Capt. Taiwan Veney, cyber warfare operations officer, watches members of the 75th Cyberspace Operations Group, Warfield Air National Guard Base, Middle River, Maryland, June 3, 2017. (Photo: J.M. Eddins Jr./US Air Force)

Integrating the IC's Cyber Security Mission

Melissa Hathaway

Melissa Hathaway is president of Hathaway Global Strategies, which provides strategic advice to companies, NGOs, and countries. She led cyber security initiatives under Presidents George W. Bush and Barack Obama.

Information warfare is not new, nor is the fact that our cyber insecurity has been growing for nearly four decades. In the 1980s, US cyber capabilities were called information warfare, communications countermeasures, electronic warfare, propaganda, information operations, etc. Using such activities to disrupt, degrade, deny, or destroy could produce strategic effects on the adversary. Russian military theorists called it information confrontation in a technical and psychological manner.

In the early 1990s, I worked on a net assessment of information warfare requested by Secretary of Defense William Perry and conducted by the Office of Net Assessment under Andrew Marshall. The study compared US capabilities vis-a-vis our competitors, acknowledging that the United States needed to understand whether we had a comparative advantage. At that time, the community of military and intelligence personnel working these issues was quite small. What emerged from that study and subsequent efforts was the fact that as the United States digitized more of its critical infrastructures and military capabilities, it would become more vulnerable.

In 1998, President Bill Clinton signed Presidential Policy Directive 63 recognizing this vulnerability. It stated, "because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in nontraditional ways including attacks within the United States. Because our economy is increasingly reliant upon interdependent and cyber-supported infrastructures nontraditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy." It would take another decade before the United States would harness the strengths of the entire government and work to buy down the risk of the previous decades.

In March 2007, President George W. Bush received a briefing at NSA from senior IC leaders responsible for emerging and maturing cyber capabilities and operations of the United States. At the end of the briefing, the president asked what other nations were capable of and what types of cyber operations were being carried out by them domestically against the United States as well as US interests abroad.

Bush understood the situation was not good. Foreign governments, non-state actors, and criminal elements were all increasing their cyber attacks against US information infrastructures and industries with emphasis toward the defense industrial base weapon systems and intellectual property. He wanted recommendations to address the glaring deficiencies, and he tasked then DNI Mike McConnell to coordinate a comprehensive assessment of the problem.

National Cyber Study Group

On April 1, 2007, the DNI signed a memo notifying 20 agencies directing the stand-up of the National Cyber Study Group and requiring each agency to detail a senior executive of cyber intelligence and operations to the project (as authorized under IRTPA). I would lead the team as a "senior adviser" to the DNI.

I had worked with Mike for more than 10 years and I had been working in the cyber mission-space for more than 20. We knew that my job title needed to change. We modeled my title after the National Counter-Intelligence Executive, and the DNI named me the first National Cyber Coordination Executive—effectively a new mission manager.

Using the DNI's authorities, I assembled an unprecedented cross-government coalition to prepare the threat assessment, develop a strategy, identify operational capabilities needed to address the situation, and do so by taking a collaborative and cooperative perspective that recognized the breadth of expertise within and across each organization that had to come together for mission success. I helped the team earn and sustain an environment of trust.

During weekly NCSG meetings, the group of executives we nicknamed Team America engaged openly and collaboratively to learn and understand each other's stated missions, authorities, and capabilities. The goals: identify the strengths and skills of individual organizations to determine how each could best be utilized to form a comprehensive, unified strategy; and use that strategy to effectively confront malicious cyber activities across all sectors to stop what we believed to be an existential threat to the country.

Transparency was critical. To keep everyone connected and informed, we developed a fortnightly update for all agency heads, along with the National Security Council, Homeland Security Council, and Office of Management and Budget. This hyper-transparency was necessary to develop a holistic, integrated vision for the community that spanned defensive, offensive, and law enforcement operations.

On June 30, 2007, McConnell held the first Joint Intelligence Council. Under the IRTPA authorities, the DNI can convene the leaders of the Intelligence

Community and key consumers of intelligence to raise awareness of the existing and emerging threats to the country. The NCSG briefed the extent of the known cyber compromises in the country, including but not limited to: the targeting, penetration, and malicious exploitation of more than 200 companies and suppliers in the defense industrial base, including pre-positioned malicious code in the software libraries associated with the F-35; the targeting and exploitation of presidential candidates' campaign staff, policy papers, and donor lists; the constant reconnaissance and occasional penetration of sensitive government networks; and extensive criminal activity against the financial services community. It was as if the leaders of these agencies were hearing about the cyber threat for the first time. They all agreed that a comprehensive strategy must be pursued and presented to the president swiftly.

On September 20, 2007, NCSG briefed President Bush and Cabinet members at the White House. The NCSG put forth a comprehensive set of options regarding how best to integrate US government offensive and defensive cyber capabilities; how best to optimize, coordinate and deconflict cyber activities; and how to better employ cyber resources to maximize performance. President Bush concurred with the recommendations and ordered OMB Director Clay Johnson to resource the program with a sizable amount of "new" money.[a] The NCSG then became the Joint Inter-Agency Cyber Task Force (JIACTF) and developed and created a unified cross-agency budget submission for Fiscal Year 2008 and for 2009–13, assembling disparate funding sources into a coherent, integrated program.

The budget also addressed some very important and fundamental items for operational continuity and fortification. For example, CIA's cyber program had been entirely funded under the counterterrorism supplemental funding after 9/11, and it needed to be moved into its baseline funding. FBI had a significant shortfall in cyber agents and was operationally standing up the National Cyber Investigative Joint Task Force for law enforcement operations. Moreover, there was a shortfall in CI personnel and capabilities. Finally, there was an infrastructure and modernization gap for the broader signals intelligence enterprise that was under NSA's purview. These shortfalls were all addressed in the Bush administration's budget request.

In January 2008, the strategy and programs were codified in the Comprehensive National Cybersecurity Initiative (CNCI) with the issuance of NSPD-54/HSPD-23. The JIACTF created and presented a statement for the record for every committee in Congress, earning accolades from committee leaders. Members of the coalition briefed members of 110th and 111th sessions of Congress and full committees more than 150 times, crossing jurisdictional boundaries in both chambers. We presented a unified perspective on the cyber threat and the US government operations that were addressing the situation. We highlighted the shortfalls in personnel, operational capabilities, and technologies, as well as IC capabilities and supporting infrastructures needing congressional authorization and appropriation. Congress authorized and appropriated nearly all the funds requested, and CNCI became the first ever integrated cyber program for the government and one of the single largest intelligence programs of the Bush administration.

At this point, the JIACTF—or the cyber mission manager—needed to develop processes, procedures, and reporting mechanisms to drive execution and accountability across the dozens of programs associated with and starting from the CNCI. It was a true cross-cultural and cross-agency execution and system for one mission to address multiple threats. This may have been the hardest to manage, in large part because the executive branch and most notably the IC is not used to having to work

a. In government budget parlance, this means additional funding rather than taking money from one program to create another.

together to coordinate its operations or report on the collective or individual successes or gaps within the mission space. Despite all efforts to be transparent and share resources and credit for the mission, there was still reluctance to share information regarding unique accesses and capabilities with the larger group.

The JIACTF established a quarterly reporting cycle to the president that would highlight the programmatic execution and where there may be legal or policy gaps that were impediments to mission success. The quarterly report also noted where some agencies were not able to obligate and execute funds against directed missions and recommended areas where reprogramming may be necessary. It was the first time the executive branch was held to a standard reporting mechanism, similar to a quarterly report to shareholders.

The ODNI's mission is to lead and support IC integration: delivering insights, driving capabilities, and investing in the future. That mission is hard to operationalize and make effective because when a person (or group of people) must lead a multi-agency mission, the leader or mission manager really must understand the measures and rewards system of every agency to ensure the entire team is recognized and each person has career growth opportunities.

For the cyber mission, this was particularly difficult because the community is not designed to be joint and most agencies will not send their "best" leaders to a joint mission center because they do not want to lose their best talent and detail those individuals to another organization that is outside of their agency's core mission. Furthermore, it would be rare for any leader in the community to know all of the personnel systems and be able to write their performance review, recommend salary adjustments, or nominate detailed personnel for specific recognition awards either within the DNI structure or from their home agency. This is a key shortfall for any multi-agency mission center of excellence.

Second, the cyber mission was a key portfolio that was elevated among both political parties and required extensive briefings to the transition teams. The JIACTF had to ensure that cyber was positioned as a mission priority in the IC, FBI, DHS, DOD, DOJ, and DOE. This required extensive coordination and collaboration to ensure that every agency was using the same language and briefing the importance of the mission, as the threats and capabilities of the malicious actors continued to evolve in sophistication and complexity. While some of this was already done when the single statement for the record was created for Congress, the threat had continued to become more serious in the months leading up to the election.

Lastly, there is a transition period approaching and after a presidential election, especially if the White House changes political parties. The JIACTF had to maintain focus on the mission and ensure a stable and successful handoff to a new president and a largely new national security team. We established relationships and held multiple briefings with both nominee's transition teams. We communicated how important the program was to the national and economic security of the country.

Cyberspace Policy Review

The new integrated cyber program was successfully handed off in 2009. The CNCI became the centerpiece of President Obama's Cyberspace Policy Review and eventually was expanded to include a broader focus on the entire country and the vulnerabilities in the critical infrastructures and services that underpin the economy. There was also a recognition that the commercially based supply chain—the hardware and software that are the backbone of every company and government institution—remained prone to disruption, vulnerable to exploitation, and was being co-opted by malicious actors because those malicious actors recognize that this portion of the

supply chain collectively is a strategic economic and vulnerability of the United States. Addressing this situation was going to require key regulatory bodies to amend the rules and create new market forces to facilitate the fielding of better products and more resilient services in the marketplace.

President Obama appointed Special Assistant to the President and Cybersecurity Coordinator Howard Schmidt to lead and direct the executive branch toward a more unified intelligence and operations, but with a focus on ensuring the resilience of the US critical infrastructures. One of the key initiatives that needed to be accelerated was the connectivity and mission coordination between each of the cyber mission centers at FBI, NSA, CIA, DIA, and DHS to help drive situation awareness and provide actionable intelligence to decision makers and the owners/operators of the critical infrastructures.

Unfortunately, the interagency centers continued to operate in silos based on mission and are understaffed. Despite efforts to move the CNCI forward, the Obama administration was forced to react to multiple, massive counterintelligence breaches—as the Russians call it, warfare in a technical and psychological manner—by Chelsea Manning, Edward Snowden, Joshua Schulte, and others; the breach of OPM that resulted in the loss of over 22 million government personnel security investigation/clearance records; and attacks by Shadow Brokers (2016), a malicious actor that exfiltrated and posted tools and exploits from NSA on Github. These significant violations of the Espionage Act put the United States on a back foot and degraded our capabilities for years.

In 2015, DNI James Clapper disbanded the JIACTF. Rather than continue to improve on it, the DNI replaced it with the Cyber Threat Intelligence Integration Center. Again, using the IRTPA authorities, the CTIIC was set up to integrate cyber threat intelligence to better inform national interests, support national cyber policy and planning efforts, and coordinate an IC-wide approach to cyber collection and investment. However, this center was only tactically focused on ensuring that timely and objective national (cyber) intelligence was making its way into the President's Daily Brief.

The new center was not a mission manager but rather an analytic coordination center of excellence. Moreover, the other centers at FBI, NSA, CIA, DIA, and DHS remained and the community reverted to operate within their organizational remit. The leadership, management, and advocacy functions of the JIACTF were lost. Team America was disbanded.

President Trump largely focused on enhancing the military's cyber operational capabilities. In May 2018, Trump ordered Cyber Command's elevation to a Unified Combatant Command. In August 2018, he signed out National Security Policy Memorandum (NSPM) 13, which delegated key authorities to the secretary of defense to conduct time-sensitive military operations in cyberspace. This empowered Cyber Command to conduct persistent-engagement operations, which recognized that cyber forces must be in constant contact in cyberspace with competitors day to day.

A key pillar to that concept is what defense officials called "defending forward," which involved operating outside US networks to face threats as far away from the United States as possible. This of course required even more exquisite intelligence to inform operations—not only from the US intelligence community, but from our foreign partners as well. The National Defense Authorization Act for FY 2019 codified these operations, deeming them traditional military activities that no longer require special approval from the president.

IRTPA 2.0

President Biden elevated the cyber portfolio at the White House when he established the position of deputy national security

advisor for cyber and emerging technology under the leadership of Anne Neuberger. Further, the Congressionally mandated Cyberspace Solarium Commission recommended 80 different actions for the executive branch and advocated for the establishment of an Office of a National Cyber Director supported by a staff of at least 70 people to effectively perform the mission of the JIACTF. On April 12, 2021, Biden nominated Chris Inglis, former deputy director of NSA (2006–14), to lead that effort.[a]

While the executive branch continues to struggle with how best to organize the collection of actionable intelligence and out maneuver our adversaries in cyberspace, malicious cyber activities have became more sophisticated, more targeted, and more consequential. It does not stop there; the IC is also observing new tradecraft that blends electronic warfare, with cyber operations, and disinformation to achieve even more devastating effects. Each malicious actor has different levels of skill and intentions; therefore, the country must develop flexible capabilities to understand and counter the activities, but must also focus on resilience.

The ODNI's mission managers and the broader intelligence community must adapt, collaborate, and bring the power of multiple disciplines together to address the situation. The ODNI, because of its comprehensive oversight, budget advocacy, and statutory leader of the IC is the best positioned to lead and manage the community using all of their collective authorities, capabilities, and operational capacity to drive meaningful cybersecurity and resilience of the nation. This is not just an intelligence collection and analysis problem. It is an operational problem too that requires commensurate budget to prioritize programs and provide actionable intelligence to empower the collective defense of our country. It requires resolve, courage, and leadership. We cannot concede to weakness, rather we must rise to the challenge that the ubiquitous digital systems, information technologies, and connectivity that underpin our daily life and global economy are vulnerable and under attack. We must aggressively employ our full spectrum of cyber capabilities to support and defend the nation. Failing to do so is simply not an option. ■

a. Inglis served as the national cyber director from July 11, 2021 to February 15, 2023.