agencies surged analysts and

Figure 6.2. Multiple Crises



collectors for the crisis at hand, reducing coverage elsewhere and thereby decreasing the IC's ability to predict or cover another crisis. Multiple crises simultaneously only exacerbate the problem further, presenting an even more demanding management challenge, as shown in Figure 6.2. Indeed, the IC has functioned this way for many years, given the multiple crises and conflicts in the Middle East, the terrorism arena, and now Russia.

What Can Be Done to Improve the IC's Surge Response?

There are a number of measures to consider that will offer more-sustainable approaches for crisis response while not undermining or diluting existing mission areas and minimizing organizational disruption. A large expansion of intelligence resources to achieve genuine global coverage almost certainly is not a viable option, but some investment will be required to address this vexing problem. If the IC were to identify and implement systematic and sustainable approaches to resource allocation, intelligence leaders could mitigate risks associated with inadequate anticipatory intelligence and warning, and events that could not have reasonably been foreseen. Several solutions can be implemented concurrently to address different parts of this challenge and ease the transition from steady-state operations to crisis and conflict.

Foundational Intelligence

Increasing the commitment of resources to foundational intelligence is probably the most critical measure to ensuring smooth transitions to crisis and conflict. Foundational intelligence—the in-depth knowledge of the operating environment, the organization, command and control, equipment and operating practices of foreign armed forces, and the military and civilian infrastructure that supports those forces[15]—will significantly assist the IC in getting up to speed quickly and provide the baseline intelligence needed for targeting, force tracking, and overall understanding of the situation. While the IC does not have the resources to cover all places around the globe at equal priority, it is beginning to employ advanced techniques in data science to leverage big data and develop more-comprehensive foundational intelligence at a reasonable cost. DIA in particular is accessing large quantities of open-source information and employing various techniques to build out its foundational intelligence databases without the need of a large analytic workforce. The DIE is also bringing back the military capability studies, which will serve as a ready reference for analysts and be particularly helpful in getting up to speed in a crisis. To ensure high-quality analysis, foundational work needs to become career-enhancing and attractive to the workforce. For example, filling a foundational intelligence position could be a prerequisite for promotion to mid-level analytic positions.

Decentralized Centralization, or the "Virtual Task Force"

Another approach is to leverage technology and collaboration to establish a virtual crisis team that can meet mission requirements without significant disruption to the participating agencies. This approach leverages the expertise and skills of each organization in accordance with its DIAP roles and responsibilities to jointly meet the analysis and production requirements of the leadership. Such an approach is possible only with common analytic tradecraft standards for quality control, as outlined in ICD 203.[16] As noted above, this model worked extremely well during the Russian force deployment to Syria, allowing the DIE to ensure that it had the requisite expertise and resources available to meet customer requirements within the DIAP construct. This is an approach that is both repeatable and scalable across the IC to address any problem set.

Standing Crisis Teams

Agencies could create small teams with the necessary spaces, IT infrastructure, and organizational structure to seamlessly transition from routine, steady-state operations to crisis and even move from crisis to crisis. The individuals manning these teams would not be subject-matter experts, but would have the functional expertise necessary to jump-start a crisis team—such as IT, writing, briefing, and collection management—and to prepare for the arrival of additional personnel, including subject-matter experts. Each team would be the shell of an organization for analysts and managers to fall into in the event of a crisis. Such teams could be built around the 24/7 watches that most agencies already have in place. This approach would create a more seamless transition in the early phase of establishing a crisis team but would need to be augmented by experts in the topic area.

Academic Outreach/Open-Source Intelligence

Academics and outside experts have the potential to provide depth and expertise in cases where the IC lacks such expertise in-house. ODNI has called for the IC to leverage outside experts as necessary to meet the mission in ICD 205, in what is described as an "essential intelligence activity."[17] Outside experts often can provide depth and insight on specific topics for which the expertise is not resident in the IC. Outside experts can also provide valuable alternative views on particular issues. There are a number of ways to leverage outside expertise, including developing a cadre of cleared academic experts on-call who can be brought in during a crisis and function as senior analysts and advisers, or be employed as consultants. This approach is particularly useful in low-density topic areas where the IC has been unable to invest analytic resources and develop deep, organic expertise. Related, improved use of OSINT (as discussed in Chapter Five), including big data and social media analysis, can offer valuable unique knowledge and insights, and help to get a new surge team up to speed quickly. OSINT also is a valuable asset in mitigating the global coverage challenge.

The Contract Workforce

Contract analysts could be employed specifically to augment crisis teams, rapidly providing a ready cadre of analysts. They would be trained with critical skills needed to ensure a rapid and largely seamless transition. This cadre workforce would probably have limited target knowledge, because it is not possible to predict with any certainty where the next crisis will emerge, but this workforce would have the requisite functional skills for high operational tempo. Both the academic outreach and contractor options would incur some additional cost to the government.

Allies and Partners

Leveraging allies and partners has the potential to be a genuine force multiplier in crisis operations. A number of partner nations, the Five Eyes (United States, United Kingdom, Canada, Australia, and New Zealand) in particular, have very capable intelligence services with high levels of expertise. The UK Ministry of Defence–led Defense Intelligence Fusion Center at RAF Wyton in Cambridgeshire is a model for bilateral and multilateral intelligence operations.[18] This state-of-the-art intelligence center, with its modern IT suites and innovative design, is aimed at facilitating collaboration across the Five Eyes community and is well suited for collaborative crisis intelligence operations. The NATO Intelligence Fusion Center (NIFC) at RAF Molesworth, UK, provides a similar capability at the NATO level. During the Ukraine/Crimea crisis, the NIFC was able to leverage expertise from across NATO to provide high-quality, multilateral intelligence analysis to NATO leaders. Key allies and partners in most theaters and potential crisis areas often have unique and valuable intelligence that adds significant value to the U.S. IC knowledge and can augment U.S. intelligence efforts.

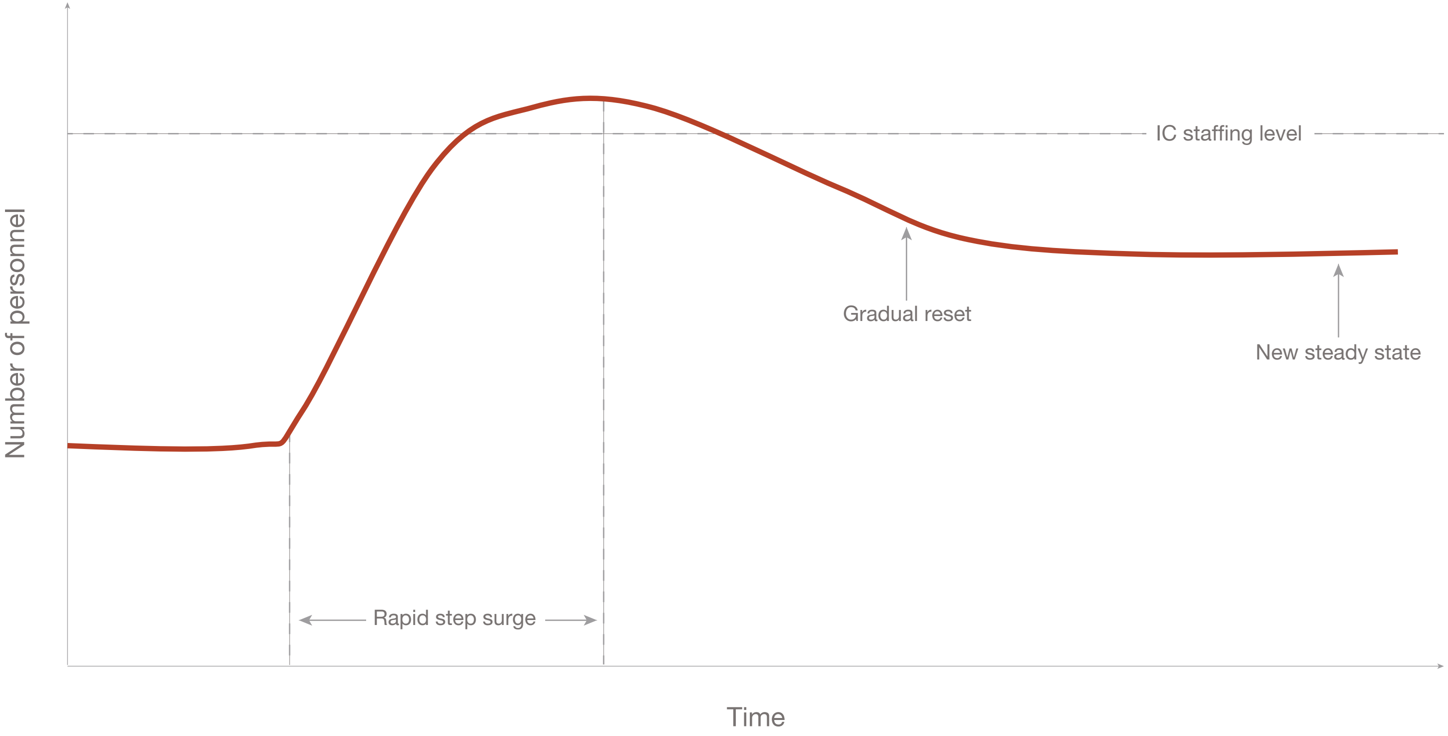
Concluding Thoughts

The complex and rapidly changing global threat environment, combined with the prospect of conflict with a near-peer competitor, presents the IC with a range of challenges in terms of how to efficiently and effectively surge to crises. The examples discussed above are just a small sample of the many crises the IC has supported over the past decades. Other notable examples include the Global War on Terror, Afghanistan, the rise of ISIS, Iranian malign activity, the North Korea nuclear problem, and China's moves in the South China Sea. All of these challenges taxed the IC in the early stages, but, over time, additional analytic and collection resources meant a return to some semblance of steady-state operations, though at a much higher operational tempo. Unanticipated crises in low-density areas, such as an implosion in Mexico, an economic meltdown in Brazil, or an unexpected disaster in Europe, will always be a significant challenge. That said, a conflict with a near-peer competitor—Russia or China—or war with North Korea or Iran would be a game changer, requiring far more resources than currently reside inside the IC to meet policymaker and warfighter demands, as shown in Figure 6.3.

None of the recommendations offered in this chapter will solve this complex problem alone. However, in combination, these options have the potential to go a long way toward easing the transition from steady-state operations to crisis and conflict with minimal organizational disruption while ensuring that requisite expertise is available to provide policymakers and warfighters with the intelligence they need for decision advantage.

> Conflict with Russia or China or war with North Korea or Iran would be a game changer, requiring far more resources than currently reside inside the IC.

Figure 6.3. Surge to Crisis with a Near-Peer Competitor



Chapter Notes

[1] Brian Murphy, "Director of National Intelligence James Clapper Outlines 'Litany of Doom' in U. S. Intelligence Community's Annual Worldwide Threat Assessment on Capitol Hill," *Medium*, June 2, 2016.

[2] Cheryl Pellerin, "Vickers: Defense Intelligence Enterprise Poised for Historic Transition," Department of Defense website, January 21, 2015.

[3] U.S. Department of Defense, 2018.

[4] John A. Kringen, "Rethinking the Concept of Global Coverage in the US Intelligence Community," *Studies in Intelligence*, Vol. 59, No. 3, September 2015.

[5] Fred Dews, "Joint Chiefs Chairman Dunford on the '4+1 Framework' and Meeting Transnational Threats," Brookings Institute, February 24, 2017.

[6] Intelligence Community Directive 204, 2015.

[7] The *Defense Intelligence Enterprise* normally refers to DIA, the four service intelligence centers, and the Combatant Command Joint Intelligence Operations Centers. See Department of Defense Instruction 3020.51, *Intelligence Support to the Defense Critical Infrastructure Program (DCIP)*, Washington, D.C.: U.S. Department of Defense, June 23, 2011 (incorporating change 1, effective March 7, 2018), p. 14.

[8] Although they are DoD agencies, neither NGA nor NSA is included in the DIAP, because they are single "INT" agencies, rather than all-source analytic organizations. See Defense Intelligence Agency, Directorate for Analysis, "DI Partners: Defense Intelligence Analysis Program," *Overview*, undated, p. 2.

[9] Kringen, 2015.

[10] Joint Publication 2.0, 2013.

[11] Author Richard Baffa was deployed as the senior intelligence officer at the CIOC from January to June 2008 and again from May to September 2009. These observations are based on his personal experience deployed in Iraq.

[12] Eitan Shamir, "Rethinking Operation Protective Edge: The 2014 Gaza War," *Middle East Quarterly*, Vol. 22, No. 2, Spring 2015.

[13] BBC, "Ukraine Crisis: Timeline," November 13, 2014.

[14] Mark Hosenball, Phil Stewart, and Matt Spetalnick, "US Spy Agencies Were 'Caught Off-Guard' by Putin's Sudden Dramatic Escalation in Syria," Reuters, October 8, 2015.

[15] Defense Intelligence Agency, *Defense Intelligence Agency Strategy 2016*, Washington, D.C., 2016, p. 4.

[16] Intelligence Community Directive 203, 2015.

[17] Intelligence Community Directive 205, *Analytic Outreach*, Washington, D.C.: Office of the Director of National Intelligence, August 28, 2013.

[18] United Kingdom Ministry of Defence, "New Defence Intelligence Buildings Handed Over to MOD," March 16, 2012.

Chapter 7. Conclusion

The essays in this Perspective describe critical hurdles for the IC to overcome in order to excel in a strategic environment of near-peer adversaries with technological innovations, but they only touch the surface. The domains described in the previous five chapters—strategic warning, TCPED, security, OSINT, and crisis surge—provide some key areas where the IC can enact changes with wide ramifications and long-term effects. We believe that changes in these five domains will improve the IC's preparedness for large-scale crises with near-peer adversaries and against emerging technological threats.

Each area we addressed needs solutions that the IC can execute. The IC and its subordinate agencies' structures, processes, tradecraft, frameworks, and training are due for upgrades amidst major drivers of change. Outdated organizational structures, legacy technology, and rigid processes create burdens that incremental changes cannot significantly overcome. This Perspective provides the first strategic steps for overcoming some of these burdens.

Abbreviations

CI	counterintelligence
CIA	Central Intelligence Agency
DHS	U.S. Department of Homeland Security
DIA	Defense Intelligence Agency
DIAP	Defense Intelligence Analysis Program
DIE	Defense Intelligence Enterprise
DNI	Director of National Intelligence
DoD	U.S. Department of Defense
FBI	Federal Bureau of Investigation
FY	fiscal year
GEOINT	geospatial intelligence
HEIC	head of an element of the IC
HPSCI	House Permanent Select Committee on Intelligence
HUMINT	human intelligence
IARPA	Intelligence Advance Research Project Activity
IC	U.S. Intelligence Community
ICD	Intelligence Community Directive
IMINT	imagery intelligence
INT	intelligence-gathering discipline
IT	information technology
IRTPA	Intelligence Reform and Terrorism Prevention Act
MASINT	measurement and signature intelligence
NCIX	National Counterintelligence Executive
NCSC	National Counterintelligence and Security Center
NGA	National Geospatial-Intelligence Agency
NIC	National Intelligence Council
NIO	National Intelligence Officer
NIPF	National Intelligence Priorities Framework
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OPM	U.S. Office of Personnel Management
OSINT	open-source intelligence
PAI	publicly available information
SAT	structured analytic technique
SIGINT	signals intelligence
TCPED	tasking, collection, processing, exploitation, and dissemination
WMD	weapons of mass destruction

References

Al-Khatib, Hady, "Examining the Chemical Attack in Sukkari District in Aleppo, September 6th 2016," Bellingcat, September 23, 2016. As of June 22, 2018: https://www.bellingcat.com/news/mena/2016/09/23/examining-chemical-attack-sukkari-district-aleppo-september-6th-2016/

Artner, Stephen, Richard S. Girven, and James B. Bruce, *Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community*, Santa Monica, Calif.: RAND Corporation, RR-1408-OSD, 2016. As of June 22, 2018: https://www.rand.org/pubs/research_reports/RR1408.html

BBC, "Ukraine Crisis: Timeline," November 13, 2014. As of June 22, 2018: http://www.bbc.com/news/world-middle-east-26248275

Bellingcat Investigation Team, "Tanks of Buhaivka: A Training Facility in Eastern Ukraine," Bellingcat, March 17, 2017. As of June 22, 2018: https://www.bellingcat.com/news/uk-and-europe/2017/03/17/tanks-buhaivka-training-facility-eastern-ukraine/

Berkowitz, Bonnie, Laris Karklis, and Kevin Schaul, "How Three Recent Launches Signaled New Leaps in North Korea's Missile Capabilities," *Washington Post*, September 3, 2017.

Best, Richard A., *Intelligence Reform After Five Years: The Role of the Director of National Intelligence*, Washington, D.C.: Congressional Research Service, June 22, 2010.

Bridgeman, Vincent H., "Defense Counterintelligence Reconceptualized," in Jennifer E. Simms and Burton Gerber, eds., *Vaults, Mirrors, and Masks*, Washington, D.C.: Georgetown University Press, 2009, pp. 125–148.

Bruce, James B., and Jeffrey Martini, *Whither Al-Anbar Province: Five Scenarios Through 2011*, Santa Monica, Calif.: RAND Corporation, OP-278-MCIA, 2010. As of June 22, 2018: https://www.rand.org/pubs/occasional_papers/OP278.html

Central Intelligence Agency, "The Beginning of Intelligence Analysis in CIA," undated. As of June 22, 2018: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no2/the-beginning-of-intelligence-analysis-in-cia.html

Christensen, Michelle D., *Security Clearance Process: Answers to Frequently Asked Questions*, Washington, D.C.: Congressional Research Service, R43216, October 7, 2016.

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States*, March 31, 2005. As of June 22, 2018: https://www.gpo.gov/fdsys/pkg/GPO-WMD/pdf/GPO-WMD.pdf

Davis, Jack, *Improving CIA Analytic Performance: Strategic Warning*, Washington, D.C.: Central Intelligence Agency, Sherman Kent Center for Intelligence Analysis, Occasional Papers, Vol. 1, No. 1, September 2002a. As of June 22, 2018: https://www.cia.gov/library/kent-center-occasional-papers/pdf/OPNo1.pdf

Davis, Jack, *Sherman Kent and the Profession of Intelligence Analysis*, Washington, D.C.: Central Intelligence Agency, Sherman Kent Center for Intelligence Analysis, Occasional Papers, Vol. 1, No. 5, November 2002b. As of June 22, 2018: https://www.cia.gov/library/kent-center-occasional-papers/vol1no5.htm

Debusmann, Bernd, "U.S. Intelligence Spending—Value for Money?" Reuters, July 16, 2010. As of June 22, 2018: http://blogs.reuters.com/great-debate/2010/07/16/us-intelligence-spending-value-for-money/

Defense Intelligence Agency, *Defense Intelligence Agency Strategy 2016*, Washington, D.C., 2016. As of June 22, 2018: http://www.dia.mil/Portals/27/Documents/About/2016_DIA_Strategy.pdf

Defense Intelligence Agency, Directorate for Analysis, “DI Partners: Defense Intelligence Analysis Program,” *Overview*, undated. As of June 22, 2018:
https://nsarchive2.gwu.edu/NSAEBB/NSAEBB534-DIA-Declassified-Sourcebook/documents/DIA-43.pdf

Department of Defense Directive No. 5200.43, *Management of the Defense Security Enterprise*, Washington, D.C.: U.S. Department of Defense, October 1, 2012, Incorporating Change 2, August 15, 2017.

Department of Defense Instruction 3020.51, *Intelligence Support to the Defense Critical Infrastructure Program (DCIP)*, Washington, D.C.: U.S. Department of Defense, June 23, 2011 (incorporating change 1, effective March 7, 2018).

Department of Defense Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, Washington, D.C.: U.S. Department of Defense, August 8, 2016.

Dews, Fred, “Joint Chiefs Chairman Dunford on the ‘4+1 Framework’ and Meeting Transnational Threats,” Brookings Institute, February 24, 2017. As of June 22, 2018:
https://www.brookings.edu/blog/brookings-now/2017/02/24/joint-chiefs-chairman-dunford-transnational-threats

Director of Central Intelligence, *DCI Task Force Report: Improving Intelligence Warning*, Washington, D.C., May 29, 1992, p. 4, approved for public release April 25, 2012.

Director of Central Intelligence, memorandum for National Foreign Intelligence Board, “Subject: Warning,” July 17, 1992.

Director of National Intelligence, *Vision 2015: A Globally Networked and Integrated Intelligence Enterprise*, undated. As of June 22, 2018:
https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Vision_2015.pdf

The Economist, “Predicting the Future: Unclouded Vision,” September 26, 2015.

Erwin, Sandra, “With Commercial Satellite Imagery, Computer Learns to Quickly Find Missile Sites in China,” *Space News*, October 19, 2017. As of June 22, 2018:
http://spacenews.com/with-commercial-satellite-imagery-computer-learns-to-quickly-find-missile-sites-in-china/

Esri, “Multispectral,” *GIS Dictionary*, undated-a. As of November 7, 2017:
http://support.esri.com/en/other-resources/gis-dictionary/term/multispectral

Esri, “Panchromatic Image,” *GIS Dictionary*, undated-b. As of November 7, 2017:
http://support.esri.com/en/other-resources/gis-dictionary/term/panchromatic%20image

Executive Order 12333, U*nited States Intelligence Activities*, Washington, D.C.: The White House, December 4, 1981, amended July 30, 2008.

Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, Washington, D.C.: The White House, October 7, 2011.

Fifield, Anna, “In Latest Test, North Korea Detonates Its Most Powerful Nuclear Device Yet,” *Washington Post*, September 3, 2017.

Gellman, Barton, Dafna Linzer, and Carol D. Leonnig, “Surveillance Net Yields Few Suspects,” *Washington Post*, February 5, 2006.

George, Roger Z., and James B. Bruce, eds., *Analyzing Intelligence: Origins, Obstacles, and Innovations*, Washington, D.C.: Georgetown University Press, 2008.

Germroth, David S., “Commercial SAR Comes to the U.S. (Finally!),” *Apogeo Spatial*, May 9, 2016. As of June 22, 2018:
http://apogeospatial.com/commercial-sar-comes-to-the-u-s-finally/

Grossman, Derek, “Keeping Up with the Policymakers: The Unclassified Tearline,” *War on the Rocks*, July 28, 2016. As of June 22, 2018:
https://warontherocks.com/2016/07/keeping-up-with-the-policymakers-the-unclassified-tearline/

Gustafson, Christopher, “Health, Obesity, and Behavioral Economics,” *Cornhusker Economics*, University of Nebraska Institute of Agriculture and Natural Resources, January 7, 2015. As of June 22, 2018:
https://digitalcommons.unl.edu/agecon_cornhusker/696/

Halman, Alexander, “Before and Beyond Anticipatory Intelligence: Assessing the Potential for Crowdsourcing and Intelligence Studies,” *Journal of Strategic Security*, Vol. 8, No. 5, Fall 2015.

Hawk, David, with Amanda Mortwedt Oh, *The Parallel Gulag: North Korea’s “An-jeon-bu” Prison Camps*, Washington, D.C.: Committee for Human Rights in North Korea, 2017. As of June 22, 2018:
https://www.hrnk.org/uploads/pdfs/Hawk_The_Parallel_Gulag_Web.pdf

Heshmat, Shahram, “What Is Behavioral Economics?” *Psychology Today*, May 3, 2017.

Higgins, Eliot, "Signs of Mustard Gas Use in September ISIS Chemical Attacks," Bellingcat, September 21, 2016. As of June 22, 2018: https://www.bellingcat.com/news/mena/2016/09/21/signs-mustard-gas-use-september-isis-chemical-attacks/

Hosenball, Mark, Phil Stewart, and Matt Spetalnick, "US Spy Agencies Were 'Caught Off-Guard' by Putin's Sudden Dramatic Escalation in Syria," Reuters, October 8, 2015.

Intelligence Community Directive 203, *Analytic Standards*, Washington, D.C.: Office of the Director of National Intelligence, January 2, 2015. As of June 22, 2018: https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf

Intelligence Community Directive 204, *National Intelligence Priorities Framework*, Washington, D.C.: Office of the Director of National Intelligence, January 2, 2015. As of June 22, 2018: https://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf

Intelligence Community Directive 205, *Analytic Outreach*, Washington, D.C.: Office of the Director of National Intelligence, August 28, 2013. As of June 22, 2018: https://www.dni.gov/files/documents/ICD/ICD%20205%20-%20Analytic%20Outreach.pdf

Intelligence Community Directive 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*, Washington, D.C.: Office of the Director of National Intelligence, January 21, 2009.

Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms*, April 2018. As of June 22, 2018: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-07-06-092813-320

Joint Publication 2.0, *Joint Intelligence*, Washington D.C.: Chairman of the Joint Chiefs of Staff, October 22, 2013.

Katsos, George, Jerome Conrad, Frank Disimino, Ted Liddy, Anna Necheles, Charles Oliver, Christina Pham, and Basil White, eds., *United States Government Glossary of Interagency and Associated Terms*, Washington, D.C., July 2017. As of June 22, 2018: https://fas.org/irp/doddir/dod/usg-glossary.pdf

Knopp, Bradley M., Sina Beaghley, Aaron Frank, Rebeca Orrie, and Michael Watson, *Defining the Roles, Responsibilities, and Functions for Data Science Within the Defense Intelligence Agency*, Santa Monica, Calif.: RAND Corporation, RR-1582-DIA, 2016. As of June 22, 2018: https://www.rand.org/pubs/research_reports/RR1582.html

Kringen, John A., "Rethinking the Concept of Global Coverage in the US Intelligence Community," *Studies in Intelligence*, Vol. 59, No. 3, September 2015. As of June 22, 2018: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-3/pdfs/Keeping-Watch-on-the-World.pdf

Madory, Doug, "North Korea Gets New Internet Link via Russia," *Dyn*, October 2, 2017. As of June 22, 2018: https://dyn.com/blog/north-korea-gets-new-internet-link-via-russia/

Menand, Louis, "Everybody's an Expert: Putting Predicts to the Test," *The New Yorker*, December 5, 2005.

Miles, Anne Daugherty, *Intelligence Community Spending: Trends and Issues*, Washington, D.C.: Congressional Research Service, November 8, 2016.

Miller, Brett, "Evolution of Intel: How Valuable Is OSINT?" *In Public Safety*, July 24, 2015. As of June 22, 2018: https://inpublicsafety.com/2015/07/evolution-of-intel-how-valuable-is-osint/

Morell, Michael, "Robert Cardillo on the NGA's Role in the Raid on Osama bin Laden's Compound," *Intelligence Matters*, podcast of the "The Cipher Brief" website, November 7, 2017. As of June 22, 2018: https://www.thecipherbrief.com/podcasts/robert-cardillo-ngas-role-raid-osama-bin-ladens-compound

Murphy, Brian, "Director of National Intelligence James Clapper Outlines 'Litany of Doom' in U.S. Intelligence Community's Annual Worldwide Threat Assessment on Capitol Hill," *Medium*, June 2, 2016. As of June 22, 2018: https://medium.com/@ODNIgov/dni-clapper-outlines-litany-of-doom-in-annual-worldwide-threat-assessment-2f8e1a55fdc

National Geospatial-Intelligence Agency, "About NGA," undated. Accessed October 6, 2017: https://www.nga.mil/About/Pages/Default.aspx

National Security Agency, "Frequently Asked Questions: Signals Intelligence (SIGINT)," last modified May 3, 2016. As of June 22, 2018: https://www.nsa.gov/about/faqs/sigint-faqs.shtml

NORSAR, "Summing Up the Nuclear Test in North Korea on 3 September 2017," September 22, 2017. As of June 22, 2018: https://www.norsar.no/in-focus/summing-up-the-nuclear-test-in-north-korea-on-3-september-2017-article1554-863.html

Office of the Director of National Intelligence, "ODNI Fact Sheet," October 2011. As of June 22, 2018: https://www.dni.gov/files/documents/ODNI%20Fact%20Sheet_2011.pdf

Office of the Director of National Intelligence, *The National Intelligence Strategy of the United States of America: 2014*, Washington, D.C., 2014. As of January 5, 2015:
http://www.dni.gov/files/documents/2014_NIS_Publication.pdf

Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, Washington, D.C., January 6, 2017. As of June 22, 2018:
https://www.dni.gov/files/documents/ICA_2017_01.pdf

Office of the Director of National Intelligence, "U.S. Intelligence Community Budget," 2018. Accessed February 28, 2018:
https://www.dni.gov/index.php/what-we-do/ic-budget

Office of Director of National Intelligence, National Intelligence Council, "Global Trends," webpage, undated. Accessed January 8, 2018:
https://www.dni.gov/index.php/who-we-are/organizations/nic/nic-related-menus/nic-related-content/global-trends

Office of Director of National Intelligence, National Intelligence Council, "Global Trends: Paradox of Progress," 2016. As of June 22, 2018:
https://www.dni.gov/index.php/global-trends-home

Pellerin, Cheryl, "Vickers: Defense Intelligence Enterprise Poised for Historic Transition," U.S. Department of Defense website, January 21, 2015. As of June 22, 2018:
https://www.defense.gov/News/Article/Article/603947/

Priest, Dana, "Russia's Election Meddling IS Another Intelligence Failure," *The New Yorker*, November 13, 2017.

PR Newswire, "Global Commercial Satellite Imaging Market Size, Share, Development, Growth and Demand Forecast to 2023—Industry Insights by Application, and by End-User," October 10, 2017. As of June 22, 2018:
https://www.prnewswire.com/news-releases/global-commercial-satellite-imaging-market-size-share-development-growth-and-demand-forecast-to-2023---industry-insights-by-application-and-by-end-user-300534274.html

RAND Corporation, "Building a Sustainable International Order," webpage, 2018. As of June 22, 2018:
https://www.rand.org/nsrd/projects/international-order.html

Richardson, Admiral John M., letter to the Secretary of the Navy regarding the Washington Naval Yard shooting, November 8, 2013. As of June 22, 2018:
http://archive.defense.gov/pubs/Navy-Investigation-into-the-WNY-Shooting_final-report.pdf

Secretary of Defense Independent Review of the Washington Navy Yard Shooting, *Security from Within: Independent Review of the Washington Navy Yard Shooting*, November 2013. As of June 22, 2018:
https://www.defense.gov/Portals/1/Documents/pubs/Independent-Review-of-the-WNY-Shooting-14-Nov-2013.pdf

Shamir, Eitan, "Rethinking Operation Protective Edge: The 2014 Gaza War," *Middle East Quarterly*, Vol. 22, No. 2, Spring 2015. As of June 22, 2018:
http://www.meforum.org/5084/rethinking-operation-protective-edge

Sinclair, Robert S., *Thinking and Writing: Cognitive Science and Intelligence Analysis*, Center for the Study of Intelligence, February 2010 (revised edition of a monograph originally published in January 1984). As of June 22, 2018:
https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Thinking-and-Writing-Feb2010-web.pdf

Sullivan, Gary, "Too Much of a Good Thing," *Baltimore Sun*, August 27, 2014.

Toler, Aric, "Geolocating Stanislav Tarasov," Bellingcat, May 28, 2015. As of June 22, 2018:
https://www.bellingcat.com/resources/case-studies/2015/05/28/geolocating-stanislav-tarasov/

Triebert, Christiaan, "The Khan Sheikhoun Chemical Attack—Who Bombed What and When?" Bellingcat, April 10, 2017. As of June 22, 2018:
https://www.bellingcat.com/news/mena/2017/04/10/khan-sheikhoun-chemical-attack-bombed/

United Kingdom Ministry of Defence, "New Defence Intelligence Buildings Handed Over to MOD," March 16, 2012. As of June 22, 2018:
https://www.gov.uk/government/news/new-defence-intelligence-buildings-handed-over-to-mod--2

U.S. Code, Title 50, Section 3383, National Counterintelligence and Security Center.

U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, Washington, D.C., 2018. As of June 22, 2018:
https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

U.S. Government, *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*, March 2009. As of June 22, 2018:
https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf

U.S. House of Representatives, H. Rept. 114-144, Intelligence Authorization Act for Fiscal Year 2016, 114th Congress, June 9, 2015. As of June 22, 2018:
https://www.congress.gov/congressional-report/114th-congress/house-report/144

U.S. House of Representatives Permanent Select Committee on Intelligence, 104th Congress, *IC21: The Intelligence Community in the 21st Century*, June 5, 1996. As of June 22, 2018:
https://www.hsdl.org/?view&did=439040

U.S. Office of Personnel Management, "Suitability Executive Agent," undated. As of June 22, 2018:
https://www.opm.gov/investigations/suitability-executive-agent/

U.S. Office of Personnel Management, National Background Investigations Bureau, "About Us: Safeguarding Integrity and Transparency," undated. As of June 22, 2018:
https://nbib.opm.gov/about-us/

U.S. Senate, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities: Foreign and Military Intelligence Book I*, Washington D.C.: U.S. Government Printing Office, 1976.

Weinbaum, Cortney, Steven Berner, and Bruce McClintock, *SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain*, Santa Monica, Calif.: RAND Corporation, PE-273-OSD, 2017. As of June 22, 2018:
https://www.rand.org/pubs/perspectives/PE273.html

Weinbaum, Cortney, Richard Girven, and Arthur Chan, *Roadmap to Succeed in the Open: For the National Geospatial-Intelligence Agency's Human Development Directorate*, Santa Monica, Calif.: RAND Corporation, TL-251-NGA, 2017. As of June 22, 2018:
https://www.rand.org/pubs/tools/TL251.html

Werner, Debra, "Raytheon Moves into Commercial Imaging Market with DigitalGlobe Camera Order," *Space News*, October 11, 2017. As of June 22, 2018:
http://spacenews.com/raytheon-moves-into-commercial-imaging-market-with-digitalglobe-order/

White House, *National Security Strategy of the United States of America*, Washington, D.C., December 2017. As of June 22, 2018:
https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

Williams, Martyn, "Russia Provides New Internet Connection to North Korea," *38 North*, October 1, 2017. As of June 22, 2018:
http://www.38north.org/2017/10/mwilliams100117/

Woods, Dan, "Do You Suffer from the Data Not Invented Here Syndrome?" *Forbes*, November 15, 2012.

Young, Alex, "Too Much Information," *Harvard International Review*, August 20, 2013.

Acknowledgments

We thank our reviewers, Stephen Cambone, former Under Secretary of Defense for Intelligence, and Andrew Liepman, senior policy analyst at RAND and former Principal Deputy Director of the National Counter Terrorism Center (NCTC), for their thoughtful feedback and guidance.

We thank our colleagues who participated in our workshop and shaped the ideas presented in this Perspective. In alphabetical order:

Stephen J. Flanagan is a senior political scientist at RAND who previously served as Special Assistant to the President and Senior Director for Defense Policy and Strategy at the National Security Council (NSC) and Special Assistant to the President and Senior Director for Central and Eastern Europe at the NSC. He served as associate director and member of the State Department's Policy Planning Staff, National Intelligence Officer for Europe, and as a professional staff member of the Senate Select Committee on Intelligence.

Bradley Knopp is a senior international/defense policy analyst at RAND who served as an intelligence officer at DIA for 33 years, including as the Defense Intelligence Officer for Europe for over 11 years, Assistant Deputy Director for Corporate Operations, Director of the Joint Foreign Materiel Program Office, and DIA Liaison to London.

David Luckey is a senior international/defense researcher at RAND. He previously served as the Director of Homeland Security and Counterterrorism Advisor on the Senate Committee on Homeland Security and Governmental Affairs, and as a professional staff member and head of Audits and Oversight for the Senate Select Committee on Intelligence. He served as the senior policy analyst for the Under Secretary of Defense for Intelligence, and as a senior inspector in the Office of Inspector General in the Office of the Director of National Intelligence after retiring from the Marine Corps.

Heather J. Williams is an associate program director for the Strategy, Policy, and Operations Program in RAND's Homeland Security Operational Analysis Center. She previously served as the National Intelligence Officer for Iran during the final negotiation of the Joint Comprehensive Plan of Action on the Iranian nuclear program. She served on the Foreign Fighter Task Force at CIA's Counterterrorism Center and as a counterterrorism targeter for the Special Operations Intelligence Center.

About the Authors

Cortney Weinbaum is a management scientist at RAND specializing in IC policies, practices, and technologies. She previously served in DIA as a project manager for radio frequency and electromagnetic MASINT collection systems. She has advised intelligence agencies on analytic and collection tradecraft, emerging technologies, and strategic planning, and her research areas include the future of secrecy and the future of the intelligence workforce.

John V. Parachini is a senior international/defense policy researcher at RAND. His research has focused on terrorist attempts to acquire chemical, biological, radiological, and nuclear weapons; how the U.S. government can capture terrorists' digital information; scenario development for counterterrorism planning; and the danger of terrorists and rogue states acquiring nuclear material expertise from the former Soviet Union.

Richard S. Girven is the director of the Cyber and Intelligence Policy Center at RAND. He previously served as the Director of Analysis for the Senate Select Committee on Intelligence. A former career foreign area officer in the Army, he served multiple tours as a defense attaché, and as director of DIA's Afghanistan Intelligence, and chief of DIA's South Asia Office.

Michael H. Decker is the director of Marine Forces Programs within the RAND National Defense Research Institute. He previously served as Assistant to the Secretary of Defense for Intelligence Oversight and Director of Intelligence for the U.S. Marine Corps. He is a former Marine Corps infantry officer and senior intelligence officer.

Richard C. Baffa is a senior international/defense policy researcher at RAND. He previously served as a senior defense intelligence analyst at DIA and U.S. European Command on Middle East, Iran, Russia, and Eurasia regional issues and military issues, and he was the chief analyst at the Army's National Ground Intelligence Center.

Threats to the international order from near-peer competitors and from rogue regimes, terrorists, and the proliferation of cyber weapons and weapons of mass destruction all challenge whether the U.S. Intelligence Community (IC) will be able to fulfill its mission. It is unclear whether the IC is prepared to provide decisionmakers and warfighters with the intelligence they need and expect.

This Perspective presents five distinct discussions of changes the IC can make to meet these challenges in the areas of strategic warning; tasking, collection, processing, exploitation, and dissemination (TCPED); security, counterintelligence, and insider threats; open-source information; and surging for crises.

Each of the five discussions in this Perspective provides analysis and recommendations that may be read, acted on, and implemented alone—but the authors believe that the IC has an opportunity to make a major leap forward by acting in a coordinated manner on all five of the topics together.

$33.00

ISBN-10 1-9774-0115-5
ISBN-13 978-1-9774-0115-1

53300

9 781977 401151

PE-287-OSD