BY OTHER MEANS
PART II: U.S. PRIORITIES IN THE GRAY ZONE

Warning for the Gray Zone
by Lindsey Sheppard and Matthew Conklin

Identifying and assessing the true nature of gray zone threats is intrinsically the intelligence mission, guided by the policy priorities set at the national level.1 Gray zone campaigns are challenging given that warning requires detection of a weak signal through global noise and across threat vectors and regional boundaries. Such activity exists below the threshold of armed conflict but within the bounds of competition, obscuring intent, capability, and impact. Gray zone activity is most effective when malign activity is executed within legal boundaries so as not to set off any alarms or cross traditional warning trigger points, further weakening the signal.2 Thus, warning in the gray zone means identifying and assessing new patterns throughout new sources of data.

This paper will discuss how intelligence, and particularly geospatial intelligence, can be collected, analyzed, and applied to better identify and enable the United States to anticipate and respond to gray zone challenges. It details past examples in which the United States effectively applied tools to monitor and respond to gray zone challenges. Key examples highlighted include China’s reef dredging in the South China Sea and Russia’s use of non-uniformed combatants in Ukraine. Interviews with representatives from the private sector, government agencies, and nonprofit organizations contextualize these examples.

Attributes of Warning

The need to assess the threat and proactively compete in the gray zone shapes how, when, and where a tool or set of tools is used. That is, providing mission value is the core guiding principle in adapting the concept of warning, policy, and intelligence processes to drive an actionable product. However, the type of information needed for gray zone warning is often different from traditional concepts of warning. Many warning problems are often tied to the use of force. When the order of battle is known, such as intent indicated by force mobilization in armed conflict, warning indicators provide a path to an expected future state or outcome. While uncertainty and questions of confidence have always been a staple of warnings and indicators, competing in the gray zone brings a new “order of battle” through competition in political, economic, energy, cyber, space, and information domains. As the United States increasingly finds itself confronting foreign threats in each of these spaces, policymakers will need to define new red lines, trigger points, and timelines. Critically, political and military leaders will need to sort through unprecedented amounts of intelligence to determine how to counter gray zone activities. As intelligence scholar Aaron Brantly describes, “Virtually every form of Technical Intelligence from SIGINT, MASINT, and IMINT (now GEOINT) to include the emerging fields of CYBINT and SOCINT (Social Media Intelligence) are expanding at near exponential rates. The signal to noise ratio within this data is very low, and vast collections of data make analysis extremely difficult.”

The overarching challenge finding the signal through the noise is posed by three interconnected gray zone elements: temporality, attribution, and intent. First, gray zone threats are temporal in nature. The nature of gray zone threats truly requires a “big picture view” over long timescales and across regions and functional topics. Identifying gray zone activity involves pattern identification. On their own, individual events are difficult to distinguish from one-off actions, statecraft, or diplomacy. This means that classifying an aggressive activity as gray zone is dependent on and informed by the analysis of aggregated data over a specified time period. For example, a seemingly routine diplomatic visit by a Russian official to a European capital might not be enough to raise suspicion about Russia’s potentially malign interests in the country. Yet, if that instance of diplomatic activity is part of a larger trend or is the first visit of a broader pattern of future visits with similar characteristics, such as coercive economic dealmaking, diplomatic activity could be analyzed as a metric of gray zone behavior. Heather Conley, author of Kremlin Playbook 2: The Enablers, describes how Russia has strategically extended its coercive influence through financial and political networks over the years:

Austria, by cultivating its posture as a space between East and West, has exploited its unique position to make itself a crucial hub for Russian investments in Europe over the past fifteen years. It has attracted the presence and riches of many of the former Soviet Union party and secret service apparatchiks-turned-businessmen. Under the current chancellor, Sebastian Kurz, the Austrian government has protected and grown its economic relationship with Moscow.
The temporality of gray zone threats requires the synthesis of observation with contextual understanding early in the identification and assessment process. Even rapidly advancing techniques, such as machine learning, are not well tailored to produce the necessary insight from time series data without the contextual knowledge and awareness of a human analyst. While machine learning may find the otherwise impossible to find insights and patterns, the human must make sense of whether that is a fair pattern worth exploration. However, given the dual needs of temporal assessment, the promise of geospatial analysis is rooted in the “signal over time” nature of consistent earth observation. Earth observation provides one mechanism for addressing the time series element of certain activities to normalize variance by sampling a target area or region over time that may then be enriched with other sources of information. Capturing the temporal nature of gray zone activities provides one means to build a clearer picture around attribution and intent once HUMINT or SIGINT have directed the target region for observation. We will discuss in later sections how the availability and sophistication of commercial geospatial capability provides a means for addressing the need for high-quality imagery to assist the intelligence analysis process.

Second, attribution of an activity to an actor serves both to enable policy and operational decisions as well as public attribution. In support of policy and operational decisions, attribution often comes at a cost. Requiring an “almost certain(ly)” or “nearly certain” analytic assessment before acting costs time and analytic effort. The cost of attribution for both policy and public purposes is heightened by the fact that much of the data needed to inform historical pattern analyses of large quantities of cyber-related information is owned by private companies.

Further, while direct observation enables attribution, direct observation of gray zone activity rarely occurs. Consider the example of Russia’s unidentified “little green men” in Crimea. While it was possible for analysts to infer from local commentary and on-the-ground reporting that the soldiers without insignia were Russian special forces, the judgment that Russia was covertly intervening in Ukraine involved contextualizing the presence of “little green men” within a larger trend pattern of Russia’s strategic behavior. However, while the intelligence community has become much better at attribution to inform policy decisionmakers of gray zone activities, making that attribution public is not the sole mechanism to deter adversaries that use gray zone tools. As mentioned in the 2019 Worldwide Threat Assessment, the growing commercial availability of advanced cyber capabilities contributes to the noise of unattributed cyber activities in which ambiguous gray zone behavior thrives.

In some cases, the investment in human and technological resources needed to reach a confident claim of attribution can be prohibitive. Denied or restricted areas may entirely prevent direct observation by civilian or military personnel. Different units across the interagency maintain varying standards about the level of certainty needed to attribute gray zone activity to a foreign state. Across interagency units, the perception that 95 to 99 percent certainty in attribution is needed to authorize a U.S. response suggests an unrealistically high standard, especially in the dynamic and ambiguous context of the gray zone environment. Lessons learned from high conflict scenarios indicate that a lower threshold such as 80 percent certainty could be a suitable baseline for gray zone attribution. According to the ODNI: “No simple technical process or automated solution for determining responsibility for cyber operations exists. The painstaking work in many cases requires weeks or months of analyzing intelligence and forensics to assess culpability.”

Public attribution may not be worthwhile in every instance, and more efficient mechanisms may be needed to ensure an agile response while also pursuing approaches that allow for direct observation sooner. For example, although the Federal Bureau of Investigation (FBI) continues to release cyber advisory warnings to industry partners that attribute malign activity to North Korean cyber agents, the advisories state that such attribution is unlikely to deter future cyber operations. “In conceding that attribution will not change North Korea’s calculus in cyber space,” writes Sean Lyngaas, “the FBI is reiterating what is widely recognized in the cybersecurity industry: that Kim Jong Un’s regime is too brazen to care about being called out for its hacking.”

Third, the challenges associated with temporality and attribution directly influence the judgment of adver-
sarial intent to conduct gray zone activity. Indeed, the purpose of countering gray zone threats is to deter an adversary from fulfilling its intent to act. Yet, making a determination about actor intent is a purely retrospective assessment based on the collective analysis of various indicators. While attribution is one piece of the puzzle, closing the space around intent often means synthesizing multiple relevant indicators and warnings, including the state’s geopolitical ambitions, military ties, trade and investment, level of corruption, and media landscape, among others.

The process of characterizing adversarial intent is illustrated in the case of China’s reef dredging in the South China Sea, where geospatial imagery revealed that Chinese vessels were building islands in contested waters. Publication of these findings brought pressure on the Chinese government to respond to international questions. Consequently, China’s official statement in response was widely interpreted as evidence of the government’s expansionary ambitions. This response is an example of the U.S. reliance on “naming and shaming” adversaries that use gray zone tools as a deterrence technique. It is important to note that the applicability of the traditional indicators and warning metrics depends on the local environment. For example, among some military analysts, indicators and warnings are thought to be less applicable to maritime gray zone activity. Instead, qualitative measures may be more useful for policymakers in the maritime domain. According to intelligence studies scholar James Wirtz, one such example would be the observable effects generated by a military’s decision to mobilize forces on a large scale. “The movement of forces from a day alert to a generated alert status,” Wirtz writes, “often creates a string of observable actions that can be detected by the collection efforts of oppositional intelligence agencies.”

As two notable examples of gray zone activity, China’s reef dredging in the South China Sea and Russia’s military intervention in Crimea highlight the various challenges inherent in the three themes of temporality, attribution, and intent. Chinese and Russian objectives and execution differed in these cases, but their tactics—leveraging ambiguity to delay response and ensuring that their activities fall short of direct conflict with the United States or regional countries—are largely the same, underlining the presence of a persistent dilemma for U.S. policymakers and operators.

Cyber Attribution

The weak signal nature of gray zone activity presents challenges for attribution. As an example, the 2018 Office of the Director of National Intelligence (ODNI) Guide to Cyber Attribution addresses the difficulties of (cyber) attribution for policy and operational purposes:

Establishing attribution for cyber operations is difficult but not impossible. No simple technical process or automated solution for determining responsibility for cyber operations exists. The painstaking work in many cases requires weeks or months of analyzing intelligence and forensics to assess culpability. In some instances, the [intelligence community] can establish cyber attribution within hours of an incident, but the accuracy and confidence of the attribution will vary depending on available data.

The ODNI report goes on to say: “The three primary indicators are tradecraft, infrastructure, malware, and intent. We also rely on indicators from external sources, such as open-source reports from the private cybersecurity firms.” Nonetheless, when the government does decide to publicly attribute a cyberattack to a foreign power, there is little evidence that denouncing a country that uses gray zone tactics will achieve the desired deterrent effect.
Challenges and Constraints
Adapting to the challenges of gray zone warning requires addressing constraints within both policy and intelligence processes. The constantly shifting and ambiguous nature of gray zone threats exposes vulnerabilities in the U.S. toolkit. For example, the applicability of geospatial data to predicting emerging gray zone threats assumes that geospatial imagery of the specific region is strategically important to the gray zone mission. In other words, for the United States to excel in the gray zone, it must first know what it is looking for. It is therefore crucial for defense and foreign policy practitioners to apply a shared analytical framework—or common threat picture—to identify, analyze, and respond to gray zone threats. However, process flow, lack of communication, unclear policy direction, and structural silos are barriers to cohesive interagency coordination and shared threat assessments and priorities.

Policy Challenges and Constraints
Through gray zone activities, actors seek to gradually change the competition environment. This incremental approach to competition often resembles the “boiling frog” fable, resulting in the United States acclimatizing to a new normal. This poses challenges to warning over long-simmering timeframes and across sectoral boundaries. When addressing gradual or incremental changes in the competition environment, the United States often confronts competing priorities in near-term gains versus long-term strategy goals or threats within a political structure that favors the near-term. Particularly when legal boundaries are not clearly violated, discerning the true nature of gray zone activity as well as the appropriate response similarly puts the near-term and long-term at odds, while also crossing public-private and foreign and domestic policy boundaries. Economic gray zone activity by China demonstrates the challenges of resolving near-term priorities with the recognition of a long-term campaign; addressing Chinese intellectual property theft, the Belt and Road Initiative, and growing dominance in the telecommunication market risks upsetting the balance of trade and other existing relations. When responses are undertaken, a gap exists in policy and process between U.S. strategic intent to compete in the gray zone—as articulated through the National Security Strategy and the National Defense Strategy—and the plans, tasks, and activities that various U.S. government organizations are undertaking. As a result, U.S. efforts may be uncoordinated and stove-piped and may miss opportunities to be proactive. The result is unclear prioritization and resource allocation for driving intelligence prioritization, collection, and analysis.

While timely and meaningful analysis of gray zone activities means the intelligence community must utilize new sources and methods, the process of addressing these collection needs can be accelerated when there is a clear policy priority. Problem prioritization can be a strong driver of maturing analytic methods. In the absence of clear policy prioritization along the chain of command, however, elements across the interagency tend to remain in their familiar context and problem-specific domain. While the post-9/11 dominance of the counterterrorism mission incentivized interagency units to justify their relevance in terms of combating terrorism, the centrality of a single mission highlights the need for leadership at the management level of the national security enterprise. While the counterterrorism mission was elevated to functional management to address similar challenges, for instance, it is at present less clear how agencies should compete in the gray zone.

Intelligence Process Challenges and Constraints
Gray zone campaigns challenge the intelligence community’s organizational structure as well as tried and true processes. Effectively addressing the gray zone through the intelligence process necessitates adapting the existing practices and processes to the nature of the activity. New data requires new sources, methods, and collection. Evidence of gray zone campaigns often exists in open-source environments or within the private sector. Particularly in the case of economic warfare, the intelligence community is not well positioned to assess activity. The collection infrastructure built up during the Cold War, designed to siphon state secrets over decades, is ill-suited to provide similar value in the economic gray zone.

Regardless of gray zone activity type, addressing the three gray zone warning elements—temporality, attribution, and intent—requires data visualization, the fusing of multiple sources, and mechanisms to make a reasonable judgement in uncertain circumstances. No single intelligence method, source, or analytic package may completely solve this puzzle—each is one tool in the toolbox, the suite needed to provide mission value. The modality of the indicators inherently impacts the efficacy and applicability of a toolkit. For example, while geospatial data may provide a means for assessing indicators with geographic and time-based significance,
it requires other means to incorporate the relevant cultural context. Without tailoring the tools and process to the nature of the threat, a generic toolkit is otherwise applied blindly. For cyber and related technical analysis in particular, it is easy to overemphasize a tool’s technological capabilities at the expense of the user’s relevant cultural knowledge. When making analytical inferences based on satellite imagery, it may be critical to incorporate local cultural knowledge about the geography under examination.

Further, the guiding process itself must evolve around the sources, methods, and analytic techniques. Like the gray zone threat, the process must similarly be dynamic. It must be flexible, adaptable, and iterative, and it should continuously experiment, test boundaries, and incorporate lessons learned to achieve outcomes. Process and analysis must reach across single threat vectors to look holistically across functional areas, technologies, and regions to surface the emergent issues to inform and shift resources. Moreover, for analysts to evaluate whether an activity under observation does in fact constitute gray zone behavior, they rely on an established set of classification types (e.g., people, activities, and traits) that correspond with collection and analytic priorities detailed in strategic documents like the National Intelligence Priorities Framework.

Unfortunately, long-established processes are not sufficiently elastic to adapt to the different kinds of data and information. Collection emphasizes tried and true sources and methods, but misses shifts toward open-source commercial research, development, and innovation. To be sure, radar engineers or nuclear scientists still have access to important state secrets. However, capability is increasingly built in the open through publicly available data sets, algorithms, and software. Further, the editorial structure of analysis may be well-suited for explaining the political behaviors of an individual or country, but it is not well-suited to conveying or exploiting rapid computational advances requiring a technical background—a significant constraint in the Information Age. The process to review and elevate analytic products may rely on regional silos, generic language for a broad audience, and a management structure unfamiliar and uneasy with technical terms and concepts. For example, an analytic product assessing Chinese economic activity in telecommunications and semiconductors crosses regional boundaries and requires an understanding of next generation telecommunication infrastructure, a complex technical topic. Restricting analysis to one region and excluding the engineering nuance to increase accessibility to a general audience paints only one part of the larger, richer picture required to bring the gray zone campaign into focus.

Further, it may be difficult for GEOINT or SIGINT analysts to know what they are observing is a priority—or more importantly if it might be salient to an incipient gray zone threat—because the analysts detecting change on the ground are not always privy to the higher-level discussions between the Director of National Intelligence, Defense Intelligence Agency (DIA), or the Central Intelligence Agency (CIA) that establish collection and analytic priorities. This challenge relates to the inherent obstacle of collection lag time in the intelligence cycle. If analysts do not have the assets they need, analysts need the ability to take initiative in thinking what relevant assets and resources could assist their mission and how to obtain them. In light of this, it is important for analysts to know what they are looking for if the United States is to mount a credible response to gray zone threats and to be able to fuse intelligence across sectors and agencies.

Global Trends Constraining Gray Zone Warning

The increasing utility of competition below the threshold of armed conflict is amplified by global technology trends. The globalization of priority technology means that adversaries, allies, and partners alike have easy access to highly capable, relatively affordable technology. While the United States strives to maintain a persistent technological advantage, other states are building more robust and diverse technology portfolios. While learning to adapt to the threat posed by gray zone adversaries, the United States must simultaneously strive to keep its lead on research and development and, perhaps most importantly, deployment. The agility of gray zone threats requires a response that operates and evolves on similar time scales. Technology trends directly affect gray zone warning, as warning also requires new sources of data and new methods to find timely and meaningful indicators. For example, the steady forward march of fifth generation (5G) wireless and the Internet of Things has strategic competitors facing off in regulatory and standards-setting bodies while free market economies contend with aggressive semi-state-backed corporations. As nations exert influence in regulatory bodies, assessing the electromagnetic spectrum needs of wireless devices with spectrum allocation may reveal intent and expect-
ed capability in a future with ubiquitous internet. In this instance, the gray zone signal is found through analysis of highly technical yet open source standards.

Meanwhile, further complicating a credible U.S. response is the varying degrees to which allies and partners perceive foreign adversaries as posing a gray zone threat. Actors and effects are entangled in economic and political structures, posing difficulties in identifying problems. For example, variance across ally and partner perceptions of Russia’s gray zone activities or the transregional nature of Chinese economic coercion may impede a unified effort to track gray zone actions. Further, there is a growing uncertainty among foreign policy commentators about the degree to which future interrelated gray zone responses will be possible due to disparities in common understanding of threatening activity and lack of strong national narratives on gray zone challenges.

Finally, distrust between the private and public sector can undermine cooperation on gray zone warnings. Collaboration with the private sector requires rebuilding relationships between a national security enterprise and privately-sector innovation base that are deeply skeptical of one another. Positive engagement is critical to counteracting the damage from leaks and opaqueness of activity. For those entities actively willing to support the national security mission, coordination through non-traditional contracting mechanisms and active investment in application provides the necessary support to private-sector firms. However, active cooperation between public and private actors also requires highlighting the risks now facing many companies in the global economic and security environments. While early 2019 exposed questionable applications of facial recognition technology in China, it similarly brought to light the dangers facing U.S.-based entities who wish to conduct research and business in China. Microsoft Research Asia, a Beijing-based Microsoft research organization, faced scrutiny in April 2019 on its decision to partner with a Chinese military-run university for research in artificial intelligence (AI) that could further human rights abuses of the ethnic minority Uighur population in Xinjiang. Further, awareness of alleged sanctions violations by Huawei Technologies and ZTE Corp led the Massachusetts Institute of Technology to sever ties with the Chinese-based telecommunications firms.

**Framework for Gray Zone Warning**

The reality is that not every question worth answering has unlimited resources, and the fidelity of information is not consistent across all regions or functional areas. The availability of quality open-source information provides an opportunity to build products and analysis prior to problem prioritization. As the value and availability of information has increased significantly, observation, attribution, and intent increasingly may be based on open-source information. In fact, commercially available open-source satellite imagery has provided an avenue for identifying and assessing gray zone campaigns and then aligning national resources to refine the understanding of events, attribution, and intent.

One key criterion for gray zone warning frameworks is to integrate disparate sources of information into a cohesive, actionable product. Data visualization combining various sources of such information allows for the understanding of broad sets of activity on an ongoing basis to support a reasoned assessment. Data analytics and visualization evolved alongside the counterterrorism mission throughout U.S. involvement in the Middle East following the events of September 11, 2001. While analysts early in the conflicts cobbled together their own interfaces and visualizations to layer the necessary information, the mission value drove the creation of various data integration and visualization platforms. Geospatial analysis is in similar early stages. Satellite imagery of North Korea’s nuclear test sites and previously undisclosed missile locations has brought GEOINT front and center to mainstream audiences. Open-source geospatial information combined with additional sources provides an accessible mechanism to close the space around attribution and intent of adversary actions in the gray zone. According to a recent annual assessment of the GEOINT community:

“The consumption of GEOINT data, products, and services should be self-service, because all produced intelligence, along with the source information that went into it, can be found on the platform. Operators would not need to wait for the finished report; they could just pull the raw information from the platform and filter for available GEOINT analytic reports.”

Through a common information-integrated picture, all actors—ranging from multiple interagency entities to various U.S. allies and partners—could be on the same page before initiating both defensive and offensive gray zone approaches. Quickly integrated and widely-shared information enabled one of the most effective responses to gray zone action to date: the multinational response
by Western governments to the March 2018 Skripal poisoning attacks.\textsuperscript{26} Usefully, U.S. Southern Command is sharing best practices with other combatant commands on how it leverages analytic toolkits like the Joint Improvised Threat Defeat Organization’s VOLTRON suite to identify, monitor, and evaluate threats in their area of operations.\textsuperscript{27}

Information integration tools provide an advantage to analysts with their capacity to make sense of seemingly disparate data points. Information integration and data visualization tools are especially effective ways to differentiate the signal from the noise in complex, unfamiliar spaces conducive to gray zone activity. For example, in the domain of economic coercion, flows of foreign capital, particularly those from state-backed corporations, could be used to infer the science and technology priorities of strategic competitors investing in firms abroad. Identifying which companies are offered even seemingly small investments from state-affiliated entities is a nontrivial signal of the state’s strategic interests. Recently, researchers published an impressive online transparency platform that exemplifies the potential for open-source research to complement the government intelligence process. “Mapping China’s Tech Giants,” an initiative of the Australian Strategic Policy Institute, tracks the global expansion of 12 Chinese technology companies. The interactive map features an extensive database of information documenting China’s involvement in overseas 5G networks, smart cities, and university and research partnerships. Through bringing together disparate sources of information to reach a judgement of intent, the report’s authors conclude that Chinese internet and technology companies are not exclusively commercial actors, due to the public-private ties with the Chinese Communist Party.\textsuperscript{28}

Data integration tools help analysts understand who and what matters most to a gray zone operation area and why. For example, several years’ worth of satellite imagery could help determine the health of local crops. Combining imagery analysis with HUMINT cultural knowledge of interpersonal connections could be visualized through lines of relation between people, activities, and economic information. These models could allow policymakers to conceptualize connections that were otherwise not readily apparent. The point is that combining HUMINT with GEOINT and SIGINT for a geographic area would assist the analyst and local operations in understanding a particular gray zone context. A second key criteria of a gray zone warning framework is a feedback mechanism to close the action-reaction cycle. Feedback loops adapt to the culture and context of the threat activity. Intelligence observes and assesses; separate organizations execute action. A feedback mechanism allows for the evaluation of how well the response is addressing the threat action and to adjust if necessary. The gray zone threat is by definition adaptable and flexible, meaning feedback is necessary to adapt the response accordingly. Once the product feedback loop is closed, U.S. interagency actors may become more proactive, as opposed to reactive, shifting the mindset from purely defense to driving the cycle through offense. Feedback throughout the action-reaction cycle must also occur within sustained, tailored activity. Information operations demonstrate the necessity of context-specific responses, rather than a “one size fits all” approach. As an example, Russian tactics in Serbia are not equivalent to Russian tactics in Ukraine. While Finland’s highly educated population and centralized whole-of-society defense make it resilient to Russian disinformation, state corruption in Ukraine and Georgia present opportunities for malign disinformation tactics.\textsuperscript{29} Finland, ranked the third-least corrupt country in the world, is also less susceptible to Russian disinformation compared to former Soviet states with large Russian-speaking populations. In other words, a country’s specific social, cultural, and political profile shapes which tactics the aggressor state will employ in the gray zone.\textsuperscript{30} While existing programs are tailored, the process of refining based on the cultural context must be improved. Further, current operations build in doctrinal vulnerability by deemphasizing the sustainment: drop-offs or halts in proactive messaging create an information void that may then be filled by an adversary. Incorporating feedback throughout a counter-disinformation campaign while also using persistent messaging—leveraging the realities of human cognitive biases—has demonstrated results in successfully protecting populations against disinformation.

Finally, effective warning in the gray zone involves active cooperation, between allies and partners as well as public and private actors. The combined response to the Russian attack on the Skripals in the United Kingdom demonstrates the efficacy of collective responses and actions from allies and partners. Best practices have arisen from coordinating responses with allies and partners. Nordic partners on the front lines of Russian influence are well positioned to share toolkits and educate
politicians on countering and preparing their citizens for disinformation campaigns. The December 2018 international condemnation of China’s cyber theft of sensitive information from private companies and foreign governments required multilateral coordination and active cooperation. In cooperation with the U.S. indictment of Chinese hackers, the UK National Cyber Security Centre (NCSC) similarly attributed the illicit cyber activity to an organization affiliated with the Chinese Ministry of State Security. Earlier in 2017, the NCSC collaborated with private-sector companies to identify the Chinese hacker group and provide guidance to companies on how to guard against the cyber threat. Multilateral coordination between governments victimized by China’s intellectual property theft—including U.S. allies such as Germany, Australia, Canada, and Japan—enabled a strong multilateral condemnation by the international community of China’s illicit behavior.

Technology is fast moving, particularly when functionality is based in software, and collaboration with private entities allows for better awareness of and access to outside innovation. In the months following Russia’s 2014 invasion of the Crimea, private-sector researchers demonstrated the potential of using open-source geospatial data from social media to establish the identity and location of Russian soldiers in Ukraine. Bellingcat—a research and investigative journalism organization—and the Atlantic Council Digital Forensics Lab disseminated open-source research on Russia’s intervention in Crimea for public consumption. According to one government agency, collaboration with think tank researchers on projects such as the CSIS Asia Maritime Transparency Initiative represents the type of partnerships that can effectively raise public education about gray zone threats.

Successfully distinguishing the gray zone campaign signal through the global noise requires action through the entirety of the national security community. Adversarial tactics to gradually change the security environment are advantaged by a system that is better suited to clear incursions and violations of boundaries, borders, and laws. Policy, process, and tools must all adapt and evolve to detect, discern, and act upon a new type of signal. The same global technology trends challenging the United States present opportunities to succeed in gray zone competition. Leadership in public- and private-sector research, development, and innovation positions the United States to maintain the persistent technical advantage necessary for gray zone warning.
Endnotes


3 Aaron F. Brantly, “When everything becomes intelligence: machine learning and the connected world,” Intelligence and National Security 33, no. 4 (2018): 566. Regarding the acronyms used in this sentence, they stand for the following: SIGINT (signals intelligence), MASINT (measurement and signature intelligence), IMINT (imagery intelligence), GEOINT (geospatial intelligence), and CYBINT (cyber intelligence). These acronyms are used throughout this paper.


5 “Many of the complex questions fielded by intelligence agencies often reside within sub-populations and outside of easily accessible information sources. It is extremely difficult to capture historical data in the present, whether by survey on what an individual’s perceptions of an event, particular policy, law, practice, or decision were, yet big data is increasingly building a historical repository of data on these perceptions in the form of social media posts, news archives, recorded emails, web-traffic logs and much more. Information captured in stream and stored for later use such as email communications, forums, chat logs, browser histories, and many other types of data can help to inform future analysis when novel questions and their subsequent informed hypotheses are developed.” Brantly, “When everything becomes intelligence.”


7 Ibid.


12 Ibid., p. 2–3; Two additional sections in the ODNI report that are relevant to this discussion are “Best Practices for Determining Attribution” and “Best Practices for Presenting Attribution Analysis.” See ibid., 3–4.


14 “It has become harder for Western countries to spy on places such as China, Iran, and Russia and easier for those countries’ intelligence services to spy on the rest of the world.” Edward Lucas, “The Spycraft Revolution,” Foreign Policy, April 27, 2019, https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/.


16 Policymakers must also be sensitive to the possibility that using public attribution to “name and shame” adversaries may unintentionally lead to negative political backlash. For an EU example, see Michael Peel, Mehreen Khan, and Max Seddon, “EU attack on pro-Kremlin ‘fake news’ takes a hit,” Financial Times, April 2, 2018, https://www.ft.com/content/5ec2a204-3406-11e8-ae84-494103e73f7f.


18 Lyngaas, “FBI to private industry: Attribution won’t deter North Korean hacking.”


Murgia, Madhumita and Yuan Yang, “Microsoft Worked with Chinese Military University on Artificial Intelligence,” *Financial Times*, April 10, 2019, https://www.ft.com/content/9378e7ee-5ae6-11e9-9dde-7aedca0a0b1a.


“The sources of information overload are not singular in nature. Instead they comprise collections from across all major intelligence agencies. The volume of every form of intelligence increased markedly in the post war era and was not confined to SIGINT. Virtually every form of Technical Intelligence from SIGINT, MASINT, and IMINT (now GEOINT) to include the emerging fields of CYBINT and SOCINT (Social Media Intelligence) are expanding at near exponential rates.” Brantly, “When everything becomes intelligence,” 566.


