Detect and Understand

Modernizing Intelligence for the Gray Zone

By Jake Harrington and Riley McCabe

All err the more dangerously, as they each follow a truth. Their fault is not in following a falsehood, but in not following another truth.
— BLAISE PASCAL

THE ISSUE

In the gray zone—the contested space between routine statecraft and conventional warfare—uncertainty permeates decisionmaking. Seeking to avoid escalation, aggressors design gray zone activities to evade detection or to frustrate intelligence efforts to attribute blame, quantify risk, and inform decisive responses. In this security environment, intelligence success will require seamless and simultaneous feedback between efforts to identify malign gray zone activities and to contextualize them within a broader analysis of an actor’s intentions and strategy. This brief’s recommended intelligence reforms—focused on a series of technological, organizational, and cultural advancements—are ultimately intended to accelerate efforts to integrate and synchronize a real-time interaction between detection and understanding of gray zone threats.

Discerning knowable truths amid obfuscation, misdirection, and outright lies is a fundamental mission of intelligence. Former Central Intelligence Agency (CIA) director Allen Dulles held this notion so deeply that he insisted that a biblical exhortation to pursue the truth be carved in stone in the CIA’s lobby. Unfortunately, the challenge—as Pascal mused 300 years prior to the construction of the CIA’s Original Headquarters Building—is that global politics are conducted in a world riven with multiple “truths.” This was a constant of the Cold War, when competing narratives informed an era of great power competition. And the same is true today, when interstate competition once again defines a security landscape muddled by ambiguity, confusion, and deception. There is a rich body of literature describing how the modern era of competition will be dominated by actors advancing their interests via malign activities in the so-called “gray zone” between peace and war. These studies have analyzed the specific ways that actors such as China, Russia, Iran, and others operate below the threshold of conventional war and mix political, economic, information, and military tools to increase their global legitimacy and advance their interests at the expense of the United States and its allies. Since the height of the Cold War, the fields of coercion, bargaining, and deterrence have studied why actors pursue these strategies; namely it is to achieve limited goals without incurring the risk of escalation into a costly and potentially devastating war.

This study extends the existing body of research on the gray zone further into the specific areas of intelligence collection and analysis. It offers a range of recommendations to improve the ability of U.S.
intelligence services to confront the gray zone challenges of modern interstate security competition. In support of this effort, CSIS researchers undertook a six-month project that set out to answer the following three questions:

- How do gray zone threats challenge the ability of intelligence planners, collectors, and analysts to deliver timely and accurate analysis and warning?
- How can emerging technologies augment the detection and analysis of gray zone activity?
- What changes across the areas of collection, analysis, and organizational structure could improve the U.S. intelligence community’s (IC) ability to identify, assess, and warn of threats in the gray zone?

To answer these questions, CSIS interviewed dozens of government, academic, and technology experts in the United States and the United Kingdom, conducted a robust literature review, and convened an expert workshop in September 2021 to review preliminary recommendations and further explore the overarching research questions. The research team extends its most sincere thanks to the individuals who contributed to this work. This brief’s recommendations to advance intelligence in the gray zone are a testament to their expertise and insights.

The findings and recommendations generated during this project coalesced around the dynamic between two fundamental intelligence functions, which this brief refers to as “detect” and “understand.” Intelligence success in the gray zone requires seamless and simultaneous feedback between efforts to identify malign gray zone activities (detect) and to contextualize them within a broader analysis of an actor’s intentions and strategy (understand). This brief’s recommended intelligence reforms—focused on a series of technological, cultural, and organizational modernizations—are ultimately intended to accelerate efforts to integrate and synchronize a real-time interaction between detection and understanding of gray zone threats.

The first section of this brief articulates how these pillars of the intelligence mission, which will not change in the gray zone, are being uniquely stressed today. In response to these challenges, the second section then introduces a series of recommendations where the IC can leverage the promises of emerging technology to succeed in the gray zone. This includes building and adopting new platforms to maximize opportunities to exploit increasingly diverse data and expertise, particularly in the rapidly evolving area of open-source intelligence (OSINT). Technology, however, can only serve as an enabler amid broader efforts to modernize intelligence collection and analysis to contend with gray zone challenges. The second section of this brief therefore concludes with additional recommendations to better prepare intelligence officers to process complexity, manage uncertainty, and communicate insights to decisionmakers. While the recommendations included in this brief are directed toward the U.S. IC, the noted challenges and potential solutions are applicable to other intelligence services, particularly members of the Five Eyes intelligence alliance.

DEFINING THE GRAY ZONE

Informed by previous works, this brief defines the gray zone as the contested space that lies between routine statecraft and conventional warfare. Importantly, gray zone strategies have two interconnected characteristics: (1) they are intended to shift the balance of power in the aggressor’s favor, and (2) they are designed to pursue this goal by avoiding, blurring, or circumventing redlines and escalation to conventional warfare.

One of the most significant research challenges during this project was the problem of discerning between routine interstate security competition and the subset of competitive activities that comprise the low end of gray zone activity. Ultimately, this study found that, from an intelligence perspective, there is little utility in differentiating between the concepts of “strategic competition” and the “gray zone.” While the gray zone may carry continued importance in broader efforts to assess interstate behavior across the peace-war continuum, intelligence efforts to detect early signs of malign behavior will need to extend into the arena of routine statecraft, since diplomatic, economic, commercial, or other tools are often components of an actor’s broader gray zone strategy.

INTELLIGENCE CHALLENGES IN THE GRAY ZONE

Seeking to avoid escalation, aggressors design gray zone activities to evade detection outright or to frustrate intelligence efforts to attribute blame, quantify risk, and inform decisive responses. Often, gray zone activities will partner age-old techniques, such as influence campaigns, with modern technologies that enable actors to carry out their activities in secret. Likewise, aggressors also pursue
operations that exploit seams where intelligence agencies
do not or cannot look. And even when detected, gray zone
operations intentionally create ambiguity and confusion
to limit the ability of intelligence services to attribute
responsibility, aggregate behavior, and develop a coherent
understanding of an aggressor’s strategy. This section
examines the ways in which intelligence efforts to detect
and understand threats are uniquely challenged in the
gray zone. It also emphasizes how, in the gray zone, these
two efforts cannot be organized as sequential activities but
must be seamlessly and continuously integrated.

THE DETECTION CHALLENGE
Malign activities in the gray zone are often transmitted
via “weak signals.” Weak signals challenge intelligence
efforts because they can materialize under the guise
of normal political, economic, or diplomatic behavior
or because they simply do not register at all, lost in an
oversaturated intelligence environment. Today, the weak
signals challenge is compounded by the growth of global
data. To put the information age in perspective, the past
decade has witnessed global data generation increase more
than 30 times over, and data generation is projected to
double again by 2025. Simply put, the signal-to-noise
ratio is overwhelming intelligence detection capabilities,
a challenge only made greater by adversaries who use
increasingly sophisticated methods to conceal signals
and introduce more noise into the system. Moreover, as
historic analyses of intelligence failure often illuminate,
even effective collection of the right signals does not
always mean they are quickly and accurately recognized
within the noise.

Compounding the signal detection challenge for the IC
is the emergence of many gray zone activities in areas
that have traditionally not been a priority for intelligence
collection or analysis, which this brief refers to as
“unfamiliar signals.” Unfamiliar signals are difficult to
identify because intelligence officers may not know what
they are looking for or, if they do, they may not know what
types of data and collection capture such activity. In the
twenty-first century, increasing attention has rightfully
been directed toward commercial remote sensors, social
media, public records, and cyber forensics as sources of
intelligence information. In the future, the diversity of
potentially valuable data will continue to grow, led by
further development of smart cities, the Internet of Things
(IoT), smartphones, and other edge devices. Likewise,
growing stockpiles of data will increasingly contain
valuable information in the form of digital exhaust—the
data generated as an unintentional byproduct of physical
and digital activities and processes.

The signal-to-noise ratio is overwhelming intelligence detection
capabilities, a challenge only made greater by adversaries who use
increasingly sophisticated methods to conceal signals and introduce more
noise into the system.

Together, weak and unfamiliar signals represent the central
challenge to threat detection efforts in the gray zone.
Obviously, this problem is not a new phenomenon for
intelligence services. Adversaries have always attempted
to conceal malign activities and sought new, asymmetric
methods to advance their strategic interests. Today, however,
technology continues to offer new opportunities for hiders
to obscure their behavior. Conversely, it also delivers some
advantages to those seeking to discover such activities.

OPEN-SOURCE INTELLIGENCE
AND THE GRAY ZONE
The research in support of this brief reaffirmed the
prior work of CSIS and many others regarding the
value of commercial intelligence and other publicly
available information (PAI) to the IC. Notably, CSIS
recommended in January 2021 that the Office of the
Director of National Intelligence (ODNI) undertake
a robust, cross-functional evaluation of the open-
source mission. Effective and mature adoption of
OSINT is essential in the gray zone, where it offers
two primary benefits.

First, OSINT can be a force multiplier. Increasingly
sophisticated commercial OSINT capabilities can
deliver unique insights, either by augmenting
government-owned traditional collection in certain
areas—such as geospatial intelligence—or by
generating new insights through access to public
records, local broadcast media, or other commercial
data. Recent developments suggest there is an
increasing interest within the IC and in Congress to
explore shared commercial-government collection
models, starting in the area of remote sensing.
Second, that OSINT insights are not derived from sensitive sources and methods increases the information's utility in efforts to confront malign adversarial behavior in real time. Narratives are a weapon in the gray zone, and OSINT can deliver the most ready and useable ammunition.

Despite its promises, numerous policy and legal implications will need to be addressed to ensure that the IC embraces OSINT responsibly and in a manner that protects the civil liberties and privacy of U.S. persons. The introduction of comprehensive, actionable recommendations to this specific challenge is outside the scope of this brief, however, it is important to note that OSINT has long been an essential (if often overlooked) aspect of the IC mission. The most significant policy and legal challenges relate to how and when the IC can purchase and exploit bulk commercial data at scale in a way that does not impinge on U.S. constitutional rights or violate conventions such as the European General Data Protection Regulation (GDPR). However, there are a myriad of lower-risk OSINT applications that could be prioritized as more comprehensive policy and legal guidance is developed to govern bulk commercial data. Responsibly embracing OSINT at scale is essential for intelligence success in gray zone, and its development will require close partnership and open dialogue between the executive branch, private sector, Congress, international allies, and the public.

In addition to introducing unprecedented volumes and new sources of data into the intelligence picture, emerging technologies also challenge the traditional role of intelligence services as the premier authority on threat detection. From commercial cloud computing to private satellites, increasingly affordable and accessible technologies are radically eroding nation-state monopolies on information collection in the space, air, sea, ground, and cyber domains. In this environment, intelligence agencies are increasingly challenged to partner with commercial entities that may have unique insights and access to valuable intelligence. At the same time, intelligence agencies must work with commercial partners who possess technologies that can be exploited by adversaries to advance gray zone strategies. In some cases, these two entities—commercial sources of intelligence and targets for gray zone activity—are one and the same. Nowhere is this clearer than on social media platforms, where adversaries both often reveal valuable intelligence and conduct operations to spread disinformation and sow discord. Failure to properly partner with social media and other commercial technology firms will continue to create collection (and in turn detection) gaps as new technologies democratize the generation, collection, and analysis of information.

In contrast to these new technological partnerships, confronting the loss of the monopoly on information and threat detection will require cultural changes within intelligence agencies—a distinct challenge in and of itself. The ability of intelligence agencies to uncover gray zone threats is also challenged by misalignment between the transnational capabilities of modern technologies and long-standing legal delineations of the authorities of various IC components. Designed to protect the civil liberties of U.S. citizens, such legal gaps are today deliberately exploited by sophisticated gray zone operations to avoid detection by U.S. intelligence services. For example, the foreign cyberattacks that made headlines in late 2020 and early 2021 were actually each launched from computers leased in the United States, therefore limiting the legal authority of various IC agencies to monitor and detect the now “domestic” malign activity. Navigating the legal, policy, and civil liberties implications of this challenge and developing actionable solutions to address it is beyond the scope of this project, but it is an issue of continued concern for both intelligence officials and lawmakers.

Failure to properly partner with social media and other commercial technology firms will continue to create collection (and in turn detection) gaps as new technologies democratize the generation, collection, and analysis of information.

Finally, perhaps the most fundamental challenge to detecting gray zone threats is a matter of terminology. As already considered, the term “gray zone” encompasses an exceptionally broad spectrum of activities, ranging from the outright brazen to the indistinguishable. A variety of interchangeable terms are frequently used to characterize these activities, including “irregular warfare,” “hybrid threats,” or simply “strategic competition.” Individual
threat vectors within this broader landscape also suffer from diverse and often inconsistent terminology, most notably in efforts to describe and assess disinformation and covert influence campaigns. Without a clear and consistent vocabulary for describing both the gray zone and the activities conducted within it, efforts to develop collection requirements and comparatively assess activities will be severely limited. To prepare for a modern security environment characterized by blurred lines, clarity could be the ultimate intelligence asset.

THE UNDERSTANDING CHALLENGE
Gray zone strategies are designed to frustrate efforts to clearly understand the true nature of threats. Even when a threat has been detected, attribution—both in identifying the responsible actor and articulating the degree of danger posed by the activity—is often accompanied by varying levels of uncertainty. Uncertainty becomes a particularly acute challenge on the low end of the gray zone spectrum, where attribution with any level of certainty may be difficult or even impossible. For example, during the 2020 U.S. presidential election, Russia employed actors in Nigeria and Ghana to sow political discord on social media. Such an approach illustrates the multifaceted challenge of attribution, as Russia leveraged multiple cut-outs and proxies to advance this one specific activity within a broader campaign of election interference. On the high end of the gray zone spectrum, attribution may be easier, but initial confusion and uncertainty can last long enough to undermine potential response options. When “little green men” led the Russian annexation of Crimea in 2014, confusion surrounding events on the ground provided enough cover for the Kremlin to achieve its goals fait accompli. Moreover, because gray zone activities are designed to obscure the actors involved, a known activity may only be understood as a threat when extra effort has been expended on attribution.

In addition to attribution, intelligence understanding in the gray zone requires proper aggregation of diverse, multidomain activities. This is particularly challenging in the hazy domains of economic influence, information operations, and other political, diplomatic, or commercial activities that defy easy categorization or clear connection to a known campaign of malign behavior. In some cases, the connection to malign behavior can only be understood in retrospect, when it becomes apparent that certain activities previously understood as routine were early steps in shaping later gray zone activity. If the gray zone is an arena for actors to employ “salami tactics” to gradually achieve their ends, efforts to understand them grow increasingly complex the thinner the salami is sliced.

Aggregation is also necessary in situations where gray zone activity is knowingly malign. For example, Russian strategy today is a laboratory for gray zone techniques. From its annexation of Crimea in 2014 to its influence and cyber operations during the 2016 and 2020 U.S. presidential elections to its use of private military companies in Africa today, Russia expertly exploits the gray zone to maintain plausible deniability and successfully deter responses.

To view these Russian activities in isolation is both a natural inclination for analysis and a deeply harmful one. This approach is supported by conventional metrics that suggest Russia should be a power on the decline. Russia accounts for less than 2 percent of global GDP, its population is both aging and shrinking rapidly, and despite its nuclear arms, Russia’s military is little match for the likes of the United States and the North Atlantic

GRAY ZONE SPECTRUM

Source: CSIS International Security Program.
Treaty Organization (NATO). Nonetheless, successful territorial grabs, the degradation of the social and political fabric of its perceived adversaries, and new economic gains represent quite the opposite of a declining power. In this way, detecting and attributing malign activity is not enough. It is only when gray zone activities are considered in the aggregate that a more accurate understanding of the overall threat emerges.

If the gray zone is an arena for actors to employ “salami tactics” to gradually achieve their ends, efforts to understand them grow increasingly complex the thinner the salami is sliced.

Proper intelligence understanding in the gray zone is necessary for two purposes. For one, it grows the base of knowledge surrounding an adversary’s strategy and decisionmaking. This can facilitate the production of more complex forms of analysis, such as identifying where on the gray zone spectrum an adversary’s actions sit or determining longer-term predictions, risks, and opportunities. Second, an understanding of broader gray zone strategy can be translated into compelling and coherent narratives that can be used to call out and publicly counter an actor’s gray zone strategy.

As a recent memo signed by nine combatant commanders noted, campaigning in the gray zone requires timely and publicly usable facts to cut through the ambiguity and confusion intentionally created by adversaries.

Understanding the gray zone requires timely and accurate detection, but in order to detect, intelligence services must know what to look for and where to look. In this way, detection and understanding are not just cyclical, they must constantly and simultaneously inform one another. They must also remain balanced. Efforts that overemphasize observing indicators over time could lead to a warning failure. Even if detected, by the time a threat is fully understood, an adversary may have already successfully achieved their objective. Conversely, approaches that start with a poorly informed understanding of an adversary’s intentions have their own problems. As others have written, the planning and decisionmaking processes of hostile governments are often opaque. Without sufficient understanding of what an adversary wants to achieve and how they plan to achieve it, detection efforts can descend into an exercise in cherry-picking that does little to advance credible warning. Seamlessly integrating efforts to detect and understand gray zone behavior, and building an effective feedback loop between these lines of effort, is essential.

RECOMMENDATIONS

The following recommendations are intended to accelerate and integrate the intelligence functions of detection and understanding. They progress from tactical-level improvements that expand intelligence access to diverse data, tools, and analysis to broader structural and cultural improvements that rethink how intelligence agencies assess behavior, manage uncertainty, and communicate judgements in support of gray zone policy. Importantly, although technology is central to many of the following recommendations, its effective incorporation will depend on creating the right cultural and organizational conditions that enable the IC’s people to leverage technology as they develop thoughtful strategic analysis.

1. **ODNI should sponsor an IC-wide, collaborative OSINT data catalog.**

   An important step in facilitating broader knowledge sharing and awareness of non-traditional collection opportunities should be the creation of an IC-wide, collaborative OSINT data catalog. Robust cataloging tools that organize and facilitate discovery of an organization’s data accesses and holdings are essential to any data-driven organization. Finding ways to widely distribute knowledge of new, emerging, and unique OSINT data sets could significantly advance efforts to contend with the challenges of weak and unfamiliar signals. ODNI should endorse and sponsor ongoing efforts to improve data curation, discovery, and interoperability and further extend these efforts into the OSINT arena.

   Such a catalog could serve as a centralized warehouse of open-source data sets at the functional, country, regional, and global levels. OSINT information, like all intelligence information, is subject to varying levels of quality, reliability, and timeliness. Historically, analysis of foreign broadcast media outlets—their ownership, structure, relationships with political parties, and other information about objectivity and reliability—has been crucial to the OSINT discipline.

   Expanding similar collaborative and qualitative analysis of data across public records, economic indicators, social media, remote sensors, and other
available OSINT streams can deliver an essential source of knowledge in seeking out data sets that can be used to monitor for indicators of malignant behavior.

The collaborative aspect of this catalog is essential. In conducting this project, CSIS interviewed several experts in data management and analysis. These discussions underscored the importance of continuous reevaluation of data structure, timeliness, reliability, and security, which are each subject to change over time. To illustrate, the availability and utility of public records about business incorporations or economic indicators may vary substantially from one country to another. This is dependent on factors such as a country’s legal requirements, transparency regulations, and the frequency with which such data is made available. If an analyst is monitoring for certain economic indicators across multiple countries, it is essential to understand how such behavior could manifest differently depending on what data is available, where it is generated, how it is captured, and who has access to it. In sum, to be secure and useful, open-source data must be thoroughly and continuously contextualized. This data contextualization can emerge from multiple sources, including forward-deployed, in-country personnel familiar with the host government and culture as well as headquarters analysts responsible for conducting strategic-level analysis.

Ultimately, implementation of this recommendation would help transform the OSINT mission into an IC-wide “team sport.” Unlike other intelligence disciplines or specific lines of collection, no single agency owns OSINT. The information is, by definition, generated and maintained outside of the direct ownership or oversight of any IC entity. Therefore, OSINT is a discipline uniquely suited to catalyze widespread interagency collaboration on how different data can contribute to broader collection and analysis across functional and geographical portfolios.

2. **All IC components should expand efforts to deploy low-code and no-code data analytic capabilities.**

Embracing the need to monitor ever increasing volumes and types of data in search of weak or unfamiliar signals will require advanced machine analytics. Effective adoption of artificial intelligence and machine learning (AI/ML) is already a priority for

---

**Representation of a hypothetical OSINT data catalog with datasets organized into categories and accompanying community-generated analytic perspectives.**

Source: CSIS International Security Program.
the IC, and comprehensive visions for success of this kind have been proposed by CSIS, the National Security Commission on Artificial Intelligence (NSCAI), and the Department of Defense (DOD). One of the most significant ongoing developments in this area is the emergence of low-code and no-code (LC/NC) analytic tools that enable non-technical personnel to create solutions to mission-specific bulk data challenges.

A useful application for LC/NC tools in the gray zone is the development and training of various change detection models that rely on diverse geospatial or other remote sensing data, either monitoring for changes in a single geographic area or a pattern of behavior on a global scale. Autonomy over how these tools are trained to alert users to potential changes in a pattern can allow subject-matter experts more flexibility in determining thresholds and risk tolerances for their specific mission. For example, a model may need to cue when a specified number of sea vessels enter a geofenced area for an established period. Another may be deployed into a specific area of interest to act as a persistent sensor monitoring for certain open-source information, whether it is on broadcast media, social media, or in public records. In some use cases, the risk tolerance will be zero and low threshold alerts will need to be enabled so all responsive hits are carefully reviewed. In other cases, risk tolerances may be higher and alerts only generated when a model has a high degree of confidence. In either case, the real-time ability to adjust these thresholds based on environmental expertise delivers significant benefit and utility to the mission user, regardless of technical prowess.

Importantly, access to these capabilities will reduce the demand on highly skilled but overcommitted computer and data scientists within the IC and simultaneously deliver flexibility to mission teams to develop tools finely tuned to their goals.

3. **ODNI should test and evaluate gray zone behavior-modeling capabilities.**

ODNI, working through the Intelligence Advanced Research Projects Agency (IARPA), should explore options to test and evaluate machine analytic capabilities that can conduct complex forms of pattern and behavior analysis. While traditional change-detection AI/ML models are capable of cuing analysts to changes according to known indicators, more complex behavior models may help discover new patterns of gray zone activity.

Benefiting from deep learning techniques and human oversight, these models can be continuously optimized to survey available data globally for patterns of potentially similar behavior. These modeling approaches are common in the fields of cybersecurity and financial intelligence. For example, algorithms to detect financial fraud are trained to continuously monitor for suspicious financial transactions around the globe and adjust to known or suspected changes in the signatures and techniques of those engaged in illicit finance. Similarly, cybersecurity efforts to develop and train models to detect unknown, undefined zero-day exploits could be expanded into the broader domain of interstate security competition.

4. **ODNI should continue exploring methods to incorporate diverse perspectives into forecasting and warning.**

The IC should reinvigorate efforts to incorporate a broader range of perspectives into forecasting and warning efforts. The U.S. IC has evaluated various geopolitical prediction and forecasting platforms for more than 20 years, according to a recent study on the topic by the University of Pennsylvania. More recently, IARPA explored innovative approaches to forecasting and warning. However, the concept is most mature within the United Kingdom through its platform Cosmic Bazaar, which integrates forecasting predictions from a wide range of government and trusted non-government experts. Despite mixed success in fielding these platforms over the past 20 years, their promise will only grow as the IC’s monopoly on information continues its decline. If there is consensus that OSINT will be a disruptor and an asset in adapting to this era of interstate security competition, the analysis and insights of experts from across and outside of the IC who are conducting unique and innovative exploitation of this data will be essential. As information is democratized, analysis of it must as well.

5. **ODNI should develop uniform gray zone terminology.**

One of the most significant conceptual challenges in the gray zone is a lack of standardized taxonomy of specific categories and types of behaviors. From this issue extend numerous collection, analysis,
and warning problems, as inconsistent approaches to capturing and categorizing gray zone activities undermine efforts to identify, aggregate, and measure such activity against objective, consistent methodology. To strengthen the IC’s ability to detect and understand gray zone activities, ODNI—working through the deputy director of national intelligence for mission integration—should explore options to categorize types of gray zone behavior. Such an effort could align with existing ODNI processes governing the creation of collection and analysis priorities under the National Intelligence Priorities Framework, which could serve as a vehicle for integrating standardized gray zone terminology across all intelligence priorities and requirements.\textsuperscript{34}

A gray zone lingua franca will serve multiple purposes, including guiding what to collect in the gray zone and how to characterize and measure an activity’s threat level. Intelligence agencies then need to build upon this framework and evaluate new techniques to deliver effective intelligence information, judgments, and warning that can minimize the risks of intelligence failure. This proposal carries similarities to the successful development and broad acceptance of the MITRE ATT&CK framework as the standard lexicon for capturing and describing the exceptionally diverse—and continuously evolving—range of computer network intrusion techniques.\textsuperscript{35}

To develop coherent strategy, analytic consistency, and a common jargon between intelligence and policy stakeholders, ODNI should also partner with international allies to promote a common lexicon of gray zone activities across the various domains in which they can emerge. The ability to apply common terminology across actors, regions, and activities would assist technical efforts to develop models that can detect new or unexpected patterns of behavior globally.

Finally, the gray zone is a complex system of systems, where opportunistic adversaries are exploiting vulnerabilities when they arise, learning from each other’s behavior, and constantly adapting techniques in response to detection. As such, efforts to define, categorize, or model gray zone behavior must balance the need to create structure against a constantly evolving field of activity.

**THE IMPERATIVE OF DIGITAL TRANSFORMATION**

Robust analysis of the technology, policy, and cultural challenges facing the IC is reflected in existing work by CSIS, the NSCAI, the U.S. IC, and the DOD.\textsuperscript{36} Core recommendations within these studies frequently include the need to develop policies and architecture to facilitate trusted data sharing, discovery, and interoperability. These are essential preconditions for realizing the promises of emerging technologies. Indeed, achieving intelligence success in the gray zone will be heavily dependent on a broader digital transformation effort across the U.S. national security community.

In early 2021, the DOD issued new guidance in the form of “data decrees” reflecting the principles upon which a more open, collaborative, and data-driven organization could be built.\textsuperscript{37} Success against any type of threat in the information age—including gray zone behavior—requires this transformation. Instead of restating in detail the myriad of thoughtful recommendations that have already been made on the topic of data management and data sharing, this study’s technical proposals build upon the baseline assumption of a need for digital transformation to extend into specific applications of this transformation for gray zone intelligence analysis.

6. **Pilot new constructs that promote intelligence-policy collaboration at lower levels of authority.**

Ultimately, it is the duty of intelligence to deliver timely and accurate insights to decisionmakers who translate that analysis into strategy and policy. Even though these are justifiably separate functions—and retaining distinctions between intelligence and policy remains essential—the process of turning warning into decision is a shared responsibility. As Roberta Wohlstetter observed when dissecting intelligence failures at Pearl Harbor in 1941 and Cuba in 1962, “The problem of warning is inseparable from the problem of decision.”\textsuperscript{38}

Balancing the challenges of managing uncertainty and warning in the gray zone requires new paradigms to facilitate interaction between intelligence officers and policymakers. An important element of this reimagining should be the development of ad hoc working groups comprised
of mid-level intelligence officers and policymakers. These groups should be charged with working through specific and particularly tricky gray zone issues, with a focus on better facilitating that “inseparable” relationship between warning and decision. These working groups could serve as an essential element of broader efforts to understand difficult strategic challenges, enabling the cross-pollination of intelligence information with policy insights in an open, collaborative, and non-competitive environment.

This approach is intended to overcome several of the structural and psychological failings that can occur within existing interagency processes. In particular—as described in exceptional detail by Morton Halperin, Priscilla Clapp, and Arnold Kanter—intelligence agencies have historically sought to avert warning failure, in many cases by predicting crises continually. This “hedging” has tended to erode trust between intelligence and policy over time, particularly because, as Joseph de Rivera wrote, “false leads swamp the information channels” at higher and higher levels of leadership. According to de Rivera, information “filters” in these cases may be at the wrong place in the system and “persons nearer the source of intelligence might be better judges of the accuracy and importance of information.”

Moving more filters into these working groups would enable intelligence officers and policymakers to work through various indications and warning issues below the senior official level. Such an approach could avoid the primary shortcomings that Halperin, Clapp, Kanter, and de Rivera highlighted, namely that opportunities to deliver key intelligence analysis in support of policymaker decisions can be infrequent or subject to bias, resulting in warning fatigue, intelligence failure, or politicization. By delegating discussions about intelligence and policy issues to lower levels, the process of evaluating timeliness and credibility—and setting thresholds for when higher-level warning or policy decisions need to be delivered—can be a shared and more informed decision between intelligence and policy stakeholders.

While this function has significant overlap with the interagency process led by National Security Council (NSC), there is utility in retaining the proposed working groups as informal, potentially leaderless units outside of that traditional construct. In addition to serving as a platform for ad hoc, informal collaboration, these groups will need continuity. Convening them outside of the cyclical reconstitution of an institution such as the NSC can support efforts to continue aggregating and tracking gray zone behaviors over time. The establishment of groups that can sustain efforts across administrations could ameliorate the reality that, in the words of Michael Mazarr, the United States is “constitutionally challenged in its ability to sustain coherent long-term efforts.” Over time, if such approaches prove valuable, they should also be expanded to include close allies and partners.

Finally, it is important to note that these groups should not become dedicated organizational components. Their greatest value is in convening experts from across government who maintain deep subject-matter knowledge and broad insights into how their home agency can contribute to broader efforts to understand and mitigate threats.

**CONCLUSION**

As in any case of institutional modernization, implementing the intelligence reforms proposed in this brief will require the right combination of incentives, training, and leadership to be successful. They are also heavily dependent on successful broader efforts to transform the IC’s technology and culture. This requires, as previous CSIS studies have advocated, the prioritization of continued and urgent efforts to empower and incentivize innovation. It also requires that leaders sustain efforts to recruit, train, and retain diverse, digitally literate intelligence officers who can inject new techniques, perspectives, and expertise into the IC.

Rededicating intelligence agencies to the pursuit of meaning in complexity will be difficult without also making fundamental changes in the ways that intelligence and policy stakeholders broadly interact. Maintaining relevance to policy is one of the age-old dilemmas for intelligence agencies, and current intelligence has long been the primary mechanism through which the IC communicates with policymakers. However, as a recent MITRE study noted, “Today’s current intelligence is neither current nor of sufficient quality to support its intended purpose.” Writing as far back as 2005, Gregory Treverton caricatured the President’s Daily Brief (PDB) as “CNN plus secrets” and lamented that biases toward current intelligence drove the IC toward an emphasis on “reporting” rather than “in-depth analysis.”
The long-standing emphasis on current intelligence has normalized an expectation that indicators, tracked and collated over time, can be analyzed, packaged, and delivered as warning. However, as Cynthia Grabo wrote in her book *Anticipating Surprise*, “Warning does not emerge from a compilation of facts.”

Capturing the nuance of gray zone threats in particular requires a shift in intelligence toward more complex, long-term, and strategic-level analysis. That is not to suggest policymakers should be deprived of current intelligence. On the contrary, as the IC assesses the numerous ways that emerging technologies and commercial intelligence can advance its mission, the area of current intelligence is one of the most promising. Machine learning capabilities powered by natural language processing carry the potential to conduct low-risk tasks, such as combing through open-source and classified information and compiling situation reports for executive readers to remain informed during crises. Indeed, intelligence officers less consumed by such efforts to compete with the news cycle can dedicate more time to the complex analysis policymakers need.

Approaching its 50th birthday, Grabo’s book remains prescient about the fundamentals of the intelligence discipline, but it was framed in the context of a world very different from today’s. Similar thinking needs to be dedicated to adapting the traditional “hard” intelligence disciplines for the digital age. In particular, the IC must be prepared to manage and effectively communicate the complexity of modern denial and deception. As the National Intelligence Council recently highlighted in its quadrennial Global Trends report, the IC will need to navigate a world where denial, deception, and disinformation is “fueled by AI, synthetic data, and deep fakes.”

When recently asked to opine on the biggest threat in this era of gray zone conflict, British chief of defense staff General Sir Nick Carter was blunt: “Miscalculation.” In the modern gray zone, uncertainty permeates decisionmaking and the stakes can be incredibly high. The development and implementation of appropriate and effective strategies to confront malign behavior amid deep uncertainty and with constant risk of miscalculation and escalation will heavily depend on modernizing the ways that intelligence is collected, analyzed, and delivered to decisionmakers.

*Jake Harrington* is an intelligence fellow with the International Security Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C. *Riley McCabe* is a research assistant with the CSIS International Security Program.

This brief is made possible by support from Thomson Reuters Special Services.

**CSIS BRIEFS** are produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s). © 2021 by the Center for Strategic and International Studies. All rights reserved.

Cover Photo: Sean Gallup/Getty Images; Park Young-Chul/AFP/Getty Images
ENDNOTES


2 Ibid.


8 Lindsey Sheppard and Matthew Conklin, “Warning for the Gray Zone,” in Hicks et al., *By Other Means Part II*, https://www.csis.org/analysis/warning-gray-zone.


12 Katz, *Maintaining the Intelligence Edge*.


