December 2022

Crucial Considerations for Federal Government Cybersecurity Strategies

Steve Kapinos, ICIT Fellow & VP of Cognitive Cyber, ManTech

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

ManTech
Securing the Future

ICIT | Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

ICIT's Bright Minds Q&A Series

Crucial Considerations for Federal Government Cybersecurity Strategies

With Steve Kapinos, VP of Cognitive Cyber, ManTech

December 2022

ICIT Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

About This ICIT Bright Mind Q&A

In continued support of our mission to cultivate a cybersecurity renaissance that will improve the resiliency of our nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders, ICIT has embarked on a journey to hold candid interviews with some of the brightest minds in national security, cybersecurity, and technology. Our goal is to share their knowledge and insights with our community to shed light on solutions to the technology, policy, and human challenges facing our community. Our hope is that their words will motivate, educate, and inspire you to take on the challenges facing your organizations

This Bright Minds Q&A explores crucial considerations for government cybersecurity leaders developing and implementing their 2023 strategic plans. In addition to the responsibilities and challenges all cybersecurity leaders are facing, such as the talent gap and continually evolving adversaries, Government leaders are tasked with balancing public-private partnership and working within established government processes; one such example is the Authorization to Operate process.

ICIT Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

About this Bright Mind:

Steve Kapinos is ManTech's Vice President of Cognitive Cyber responsible for new innovations and capabilities that turn cybersecurity-relevant data into insights that support mission operators. Mr. Kapinos' more than 10-year tenure at ManTech spans working with customers in support of cyber missions as well as overseeing people and budgets. While contributing to capability development for customer missions, he has led efforts that protect ManTech customers' information and systems.

Mr. Kapinos has managed a team of researchers, developers and engineers in the pursuit of novel cyber capabilities to overcome significant customer challenges. Additionally, he advises ManTech's executive leadership team on cyber policy issues.

Prior to joining ManTech, Mr. Kapinos delivered information security services, both internally and externally as a consultant, to communications, financial and energy sector clients. He holds both a Certified Information Systems Security Professional (CISSP) and a Project Management Professional (PMP) certification. Mr. Kapinos earned an MBA from the Raymond A. Mason School of Business at the College of William and Mary. He also holds a Bachelor of Science in Criminal Justice - Economic Crime Investigation from Utica College of Syracuse University.

ICIT:
How should organizations think about adversaries, their goals, and objectives?

Steve Kapinos:
In general, cybersecurity tends to focus on the most recent big event and how defenses can be adjusted to better prevent that threat. Meanwhile, advanced adversaries are already working on their next novel means of meeting their objectives. Instead, offense-informed defense augments advanced threat hunting, allowing us to understand adversaries and how tactics, tools, and procedures (TTPs) change over time. We look at changes in the defensive landscape, such as zero trust architecture, and examine how they could impact adversary campaigns, costs, and TTPs. With this knowledge, we implement advanced deception techniques and analytics to identify adversary activity before compromise.

For example, we believe insider threat programs must adjust to better understand and defend in a zero trust world. As adversaries are forced to utilize approaches that more consistently mimic an authorized user's behavior, detection programs will need to be modified. Additionally, adversaries may move from technical capabilities to targeting specific individuals and co-opting them to accomplish their objectives. Simultaneously, individual users are often annoyed by the necessity of multi-factor authentication, so organizations need to deal with the challenge of consolidating their identity and credential access management to provide a seamless experience for users.

Cybercriminals are agile and constantly sharpening their craft, as their continued success depends on it. Thus, this same mindset needs to become more pervasive among cyber defenders. Once organizational defensive cyber operations have matured, they should consider utilizing more active defensive techniques to confuse and entrap adversaries rather than just reacting. These active defenses bring more creativity to bear and could incorporate capabilities such as attack surface obfuscation and deception techniques. However, these capabilities must be well-designed and evolve with the adversary to be truly effective.

ICIT:
As you think about the defense of critical infrastructure, is there a recommendation you'd make?

Kapinos:
One remaining critical recommendation from the original Cyber Solarium Commission report is to codify the concept of systemically important critical infrastructure (CSC Recommendation 5.1[1]). We need to make sure the definition of entities covered by this designation is robust yet flexible enough to ensure that, as technologies and interconnections change, the ability to cover additional entities is not overly burdensome. Ten years ago, we would not have foreseen how

[1] The recommendation included, "whereby entities responsible for systems and assets that underpin national critical functions are ensured the full support of the US government and shoulder additional security requirements befitting their unique status and importance."

critical the cloud provider architectures would become to government, business, and citizens, yet they are today. The Cybersecurity and Infrastructure Security Agency's (CISA) work to create the National Critical Functions set, with its associated framework and approaches, should be leveraged to create this definition. Bringing these efforts together and maturing them will enable a strong, critical infrastructure ecosphere.

There has been concerted effort over the past year to define systemically important entities and clearly identify their roles and responsibilities. Early draft versions of the National Defense Authorization Act (NDAA) for Fiscal Year 2023 contained Section 5207 Systemically Important Entities, which had language for this purpose. That draft contained key provisions with significant potential such as in Subsections (e) through (k), which focused on better collaboration between the government and the covered entities as well as detailing support required from the government for specific entities. While this section was not included in the latest proposed NDAA, we subsequently saw President Biden issue a letter to Congressional leadership in early November stating his administration's support for reviewing and revising United States policy for critical infrastructure. The communication stated a critical need in that "Updated policy would strengthen the public-private partnership and provide clear guidance to executive departments and agencies (agencies) on designating certain critical infrastructure as systemically important." We must make sure these efforts culminate in the required policy changes.

ICIT:
What could be done to better understand the complexity of critical infrastructure and improve resiliency?

Kapinos:
A ransomware attack against the IT network of Colonial Pipeline taught the cybersecurity community that the interconnectedness of systems needs to be understood and risks considered from that perspective. However, an aging critical infrastructure with new technology layered on top makes it difficult to understand the holistic system's architecture. Due to this, we must advance how we model and assess critical systems' risks, especially those deemed systemically important.

We also need to focus on recovery and resilience, not just detection, prevention, and response. Even the best-prepared organizations have cyber incidents, and it is vital to limit the impact through resilient systems and robust, well-practiced recovery processes. For critical infrastructure, exercising and validating expected outcomes is likely impossible on physical systems. Thus, digital models and architectures achieved through applying model-based systems engineering will be critical to accurately understanding risk, impact, and recovery. These exercises should leverage adversarial threat-based analysis to ensure they accurately reflect the capabilities that adversaries may deploy in campaigns targeting them. The capabilities deployed will vary based on the adversary's goals, from extortion through ransomware to large-scale disruption via interrupting electricity distribution. As attacks are contained and the environment is recovered, actual exercises will validate controls such as the immutability of backups in the face of ransomware.

ICIT:
What are some ways the Federal Government could improve the security of their systems?

Kapinos:
Government processes are not flexible enough to keep pace with the rate of technological changes. In some cases, such as the Authorization to Operate (ATO), that inflexibility leads to less security. The processes required to review and approve changes to an environment cause significant delays, allowing known vulnerabilities remain, increasing risk. Changes are required to introduce modern methods, like DevSecOps and continuous compliance.

Likewise, the lack of reciprocity for ATOs among government agencies leads to massive inefficiencies and a significant waste of scarce resources. At minimum, similar agencies should be grouped together with a defined ATO process overseen by an "Authorization Official of Common Concern" that would be accepted by all agencies in that group so that once an environment is granted an ATO, it is acceptable to all.

That being said, the Department of Defense's Continuous ATO (cATO) initiative, launched in February 2022, recognizes the shortcoming of reactive processes, such as scanning and patching, and looks to provide continuous monitoring and evaluation of an environment's actual threat posture. Organizations need to think about and address the problem in a similar fashion.

ICIT:
Could you give some examples of where you think government and industry are working well together?

Kapinos:
The Joint Cyber Defense Collaborative (JCDC) housed within CISA is an example of a public-private partnership positively impacting the cyber threat landscape. Initially established with a handful of key industry partners, it now includes 21 major cyber companies. Recently, a dozen major industrial control system (ICS) companies were added to focus specifically on that critical sector.

The CISA Known Exploited Vulnerability Catalog is another great example. It is a government-provided resource to help organizations leverage and prioritize their patching and vulnerability remediation efforts. It also informs risk assessments based on known activity. Additionally, the NSA, CISA, FBI, and International Partners publish joint cybersecurity advisories that provide detailed technical information on the latest emerging threats. The private sector leverages this

information to greatly enhance the availability and coverage of Indicators of Compromise (IOCs) as well as to enrich threat intelligence and threat hunt activities.

Last, the NSA's Cybersecurity Collaboration Center (CCC) continues to expand its relationships with industry and interagency partners to reduce the attack surface across the defense information base DIB. This activity helps ensure that sensitive US intellectual property, military research, and innovative technical economy are protected at scale in cyberspace. The CCC also provides free commercial cybersecurity services to scale protection to small and medium-sized businesses for broad impact.

These beneficial collaborations enhance the detection and response capabilities of defenders. We encourage the US government to consider making similar efforts to improve companies' recovery and resilience capability.

ICIT:
What are some advantages of technology modernization that are often overlooked?

Kapinos:
IT modernization budgets are insufficient to support the level and pace of change needed. Transitioning to the cloud, a government priority, uses less electricity. This fact should be recognized and potentially used to justify additional funding. In cases where the change will drive a significant improvement in energy efficiency, allocating funding from energy initiatives may be appropriate and accelerate the modernization timeframe. The Federal Government could implement this idea via tax incentives available through the recently passed Inflation Reduction Act.

By modernizing applications to be cloud native, we are future-proofing the technologies while exercising the benefits of on-demand resource management that consumes little to no energy while sitting idle for extended periods. Conversely, staying on old platforms which utilize archaic programming languages with a shrinking talent pool creates a resource scarcity issue, increases costs, and puts critical systems at operational risk. Better cost-benefit analyses that include energy utilization will identify these discrepancies and justify these systems' modernization or retirement.

ICIT:
How do you see automation and machine learning impacting the workforce, and what steps could the government take to adopt them?

Kapinos:
A workforce strategy is required to understand and address the impact of automation replacing more functions within the cyber workforce. Advances include Robotic Process Automation (RPA) and Security Orchestration Automation and Response (SOAR). However, these technologies have just begun to roll out and will take a significant amount of time before they fully displace workers.

Any strategy also needs to be able to evolve over time. The National Cyber Workforce and Education Strategy, which National Cyber Director Chris Inglis is developing, could focus on this. Ideally, it should understand the timing and sequencing of these changes and work to upskill impacted employees into related areas, keeping cyber talent productive and in the workforce. Oftentimes, this last part is ignored, but it is imperative that new strategies work to incentivize and enable the workforce to train up to and take on the most significant challenges.

For example, analytics and automation are making huge gains in security operations centers, providing opportunities to upskill team members and pivot those existing resources to tackle other critical functions. These analysts have technical skills and are already government employees; a concerted plan and the development of the associated training necessary to upskill them into areas where significant talent shortages exist, such as red teaming and threat hunting, would greatly benefit everyone.

Automation and machine learning also provide significant opportunities to derive insights from data that might never get reviewed or that human analysts might not spot. Thus, the Federal Government should continue to develop a focused machine learning and artificial intelligence strategy. This could be a product of the National AI Advisory Committee (NAIAC), which is another area of significant potential for public and private collaboration.

ICIT:
Are there other workforce initiatives that could enhance the cyber talent pipeline?

Kapinos:
The July National Cyber Workforce and Education Summit at the White House led to substantial commitments that should positively impact our cyber workforce. We should continue to look for ways to increase the pathways to cybersecurity careers, as many currently require a four-year degree that does little to prepare individuals for the actual problems they will face in the workplace.

A trade-focused high school pathway with four years of work experience will greatly increase the competency of cyber defenders. Increasing the scale of vocational high schools with a cybersecurity path for their students and incentivizing industry to support this path through internships and subject matter experts (SME) guidance to the vocational programs will be beneficial. It should be much easier to involve cybersecurity SMEs as adjunct lecturers, course developers, etc., at the vocational high school level than at the university level. This would also significantly decrease the cost of entry into the cybersecurity profession, making the career more desirable to diverse communities. Likewise, increasing the number of community colleges that offer associate degrees in cybersecurity will make cybersecurity careers easier to embark on while decreasing the costs and potentially increasing the cybersecurity workforce's proficiency.

ICIT:
How do we bring this all together?

Kapinos:
The "How did we get here?" section of the 2018 National Cyber Strategy's introduction addresses challenges that still exist today and have only further deteriorated. This unfortunate reality is not due to a lack of progress but rather defense being outpaced by our adversaries' progress.

As we implement ongoing strategic initiatives and undertake new efforts, the focus should shift to ranked order policy changes which will drive effects and desired outcomes. Results need to be measured to validate we are properly applying scarce resources. Organizations that establish a track record of success should be recognized as early adopters. Their framework and experience should be used to allow other companies to apply resources in the areas that drive the most benefit. Similarly, supporting efforts must be analyzed to identify inefficiencies, offer process improvements, and reduce resource requirements.

We cannot continue to focus on building out the new without revisiting longstanding efforts to identify how they fit - or do not fit - into the new frameworks that are being developed.

ICIT:
What would you like to share about ManTech's Cyber capabilities?

Kapinos:

ManTech has a long history of providing full-spectrum cyber capabilities to support our customers' missions. Throughout our history, we have been innovators in the offensive and defensive cyber arena. Our contributions include significant advances in Cyber Network Operations (CNO), insider threat, cybersecurity operations, threat hunting, cyber analytics, and computer and mobile forensics across the Federal Government.

We leveraged our expertise in these areas to create differentiated training offerings. These started with our Advanced Cyber Training Program (ACTP) for CNO developers and extended to other topics where we have identified workforce shortages. Through these offerings, ManTech can upskill engineers and increase the talent pool to meet customer missions.

We champion communities of practice, so ManTech's SMEs have a venue to share and learn from each other's experiences. Our Cognitive Cyber community combines our offensive and defensive cyber expertise and enables our differentiated approach to offense-informed defense.

Within ManTech's Innovation and Capabilities Office (ICO), our technology investments are centralized through five technology focus areas (TFAs). These TFAs, Cognitive Cyber, Mission & Enterprise IT, Analytics, Automation and Artificial Intelligence (A^3), Intelligent Systems, and Data at the Edge. These topics represent key investment areas we believe will best drive value for our customers. For example, combining our Cognitive Cyber and A^3 focus areas enables cyber defenders by operationalizing cyber telemetry to derive insights into today's complex

environments, such as hybrid multi-cloud enterprise architectures. We understand that collecting telemetry only adds value if the defenders can quickly operationalize, and that it is often easier for organizations to collect information than to follow through on the data.