The Intelligence Posture America Needs in an Age of Great-Power Competition

David R. Shedd

The United States faces an expanded national security landscape of threats that are interconnected by the rise of great-power competition from China, Russia, and their allies. The wide array of these threats to America's security will require our national defense and intelligence posture to adapt to a world that for nearly 20 years has been fixated on defeating international terrorists. For decades following the end of World War II and the onset of the Cold War, America's attention was focused almost entirely on the Soviet threat. Now our intelligence capabilities must be refocused to counter the global challenges to American national security interests from a rising China and an emboldened Russia in order to give decision-makers options for addressing the nefarious activities of these two great powers.

In the decades preceding the collapse of the Soviet Union, America's spies were almost singularly focused on collecting secrets on the USSR and its Communist allies. For the past two decades, however, U.S. intelligence agencies have been dedicated to thwarting international terrorism and supporting two long unconventional wars in Afghanistan and Iraq.

In the 1990s, intelligence capabilities were hollowed out by President Bill Clinton under the false premise of a "peace dividend" from a defeated Soviet Union. That assumption of a safer world proved false in the wake of the September 11, 2001, terrorist attacks. Almost immediately, America's slimmed-down Intelligence Community (IC) shifted its focus from nation-state threats posed by a rising China or a defeated Soviet Union to a new type of adversary. The events of 9/11 demonstrated that nontraditional enemies could do enormous damage to our way of life while expending few resources—either people or funds—in the process. After 9/11, the IC rallied to shift a shrunken resource base—people, secret collection, and analytic capabilities—and spent the next five years rebuilding itself to address the new threat of Islamic radicals.

Following those attacks, President George W. Bush called for a significant increase in resources for the IC, which had been starved by budget and personnel cuts during the 1990s. There was an immediate redirection of intelligence capabilities to confront a new and growing threat from international terrorism and a war in Afghanistan aimed at denying the terrorists a safe haven. The IC acted expeditiously and effectively to undertake the necessary shifts by becoming much more focused on finding terrorists and denying them the ability to plan and execute their attacks. The intelligence officer also moved to serve side-by-side with the warfighter, first in Afghanistan and then in Iraq after the U.S. invasion in 2003.

Obtaining intelligence to warn of, prevent, and respond to the actions of an adversary remains the core business of the IC. Yet America's intelligence agencies remain ill-postured to address the threats posed by China and a

reemergent Russia. These gaps must be closed while the IC continues to address the disruptive capabilities of non-state terrorist groups such as al-Qaida, ISIS, and Hezbollah.

Complicating the landscape, globalization is producing its own national security challenges. Propaganda campaigns to shape people's hearts and minds are but one example of the global nature of these challenges. The disinformation campaigns mounted by state and non-state players promoting unanticipated objectives leverage commercial mass-media outlets, further complicating the process of warning, preventing, and responding. The IC's shortfall in providing anticipatory warning about complex emerging threats is the result of insufficient resources. Even though the IC simply does not have sufficient capability and capacity to deal equally with every threat that America faces, it must adapt to this changing reality.

The 2017 National Security Strategy and the Intelligence Community

President Trump's 2017 National Security Strategy states that our national security requires that the U.S. be able to determine whether and where geostrategic and regional shifts are taking place that will threaten our interests. To that end, the strategy calls on the IC to collect, analyze, and develop options for the decision-maker to address the panorama of threats. Policymakers expect the IC to engage in aggressive collection of strategic-level intelligence that enables the anticipation of geostrategic shifts such as we see currently with China and Russia. At the same time, American intelligence also needs to obtain secret information essential to generating reliable tactical intelligence so that decision-makers can respond effectively to the actions and provocations of our adversaries.

The President recognizes that modernization of U.S. military forces to overmatch America's adversaries requires intelligence support. To have an improved capability, one has to have some idea of the opponent's capability. Moreover, the strategy underscores that "[i]ntelligence 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."[1]

Adversaries like China and Russia are now mastering technology to build up their own capabilities, which in turn are used to undermine U.S. interests at home and abroad. These same adversaries are making significant investments in artificial intelligence (AI) and machine learning (ML) initiatives for processing and analyzing large quantities of data. Knowing specifically what our adversaries are doing requires that the U.S. IC be able to understand their languages in addition to having the expertise to understand the scientific and technical capabilities that they are pursuing. As they did during the Cold War, U.S. spy agencies need to attract and retain deep country and regional subject matter experts with ample foreign language capabilities and professional spies with technical proficiency in order to gain a significantly increased understanding of the intentions of China, Russia, and their allies.

Spy tradecraft—the art of collecting secrets—needs to be adapted to match today's threats. We know, for example, that China is investing vast sums of money in cutting-edge dual-use technologies that will enable the government to track its own citizens. These same technologies are being used to uncover the plans and intentions of China's adversaries including the U.S. A plan backed by Chinese President Xi Jinping illustrates just how critical technology development is to the Chinese government (and the Chinese Communist Party):

> China will invest an estimated $1.4 trillion over six years to 2025, calling on urban governments and private tech giants like Huawei Technologies Co. to lay fifth generation [5G] wireless networks, install cameras and sensors, and develop AI software that will underpin autonomous driving to automated factories and mass surveillance.[2]

Intelligence: What Is It and What Role Does It Play?

In the Intelligence Community, "intelligence" refers to a dynamic set of actions that relies on collection requirements established by the customers of intelligence, sharing the information within the IC so that various types of analysis can be performed, and then disseminating the results of insights to its customers. Former longtime intelligence professional Mark Lowenthal provides a classic definition of intelligence: "[I]ntelligence is the process by which specific types of information important to national security is requested, collected, analyzed, and provided to policymakers."[3] This essay focuses primarily on information as intelligence: that is, the macro-world of ideas, propaganda, and perception and how our adversaries are working to shape public perspectives on the larger strategic competition with the U.S.

From the standpoint of national security or military operations, intelligence needs to provide decision advantage: "Successful intelligence provides advantages to decision-makers they would not otherwise have, so an analyst must know the frame of mind of the decision-maker and the strategy to help the policymaker to succeed."[4] In other words, one obtains a better understanding of the competitor and is able to hide that advantage so that the competitor is unaware that his efforts have been compromised and his secrets discovered.

In his 2019 worldwide threats briefing to the U.S. Congress, then-Director of National Intelligence Daniel Coats described the nature of the emerging new threats:

> The post-World War II international system is coming under increasing strain amid continuing cyber and WMD proliferation threats, competition in space, and regional conflicts. Among the disturbing trends are hostile states and actors' intensifying online efforts to influence and interfere with elections here and abroad and their use of chemical weapons. Terrorism too will continue to be a top threat to US and partner interests worldwide, particularly in Sub-Saharan Africa, the Middle East, South Asia, and Southeast Asia. The development and application of new technologies will introduce both risks and opportunities, and the US economy will be challenged by slower global economic growth and growing threats to US economic competitiveness.[5]

The role of intelligence, whether it is providing information or identifying options for the policymaker or the military commander in the field, is to protect American interests at home and abroad. This is not new. What has changed is that intelligence must now be refocused to cover a more diverse and complex set of national security threats. U.S. intelligence faces expanded threats emerging from cyber warfare, adversarial use of AI and ML, space-based capabilities, and very sophisticated counterintelligence from competitor nations that are able to invest in the most advanced technologies.

The National Intelligence Strategy and the Intelligence Community

The IC published its *National Intelligence Strategy* (NIS) in 2019 to provide its workforce with strategic direction for the next four years. While the NIS does not outline specific priorities (these are kept classified), the strategy asserts that "all IC activities must be responsive to national security priorities." It further specifies that:

> All our activities will be conducted consistent with our guiding principles: We advance our national security, economic strength, and technological superiority by delivering distinctive, timely insights with clarity, objectivity, and independence; we achieve unparalleled access to protected information and exquisite understanding of our adversaries' intentions and capabilities; we maintain global awareness for strategic warning; and we leverage what others do well, adding unique value for the Nation.[6]

These four principles for the intelligence enterprise give the IC's rank and file a clear framework to adjust and identify needed resources to hone in collecting and analyzing the intentions and capabilities of near-peer adversaries.

To fully understand the challenges facing the Intelligence Community as it adapts to new circumstances, it is important to know its composition and how it is resourced. The IC is composed of 17 elements, including the Office of the Director of National Intelligence (ODNI).[7] Of these, eight reside within the Department of Defense (DOD),[8] a fact that underscores the importance of intelligence to America's defense posture and to the warfighter in particular. These elements operate in a federated fashion with each one receiving its own appropriated budget within the National Intelligence Program (NIP). Supplementing the NIP funds is the Military Intelligence Program applicable to some of the DOD-based intelligence elements.

The Director of National Intelligence (DNI), a position established by the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004,[9] is called upon to "lead a unified, coordinated, and effective intelligence effort. In addition, the Director shall…take into account the views of the heads of departments containing an element of the Intelligence Community and the Director of the Central Intelligence Agency" in guiding America's disbursed intelligence personnel and capabilities.[10]

A Tale of Intelligence Transformation: 2001 to the Present

America's spy agencies have evolved since their establishment over an extended period following World War II and during the Cold War with the USSR and its allies. A certain Sovietology discipline matured over the decades. The IC benefited from deep investments in language skills; deep development of expertise on Soviet political, military, and economic developments; and unique spy tradecraft driven by the need to develop, recruit, and handle Soviet and Soviet-bloc spies and ferret out spies working against the U.S. and its allies.

After the USSR collapsed, the U.S. no longer had a clearly defined adversary. This so-called peace dividend, combined with disinvestment in human talent and technical capacity, led in the 1990s to a significant reduction in the nation's intelligence capabilities. Then, when al-Qaeda attacked the homeland in 2001, the Bush Administration directed the IC to shift its focus to countering Islamic terrorism. Soon after the terrorist attacks, President George W. Bush assigned the Director of Central Intelligence, George Tenet, the de facto responsibility to become America's combatant commander for countering international terrorism while also serving as America's top intelligence officer. This informal designation for the DCI underscored the role that intelligence would play for years to come in the war on international terrorism.

The events of 9/11 provided an opportunity both to revitalize our nation's intelligence capabilities and to redirect resources to counter a very different type of adversary compared to the USSR during the Cold War. Acquiring new capabilities was given top priority. These capabilities included recruiting Arab, Farsi, Urdu, and other language proficient personnel, adapting technical collection to pursue geolocational discovery, augmenting tactical collection to identify small terrorist cells, and identifying clandestine Internet communications by Islamic extremists.

To address the redirection and rebuilding of intelligence capabilities in the aftermath of the attacks in 2001 and the ensuing wars in Afghanistan and Iraq:

> [T]otal intelligence spending grew by about 110% from 2001 to 2012. National defense excluding intelligence grew by 55% over that time period…. [W]hen measured from 1980, total intelligence spending by 2012 had grown 274%, while national defense spending without intelligence had grown 82% over that time period.[11]

Even with significant growth in the intelligence budgets, however, a side effect of the rise of counterterrorism as the top priority for America's intelligence agencies was to downgrade collection and analysis with respect to more traditional geopolitical issues around the globe. In effect, countering terrorist organizations became vastly more important than countering competitor countries.

The demand for battlefield-level intelligence increased significantly as American and coalition warfighters went into Afghanistan after late 2001 and after the 2003 invasion of Iraq. Geolocational data to detect the enemy's whereabouts was of paramount importance. Our already limited resources shifted further away from clandestine collection on China and Russia to focus on electronically intercepting terrorist messages, honing imagery collection at the battlefield level, and performing clandestine human intelligence at a more tactical level. The warfighter demanded that strategic-level intelligence collection be fused with field-level tactical collection and analysis to find and destroy the enemy on the ground.

American Intelligence in a Rapidly Changing World

As U.S. intelligence collection and analytical priorities shifted to address Islamic terrorism, those same enemies adapted their operational planning and activities. U.S. cyber-focused operations had to adapt to finding an enemy that was modifying its use of web-based presence to communicate, recruit terrorists, and launch propaganda operations. America's spies were essential to disrupting Islamic terrorists' communications and operational planning.

The buildup of counterterrorist (CT) capabilities is now useful in meeting the intelligence demands associated with today's world. For example, data analytics that was used in CT operations to identify and counter "fake news" now has widespread application in confronting the national security challenges we face from nation-state competitors.

Former National Counterterrorism Center Acting Director Russell Travers has noted that we "will never have enough analysts to process the available information so Artificial Intelligence and Machine Learning are not 'nice to have' they are an imperative." Travers quotes from the interim report of the National Security Commission on Artificial Intelligence:

> With respect to data, the government is well positioned to collect useful information from its worldwide network of sensors. But much of that data is unlabeled, hidden in various silos across disparate networks, or inaccessible to the government… Even more data is simply expelled as "exhaust" because it is not deemed to be immediately relevant.[12]

Travers adds that "[w]e have a long way to go to realize the benefits of Artificial intelligence and machine learning."[13] Data analytic processing that results in usable information for IC analysts will help to expand the range of available sources and in turn facilitate the dissemination of better "indications and warning"[14] to the customer.

Our adversaries, both state and non-state, are resilient and adaptable. They continue to invest in their own capabilities, ranging from cyber-focused operations to advanced weaponry, in order to upend our way of life and that of our allies. Our intelligence agencies must therefore continue their own journey of change—and in some instances transformation—to meet today's more complex national security threats and stay ahead of our adversaries. This includes a reexamination of how intelligence should be managed in a post-9/11 world:

> The U.S. Government must fundamentally reexamine the manner in which the Intelligence Community manages intelligence information. In many instances, the intelligence failures that preceded the terrorist attacks of September 11, 2001 were marked by an insistence—whether historically or legally grounded—that intelligence information must be tightly

controlled by the intelligence collector. Often, this position was based on a mistaken predicate, namely that an agency "owned" information that it had collected.[15]

The reforms in America's intelligence enterprise spurred by 9/11 focused on removing barriers to the sharing of two types of information by U.S. agencies: information collected outside the U.S. and information lawfully obtained inside the U.S. Before September 11, 2001, U.S. law (as it still does) prevented the Intelligence Community from conducting surveillance of U.S. citizens. Once granted legal authority pursuant to an investigation, U.S. law enforcement agencies could surveil citizens, but they could not share that information with the Intelligence Community.

The terrorist attacks of 9/11 showed that there was a gap between these two worlds where dangers inside and outside of the U.S. overlapped to create opportunities for enemies—opportunities about which the federal government was ignorant because of the prohibition on sharing information. The Intelligence Reform and Terrorism Prevention Act of 2004[16] led to improvements that made critical CT information more readily available to those charged with disrupting terrorist plots against the homeland, but better information sharing is still needed.

Designing and directing the nation's intelligence capabilities requires a resilient and committed IC leadership operating with a sense of urgency. America's adversaries are constantly and rapidly adapting their capabilities in cyber operations, social media, and other means of technology. American intelligence must remain focused on improving its own intelligence tool kit and staying ahead of the enemy, but that is not enough. America's intelligence agencies also need to pursue improvements in their business processes so that they not only can deliver better products to the decision-maker in a timelier manner, but also will be able to operate more efficiently and effectively if significant resource constraints reappear.[17]

Despite the IC reforms enacted post-9/11, additional action is needed. Collaboration among the spy agencies needs to improve. There is still a propensity among bureaucracies to avoid sharing information. The reasons for not sharing may include concerns by the agency that collected the information that the sensitive intelligence will be mishandled by other agencies and perhaps even leaked to the media or sourced in such a way that sensitive collection methods are exposed. Notwithstanding significant changes in how the spy agencies work today, the evolving threats to the nation require that the IC and its 17 elements continue to adapt.

One area of adaptation is technology itself. In order to be more effective in driving the integration of innovative technology within American intelligence, the IC must shift its culture mindset that expects any needed new technology to be developed within the community. The IC needs to welcome commercial technology solutions, modifying them as necessary to meet the mission requirements of the intelligence professionals.

The IC leadership should consider how best to shift resources and capabilities as they pertain to the adoption of technical capabilities (AI, ML, etc.) that can be applied to the rise of great-power competition. Oracle Cloud's Adaptable Business research project led to the interesting finding that business efficiency increases by 64 percent when the right technology is implemented alongside seven key cultural factors within an organization—all of which are factors that can be linked to characteristics in today's intelligence enterprise:

1. Flexibility and embracing change,
2. Learning culture,
3. Data-driven decision-making,
4. Open communication and collaboration,
5. Shared digital vision and participative leadership,

6. Entrepreneurial culture, and

7. Critical thinking and open questioning.[18]

According to the research, many organizations have invested in the right technologies but lack the culture, skills, or behaviors necessary to fully reap their benefits. The study found that business efficiency increases by only 27 percent when technology is implemented without the identified seven factors.[19]

America's intelligence professionals, in shifting their attention to the rising security threats posed by China, Russia, and their allies, are well postured to do so in only two out of the seven areas: critical thinking/open questioning and a learning culture. The IC as a whole is reluctant either to embrace open communication and collaboration across its 17 elements or to demonstrate flexibility and embrace change. The intelligence elements also fall short of applying data-driven decision-making at every level, having a shared digital vision, or promoting an entrepreneurial culture. If the Intelligence Community is to meet the challenges of the 21st century, its leaders need to address these shortfalls with a sense of urgency. If implemented, their strong and unwavering direction can offer opportunities to enhance the effectiveness of the IC's workforce.

The pivot of 2001 toward combating Islamic extremism as the top intelligence priority and away from a focused attention on the rise of China and the geopolitical aspirations of Russia has shaped the mindset of today's collectors. For example, for two decades, an entire generation of intelligence operators has not been schooled in how to conduct traditional operations against state actors, much less against our near-peer competitors. As a former CIA human intelligence operator observed in 2017:

> Over the past 15 years, this "global war on terror" mindset has become the default at the CIA. After accusations that it was stuck in the Cold War, the agency began to trade concealment devices and human sources for military hardware. Under a directive from President George W. Bush, it expanded its ranks to fight terror. It bulked up its abilities to track and target a dispersed enemy fighting an asymmetrical war. Gone were the days, it seemed, of risky brush passes in a heart-pounding, adrenaline-filled four-second period when an officer was "black"—meaning free, just for a moment, from hostile surveillance and able to pass a message to an asset. The Cold War was over; we had a new enemy to defeat.[20]

To address the security threats posed by China, Russia, and their allies effectively, our experienced operators and analysts must be reprioritized to meet customers' demands for accurate, relevant, and timely intelligence related to capable adversaries. These adversaries are not only capable of mounting complex operations against the U.S., but also able to detect sophisticated operational activities against them. Reflecting on the challenges posed by a rising power, Secretary of State Mike Pompeo has pointedly characterized the nature of the threats presented by a rising China:

> Under [Premier] Xi Jinping, the [Chinese Communist Party] has prioritized something called "military-civil fusion."... It's a technical term but a very simple idea. Under Chinese law, Chinese companies and researchers must—I repeat, must—under penalty of law, share technology with the Chinese military.
>
> The goal is to ensure that the People's Liberation Army has military dominance. And the PLA's core mission is to sustain the Chinese Communist Party's grip on power—that same Chinese Communist Party that has led China in an increasingly authoritarian direction and one that is increasingly repressive as well....[21]

Time to Accelerate Intelligence Transformation

Technology. The IC agencies are keenly aware that they are operating in a complex world of information technology that is changing rapidly. How America's spies respond to these changes is vital. The advent of fifth generation (5G) technology is on the verge of establishing China as a near-peer competitor in telecommunications. Although there are barriers to entry that limit Huawei's access to the U.S. market, the Chinese 5G footprint is expanding at a rapid clip around the world including among U.S. allies. The intelligence threat posed by Huawei is of a significance that should not be underestimated:

> As an adversarial power, China cannot be allowed to use its government-controlled companies to gain a significant foothold in the United States' burgeoning 5G wireless networks. Such a presence would be a clear national security threat that could decisively compromise American telecommunications and data infrastructure—including the communications integrity of the US military and intelligence community...
>
> The U.S. must not be complacent. Beijing's "civil-military fusion" practices must not be allowed to threaten U.S. national security. Further, the U.S. must penalize Beijing's blatant attempts to threaten America's critical infrastructure and to use its technology industry as an extension of state espionage.[22]

Technology is generally multipurposed and often integrated into multiple strands of hardware and software. For example, AI combined with ML can be incorporated into the daily use of intelligence capabilities to support analysis, counter cyber threats, and also address insider threats. Machine learning holds promise for cyber defense.

The single biggest challenge for network defenders is detection: finding the adversary's presence in one's own network. Detection times vary based on the sophistication of the attacker and defender, but the average lingers at well over a year. While defenders have improved, in many cases, intruders can operate for months within the target network, unnoticed and unconstrained.[23] As cybersecurity expert Ben Buchanan has noted:

> Virtually every major cyber attack—such as Stuxnet, the two blackouts in Ukraine, and NotPetya—has been preceded by months, if not years, of reconnaissance and preparation. This window offers an opportunity. If machine learning can improve detection, interdiction, and attribution, it can dramatically reduce the potential dangers of cyber operations. That said, machine learning has been applied to cyber defense for several years already and challenges persist; it is thus vital to ground the evaluation of machine learning-aided cyber defense not just in theory but in practical—and ideally measurable—results.[24]

Our intelligence professionals must have the very best technology at their disposal. Today, technological innovation rests predominantly in the private sector. To bridge this gap, IC leaders need to promote the development of deeper public–private partnerships to facilitate rapid adoption of this technology. Unfortunately, because of mutual distrust, these partnerships are not easy to forge. Nonetheless, commercial companies can help to find innovative ways both to exploit the vast and increasing body of open-source information available to the intelligence analyst and to counter the sophisticated counterintelligence methods employed by China, Russia, and others to protect their secrets.

As Russell Travers noted in 2019, at least one vehicle for such collaboration already exists:

> Over the past two years, there has been a marked increase in Industries' willingness to work with one another, the

> US government and foreign partners to counter terrorism through the Global Internet Forum to Counter Terrorism (GIFCT). Originally created by Facebook, Microsoft, Twitter and YouTube, GIFCT has provided a vehicle for discussions and potential information sharing....
>
> The recent move to establish GIFCT as an independent organization, or NGO, offers a formalized opportunity to better leverage the respective strengths of the private sector and the U.S. government against this dynamic problem. The new construct looks to sustain and deepen industry collaboration and capacity, while incorporating the advice of key civil society and government stakeholders.[25]

The IC leadership needs to adapt commercially available "off the shelf" technology, even if modifications may be required to meet a specific intelligence need. Simultaneously, the IC leadership should cut off funding for technology development within its agencies if it lags far behind what is available in the private sector. This also requires a change in the cultural mindset to make the IC more receptive to adopting commercially based technology. Former Intelligence Community Chief Information Officer John Sherman has underscored that:

> Our adversaries are moving out quickly in many areas such as cyber, artificial intelligence and machine learning, information and asymmetric warfare, not to mention other capabilities such as conventional weapons and space. We must respond with equal urgency. We can and must win in an arena increasingly defined by technology, data, and cybersecurity. This requires even greater innovation and partnerships between the government, industry, allies, and academia.[26]

The IC requires commercial support in developing computer infrastructure that allows collectors and analysts to tackle rough problems such as breaking sophisticated encryption related to leadership communications or advanced weapon systems and identifying denial and deception tactics by adversaries. These capabilities must be secure yet interoperable across intelligence and defense platforms.

Information Integration. Managing information sharing effectively in a classified world remains enormously challenging because of the need to protect our secrets. Nonetheless, the balance between "the need to share" and "the need to protect" is askew under the current paradigm among our intelligence professionals. It is imperative to have in place a data management system in which every person that touches a piece of classified information is monitored to ensure not only that mission needs are met, but also that secrets are protected.

IC analysts are inundated by information, but the most important information needed to "connect the dots" can remain undiscovered or unavailable because the right information is not always identified for the right user. Barriers to information sharing persist among analysts, operators, and military personnel even within the same agency and certainly between the IC's various elements. This shortfall must be addressed to improve the quality of analytic work. As Damien van Puyvelde, Stephen Coulthart, and M. Shahriar Hossain have argued:

> Interest in data analytics has been growing due to the demand for more reliable intelligence products following the controversies caused by the 9/11 attacks and the absence of weapons of mass destruction in Iraq. Prior to 9/11 the US intelligence community lacked and missed specific pieces of information pointing to the terrorist plot. In 2002, a national intelligence estimate made a series of erroneous assessments regarding Iraq's WMD programme, which were later used to justify the US decision to go to war in Iraq. These events cast doubt on the intelligence collection and analysis

> capabilities of America's spy agencies, especially in the domain of human intelligence (HUMINT). Big data capabilities, it was hoped, would compensate for the limitations, and sometimes the absence, of HUMINT. Consequently, US intelligence agencies began to embrace more systematic and sophisticated data collection and analysis techniques.[27]

Enacting user-based access controls across IC data repositories offers a way to take the human intervention out of the information-sharing conundrum when accompanied with data user rights. What good does it do for an analyst to learn after judgments have been made that information was available but could not be accessed because of artificial barriers? Information needs to be controlled, but in a world where threats are often interconnected, the barriers to accessing mission-relevant information need to be removed so that the IC can provide the most accurate assessments possible to policy customers.

Integrated intelligence assessments are equally important for all customers. This is underscored by the case of the U.S. military, which needs reliable intelligence to maintain situational awareness and be prepared to prevent war but, if necessary, to fight and decisively win the next one. With reference to the Army (although it is equally true for all of America's uniformed services):

> Army HUMINT must be prepared to operate within multiple domains and employ materiel modernization to leverage artificial intelligence/fusion capabilities to reduce cognitive burdens on analysts. The Army G-2X enterprise must adapt to meet the readiness demands of great power competition by ensuring our CI, HUMINT, and security personnel are prepared to deploy, fight, and win across the spectrum of conflict. Through modernization, the Army G-2X enterprise must be able to build an agile CI, HUMINT, and security force that fully embraces the Information Age, including leveraging technology to reduce cognitive burdens on the force and deliver intelligence at the speed of mission.[28]

The complexities associated with understanding, preparing, and as necessary responding to more sophisticated adversaries calls for the best possible integrated intelligence for our warfighters and planners.

Talent. Removing barriers to hiring and retaining America's top talent is essential to addressing complex national security challenges. The backbone of the IC's performance, effectiveness, and efficiency is the quality and retention of its people. The good news is that the IC has no problem attracting prospective personnel with extraordinary skills and backgrounds. The bad news is that the IC lacks the ability to hire them quickly enough, and significant expertise is lost because the hiring process can takes as much as a year. Also, once in the IC, talented officers leave because they become disaffected by bureaucracy that discourages analytic dissent or by elements that discourage joint-duty career-enhancing assignments among the IC's 17 components.

As it relates to attracting and retaining the best and brightest personnel for the IC, two significant barriers need to be addressed.

First, the granting of a security clearance for an intelligence professional and/or supporting government contractor with the requisite skills remains inefficient despite some gradual improvements. In figures released in late November 2019, the Defense Counterintelligence and Security Agency "noted a dramatic drop in security clearance processing times as of FY 2019 Q4—295 days for Top Secret clearances (down from a high that reached over 500 days), and 181 days for Secret security clearances, down from over 300 days." These "DoD/Industry only numbers…represent the fastest 90% of all clearances."[29] However, the most talented professionals are not likely to wait a year or longer to start their jobs.

Second, when the time it still takes to get a security clearance is combined with the time

needed for a hiring decision—often more than a year—it is not hard to see why the new graduate in one of the highly sought-after technology fields may well not wait to be hired by an intelligence agency. It often takes much longer for first-generation American applicants with highly desirable native foreign language skills to be cleared. It is difficult to quantify the loss of talent and capability this represents, but we can assume that the Intelligence Community does lose badly needed talent.

A case study of graduates from the North Carolina State University Master's Program in Advanced Analytics provides some insights. If a graduate of this 10-month program were interested in a career in national security, it would be next to impossible for that individual to be interviewed, offered a job, and cleared through the process in less than 10 months. Even assuming a somewhat faster hiring process, 40 percent of those hired will leave their employment within two years because of perceived opportunities for job growth elsewhere—obviously a huge loss for any intelligence agency. Many leave for the private sector.[30]

Suitability Barriers to IC Talent Management. Different suitability norms ("suitability" refers to judgments about a person's character traits and conduct) among the IC elements act as a significant constraint on the movement of talent within the IC to meet the highest intelligence priorities. This obstacle also undermines IC team building. The receiving element often raises subjective objections under the guise of finding the prospective person "unsuitable" for the rotational assignment even though the criteria for security clearance are the same for all IC personnel. The resultant delays, often measured in months, undermine the use of the best talent despite IC mission requirements.

This obstacle must be removed if the IC is going to be able to place its talent where it is most needed to meet the requirements of the nation's political or military leadership and prioritize resource allocations to match the greatest threats that appear on the horizon. Removing the suitability barriers to transfers of IC personnel would also remove an important reason for the IC's talent drain. The ODNI should establish policies that significantly reduce what are often many months of delay in having personnel move from one IC element to another.

The Changing Persona of Clandestine Collection. The advent of biometrics and other threats to secure operation make obtaining core secrets from clandestine human sources extraordinarily challenging. Many of the technologies used by intelligence professionals are readily available to our adversaries, state and non-state alike. Facial recognition and biometrics more generally make the use of alias operational tradecraft nearly impossible. Human intelligence collection must therefore continue to evolve both to address the counterintelligence threats to securely running foreign human spies and to protect its own operational capabilities from the watchful eye of our adversaries.

A major shift in how human intelligence operations are conducted is required. While not easy, and while tradecraft must be applied, online (or cyber-based) human intelligence operations must be increased to spot, assess, develop, recruit, and handle human sources. At the same time, human-to-human interaction in a clandestine manner faces significant hurdles. "U.S. spies are no longer being tailed by foreign governments in about 30 different countries," according to one report, "because advances in facial recognition, biometrics and artificial intelligence have made it almost impossible for the agents to [maintain a false identity]."[31] One former CIA senior officer noted insightfully in 2015 that:

> As we continue to advance technologically, in essence making our world smaller, the potential threats posed by these advancements will make both protecting and exploiting real secrets exponentially more difficult. In addition, as these challenges continue to grow, those tasked with addressing them will need to adjust at a much more rapid rate. This applies

> both to field operatives as well as to their managers...
>
> The next generation of operatives and their managers will need to be more familiar with, if not adept at, technological augmentation. Augmentation, not replacement. While the tendency to rely increasingly on technology to make HUMINT collection more efficient is commendable, adherence to the core principals [*sic*] will ensure that human operations remain as secure as possible.[32]

Cyber Integration. The DNI has the authority to assign responsibilities within the IC, but the absence of clear policy direction on cyber issues leaves intelligence professionals without the guidance they need with respect to the parameters of their cyber activities. In addition, because of the absence of a policy framework, the IC elements, alongside other elements of the executive branch, have been left to chart their own courses as individual departments or agencies in executing offensive and defensive cyber activities as an element of U.S. national security.[33]

Adversarial threats in the cyber domain change quickly and are increasingly complex. As for the appropriate governance to meet cyber threats, Executive Order 12333, as amended by President George W. Bush in July 2008,[34] did not specifically address cyber as an intelligence discipline. Nonetheless, in just the few years since the IC's principal presidential directive was amended, it has become apparent that specific cyber "lanes in the road" need to be identified within the IC and throughout government.

Cyber intelligence informs a significant number of sub-disciplines such as cyber security, cyber defense, cyber offence, and cyber support to traditional military operations, as well as the establishment of international norms on cyber behavior during peacetime. These missions call for intelligence professionals who are competent to address the multi-strand demands associated with cyber operations, but there is a critical shortage of cyber talent in the public sector as it competes with private industry because demand for the unique skills and knowledge needed to combat the growing threats in the cyber domain has outpaced the supply of that talent for years. The public sector struggles to attract the required numbers of cyber-trained and experienced personnel because of its slow hiring process and lower compensation compared to the private sector.[35] For example, February 2015, the Pentagon had reached only the midway point in staffing Cyber Command and was backing away from the long-held goal of deploying a full force of 6,000 cyber personnel by 2016.[36] As a top priority, the IC must spend whatever is necessary to train existing IC officers with transferable skills and high potential to be cyber intelligence officers. Training is available in the private sector.[37]

Executive Order 12333 as amended gives the DNI the authority to define roles and responsibilities for elements of the Intelligence Community.[38] What is needed now to achieve enhanced integration among the key cyber collection agencies—the National Security Agency, Central Intelligence Agency, and Federal Bureau of Investigation—are clearly articulated policies for defining their respective missions and how information will be shared among them in a transparent manner. The IC leadership needs to remain focused on achieving "unity of cyber mission," which must be the top priority for anticipating and providing warning to the decision-makers about future threats. Under well-defined rules, the Cyber Threat Intelligence Integration Center (CTIIC) may eventually be in a position to contribute a strong analytic product on cyber threats.

Some progress has been made, but it is not enough. Cyber legislation was stalled for years, but with passage of the cyber bill in 2015, a framework for addressing cyber-related activities has begun to take form.[39] The CTIIC, established at the instigation of the White House ostensibly to conduct analysis of cyber threats, appears to have an ill-defined mission. It also has neither the resources nor the standing among the big departments and agencies to assess cyber threats.[40]

Counterintelligence. Catching spies and protecting our secrets is the traditional framework for counterintelligence. In order to counter highly sophisticated adversaries, however, the scope of counterintelligence needs to be expanded. This broader definition needs to include what our adversaries are doing through disinformation and other forms of information warfare to undermine both the U.S. and its friends and allies. IC talent needs to be placed against this broader definition of counterintelligence.

While the Chinese, Russians, and other adversaries have long wanted to steal our secrets by any means possible, these nations now leverage big data to promote their interests, using all forms of media to foster a false narrative of events in and outside the U.S. Counterintelligence requires identifying and then protecting our national security information on a much broader level. CI must still include its traditional focus on protecting our own secrets from foreign spies, but our security also depends on identifying and countering disinformation and insider threats, as well as responding to adversaries' efforts to disrupt U.S. intelligence. As Christopher Costa and Joshua Gelzter have written:

> If the U.S. government is to fight off disinformation—which can now be created on an industrial scale and spread globally not just by states but also by terrorists and criminals—it must reinvigorate and broaden the practice of counterintelligence.
>
> For too long, the focus of U.S. counterintelligence has been safeguarding government secrets and corporate intellectual property, particularly by thwarting foreign efforts to recruit potential thieves. We must remember that counterintelligence also means warding off efforts to divide and weaken us. We can draw on our Cold War experience and update our responses to reflect modern technologies.[41]

Today, "Moscow and other governments are learning key disinformation tactics from non-state actors" that are using more sophisticated cyber-generated influence operations. All adversaries are now in the cyber domain.

> These developments suggest a future in which both non-state and state actors will contest the United States through online disinformation campaigns, even while more traditional global power competition tied to geography continues to play out. Moreover, it seems inevitable that the Chinese, Iranians, and others will escalate their malign social media efforts much as the Russians have done. FBI Director Christopher Wray recently acknowledged that other countries have been exploring such influence efforts.[42]

The opportunities for the IC to identify and then counter the broad range of counterintelligence threats are coupled with the challenges and opportunities related to technology, information integration, people talent, and clandestine collection. All of these pieces must fit together to maximize the ability of our spy agencies to respond to a much higher national security threat environment for years to come. An effective response to these threats does not require additional funding or personnel resources for the IC, but rather reprioritization of existing capabilities.

Building a More Effective Intelligence Enterprise

As demonstrated after the terrorist attacks of 2001, the U.S. Intelligence Community has demonstrated that it can redirect its resources to meet a different type of threat. It did so immediately in the aftermath of the attacks in 2001 in order to pursue aggressive collection and analysis of Islamic terrorist groups. The goals for intelligence are immutable. Intelligence resources must be postured to give the policymaker and warfighter alike the upper hand against the adversary. That upper hand requires collecting threat warnings that can be

prevented from becoming a reality or be countered by reliable intelligence.

The ability of America's spy agencies to address the wide array of complex threats emerging from the need to deter great-power rivals requires IC leadership committed to applying the resources to address the highest threat vectors. It requires a strong sense of urgency with a top goal of harnessing the power of emerging and disruptive technologies as applied to data analytics, artificial intelligence, machine learning, 5G, and quantum computing while enabling the integration of autonomous systems. Currently, America's intelligence professionals must be prepared to ensure unambiguous advantage in the event of conflict escalation, but the IC needs to be able to act preemptively and provide advance warnings of threats to our national security from both state and non-state actors.

With this in mind, there are several actions that can and should be taken. Specifically:

- **The Director of National Intelligence should require all IC members to provide a plan with specific goals to increase their partnerships with the private sector to acquire cutting-edge technology and infrastructure support.** Each plan should be accompanied by a road map and timetable for adoption of that technology. In an era of significant growth in data and data processing requirements, America's intelligence professionals require the best technology that the private sector has to offer. They should therefore promote agile public–private partnerships to assure their access to the technological innovation that is constantly emerging from America's vibrant commercial sector.

- **The DNI needs to establish a needs-based information-sharing model with appropriate auditing functions to enable enhanced data access by all intelligence professionals with a need to know.** Notwithstanding advances over the past two decades, mission-essential information sharing remains too restricted within the IC due to the propagation of data stovepipes and absence of user-based permissions. Fear continues to drive the risk calculus by the so called owners of data (the agencies that obtain the classified information). The result could be failure to provide adequate warning because mission users are unable to access siloed information.

- **For the Top Secret/Sensitive Compartmented Information clearance, the DNI should mandate and then rigorously enforce time constraints on the security clearance process.** The IC must depend on state-of-the art CI monitoring for its first ring of protection. Therefore, bureaucratic barriers that prevent the timely entry of much-needed talent must be eliminated, and every effort must be made to retain vital personnel and to facilitate ingress to and egress from the IC for that talent. Special allowances are needed for compensation related to highly desirable science, technology, engineering, and mathematics (STEM) talent. Interchangeability of intelligence personnel talent must be promoted aggressively among the 17 elements of the IC to meet the highest intelligence requirements. Suitability barriers to accepting transfers of personnel need to be removed.

- **Clandestine human intelligence collection needs to reevaluate how it can identify, assess, develop, and recruit foreign spies by using different tactics.** Human intelligence operations can no longer rely solely on traditional tradecraft for in-person meetings using alias personas that are subject to discovery because of microchip information and biometrics. A comprehensive revamping of clandestine human intelligence collection is needed. Today's threats to traditional spying will require far more reliance on

online cyber personas and far less reliance on foreign-based collection efforts by American operators.

- **The Acting DNI took an important step in mid-May with the announcement that intelligence-focused cyber efforts would be consolidated under an IC Cyber Executive.** However, this does not go far enough to meet the challenges of cyber-centric requirements. The IC's capabilities against determined adversaries now need to be rigorously assessed with a view to ensuring the IC's ability to defend and respond as necessary to an adversary's capabilities in cyberspace.

- **The DNI needs to lead in expanding the scope and depth of America's counterintelligence focus to address our adversaries' ability to use aggressive cyber online operations to influence the hearts and minds of Americans.** This expanded application of CI can meet the continued need to address more complex challenges pertaining to insider threats in a cyber-centric world and the need to protect national security secrets.

Conclusion

The foundation of U.S. intelligence is sound, but America's intelligence agencies face a range of new national security challenges from emerging great-power competitors. To meet these challenges, the IC needs to attract and retain deep subject matter expertise, including foreign languages, and to focus on China and Russia (and their allies), enhanced operational tradecraft, and a significant increase in the use of technology and STEM-trained personnel to apply artificial intelligence, machine learning, and data analytics in an effective manner. Cyber-centric operational capabilities for U.S. intelligence personnel must become the norm for achieving success against determined and relentless adversaries.

The Intelligence Community, with the benefit of clearly articulated requirements from the policymaker and the warfighter, is capable of delivering invaluable intelligence. This requires bold leadership that is prepared to invest in its people, technology, and security. The leadership needs to incentivize the increase of IC integration and strengthen public–private partnerships to maximize access to innovative technologies.

The challenges facing our intelligence professionals are not for the faint of heart. Dealing with these challenges will require creativity and meaningful steps to break down the bureaucratic walls among the IC's 17 elements. America's national security deserves nothing less than a federated Intelligence Community that operates with unity of effort and interdependence, confronting the capabilities of our adversaries with an eye to providing high-confidence decision advantage for every customer of the world's finest intelligence organizations.

Endnotes

1. *National Security Strategy of the United States of America*, The White House, December 2017, p. 32, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (accessed June 17, 2020).
2. Bloomberg News, "China's Got a New Plan to Overtake the U.S. in Tech," updated May 21, 2020, https://www.bloomberg.com/news/articles/2020-05-20/china-has-a-new-1-4-trillion-plan-to-overtake-the-u-s-in-tech (accessed June 17, 2020).
3. Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 2nd ed. (Washington: Congressional Quarterly Press, 2003), p. 8.
4. Jennifer E. Sims, "Decision Advantage and the Nature of Intelligence Analysis," Chapter 24 in *The Oxford Handbook of National Security Intelligence*, ed. Loch K. Johnson (New York: Oxford University Press, 2010), Abstract, https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780195375886.001.0001/oxfordhb-9780195375886-e-0024?result=4&rskey=0ztes9 (accessed July 26, 2020).
5. Daniel R. Coats, Director of National Intelligence, "Worldwide Threat Assessment of the US Intelligence Community," statement before the Select Committee on Intelligence, U.S. Senate, January 29, 2019, p. 4, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf (accessed June 17, 2020).
6. Office of the Director of National Intelligence, *National Intelligence Strategy of the United States of America*, 2019, p. [1], https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf (accessed June 17, 2020).
7. The Office of the Director of National Intelligence; the Central Intelligence Agency (other than the ODNI, the only element of the IC that is outside of a department); the National Security Agency; the Defense Intelligence Agency; the National Geospatial Agency; the National Reconnaissance Office; the four intelligence elements of the Army, Navy, Air Force, and Marine Corps; the Federal Bureau of Investigation's National Security Branch; the Department of State's Bureau of Intelligence and Research; the Department of the Treasury's Office of Intelligence and Analysis; the Drug Enforcement Administration's Intelligence Program; the Department of Homeland Security's Office of Intelligence and Analysis; the Department of Energy's Office of Intelligence and Counterintelligence; and U.S. Coast Guard Intelligence.
8. The National Security Agency, the Defense Intelligence Agency, the National Geospatial Agency, the National Reconnaissance Office, and the four intelligence elements of the Army, Navy, Air Force, and Marine Corps.
9. S. 2845, Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, 108th Cong., December 17, 2002, https://www.congress.gov/search?q=%7B%22search%22%3A%22cite%3APL108-458%22%7D (accessed July 17, 2020).
10. Executive Order 13470, "Further Amendments to Executive Order 12333, United States Intelligence Activities," July 30, 2008, in *Federal Register*, Vol. 73, No. 150 (August 4, 2008), p. 45326, https://fas.org/irp/offdocs/eo/eo-13470.pdf (accessed July 17, 2020).
11. Marshall C. Erwin and Amy Belasco, "Intelligence Spending and Appropriations: Issues for Congress," Congressional Research Service *Report for Members and Committees of Congress*, September 18, 2013, p. 6, https://fas.org/sgp/crs/intel/R42061.pdf (accessed June 17, 2020).
12. Russell E. Travers, Acting Director, National Counterterrorism Center, "Counterterrorism in an Era of Competing Priorities," remarks delivered at Washington Institute for Near East Policy, November 8, 2019, p. 8, https://www.dni.gov/files/NCTC/documents/news_documents/Travers_Washington_Institute_Remarks_as_Prepared.pdf (accessed July 17, 2020). Punctuation as in original.
13. Ibid.
14. "Indications" are signs or evidence that reveal an entity's intent to perform some act, and "warning" connotes an immediacy of action that poses a danger. The unexpected recall of soldiers from leave or movement of supply trucks to an area indicate that an opponent is up to something of importance per an IC analytic customer's stated interests. Similarly, the movement of fueling vehicles to a missile launch pad is a sign or warning that the launch of a missile is imminent.
15. Senate Report 108-258, *To Authorize Appropriations for Fiscal Year 2005 for Intelligence and Intelligence-Related Activities of the United States Government, the Intelligence Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for Other Purposes*, 108th Cong., 2nd Sess., May 5, 2004, p. 7, https://www.congress.gov/congressional-report/108th-congress/senate-report/258/1?s=1&r=42 (accessed July 17, 2020).
16. See note 9, *supra*.
17. David R. Shedd, "Intelligence and National Defense," in *2016 Index of U.S. Military Strength*, ed. Dakota L. Wood (Washington: The Heritage Foundation, 2015), pp. 45–59, https://s3.amazonaws.com/ims-2016/PDF/2016_Index_of_US_Military_Strength_FULL.pdf (accessed July 17, 2020).
18. Oracle Cloud, "Adaptable Businesses and the Productivity Paradox," in *The Adaptable Business: Future Skills and Cultural Forces*, 2019, pp. 3 and 11, https://www.oracle.com/a/ocom/docs/dc/the-adaptable- business.pdf?elqTrackId=28c5abc9c44d4a5d872b2e6cd1a92c68&elqaid=79966&elqat=2 (accessed July 17, 2020).

19. Ibid., p. 3.
20. Alex Finley, "How the CIA Forgot the Art of Spying," *Politico Magazine*, March/April 2018, https://www.politico.com/magazine/story/2017/03/cia-art-spying-espionage-spies-military-terrorism-214875 (accessed July 17, 2020).
21. Secretary of State Michael R. Pompeo, "Technology and the China Security Challenge," remarks delivered at the Commonwealth Club, San Francisco, California, January 13, 2020, https://www.state.gov/silicon-valley-and-national-security/ (accessed July 17, 2020).
22. Klon Kitchen, "The U.S. Must Treat China as a National Security Threat to 5G Networks," Heritage Foundation *Issue Brief* No. 4952, April 16, 2019, p. 1, https://www.heritage.org/technology/report/the-us-must-treat-china-national-security-threat-5g-networks.
23. FireEye, *M-Trends 2020*, FireEye Mandiant Services *Special Report*, p. 11, https://content.fireeye.com/m-trends/rpt-m-trends-2020 (accessed June 16, 2020).
24. Ben Buchanan, "A National Security Research Agenda for Cybersecurity and Artificial Intelligence," Center for Security and Emerging Technology *Issue Brief*, May 2020, p. 7, https://cset.georgetown.edu/wp-content/uploads/CSET-A-National-Security-Research-Agenda-for-Cybersecurity-and-Artificial-Intelligence.pdf (accessed July 17, 2020). See also Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (New York: Oxford University Press, 2017), Chapter 2.
25. Travers, "Counterterrorism in an Era of Competing Priorities," p. 12.
26. John B. Sherman, Assistant Director of National Intelligence and Intelligence Community Chief Information Officer, "From the IC CIO," in Office of the Director of National Intelligence, "Strategic Plan to Advance Cloud Computing in the Intelligence Community," June 26, 2019, p. 1, https://www.dni.gov/files/documents/CIO/Cloud_Computing_Strategy.pdf (accessed July 17, 2020).
27. Damien van Puyvelde, Stephen Coulthart, and M. Shahriar Hossain, "Beyond the Buzzword: Big Data and National Security Decision-Making," *International Affairs*, Vol. 93, No. 6 (November 2017), p. 1398, https://www.chathamhouse.org/sites/default/files/images/ia/INTA93_6_06_VanPuyvelde%20et%20al.pdf (accessed July 17, 2020).
28. Lieutenant Colonel Marcus O'Neal, "Army G2X Support to Army Readiness and Modernization Priorities," *Military Intelligence Professional Bulletin*, Vol. 46, No. 1 (January–March 2020), p. 23, https://fas.org/irp/agency/army/mipb/2020_01.pdf (accessed July 17, 2020).
29. Lindy Kyzer, "How Long Does It Take to Process a Security Clearance? (Q4 2019)," ClearanceJobs, November 20, 2019, https://news.clearancejobs.com/2019/11/20/how-long-does-it-take-to-process-a-security-clearance-q4-2019/ (accessed July 17, 2020).
30. Institute for Advanced Analytics, "Master of Science in Analytics: 2019 Alumni Report," reported as of January 4, 2020, http://analytics.ncsu.edu/reports/alumni/MSA2019.pdf (accessed July 17, 2020).
31. Emily Crane, "Will the Digital Age Kill Off Spying? CIA in Crisis as Facial Recognition, Biometrics and AI Make It Increasingly Difficult for Agents to Maintain Their Cover Abroad," *The Daily Mail*, December 30, 2019, https://www.dailymail.co.uk/news/article-7837767/CIA-faces-crisis-intelligence-gathering-digital-footprints.html (accessed July 17, 2020).
32. John Sano, "The Changing Shape of HUMINT," *The Intelligencer: Journal of U.S. Intelligence Studies*, Vol. 21, No. 3 (Fall/Winter 2015), pp. 79–80, https://www.afio.com/publications/SANO%20John%20on%20The%20Changing%20Shape%20of%20HUMINT%20Pages%20from%20INTEL_FALLWINTER2015_Vol21_No3_FINAL.pdf (accessed July 17, 2020).
33. See U.S. Government Accountability Office, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, GAO-13-187, February 2013, https://www.gao.gov/assets/660/652170.pdf (accessed July 17, 2020).
34. See note 10, *supra.*
35. Amber Corrin, "Is There a Cybersecurity Workforce Crisis?" *Federal Computer Week*, October 15, 2013, https://fcw.com/articles/2013/10/15/cybersecurity-workforce-crisis.aspx (accessed July 17, 2020).
36. Aliya Sternstein, "Need a Job? Cyber Command Is Halfway Full," Nextgov, February 6, 2015, http://www.nextgov.com/cybersecurity/2015/02/need-job-cyber-command-halfway-full/104817/ (accessed July 17, 2020).
37. See, for example, SANS Institute web site, www.sans.org (accessed July 17, 2020).
38. *Federal Register*, Vol. 73, No. 150 (August 4, 2008), pp. 45326–45327.
39. Rob Lever, "Congress Passes Long-Stalled Cybersecurity Bill," *Space War*, December 18, 2015, http://www.spacewar.com/reports/Congress_passes_long-stalled_cybersecurity_bill_999.html (accessed July 17, 2020).
40. "Fact Sheet: Cyber Threat Intelligence Integration Center," The White House, February 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center (accessed July 17, 2020).

41. Christopher P. Costa and Joshua A. Geltzer, "To Fight Disinformation, Rethink Counterintelligence," *Defense One*, October 14, 2019, https://www.defenseone.com/ideas/2019/10/fight-disinformation-rethink-counterintelligence/160582/ (accessed July 17, 2020).
42. Ibid.