INTELLIGENCE INSIGHTS

EXPERT INSIGHTS ON NATIONAL SECURITY DEVELOPMENTS

MARCH 2023

Industry Contributions to U.S. Government Offensive Cyber Operations

PRESENTED BY INSA'S CYBER COUNCIL

CYBER COUNCIL

OVERVIEW

To continue mitigating and addressing cyber threats and vulnerabilities, the United States needs to counter cyber threat actors proactively through both preemptive actions and retaliation. "Preemptive actions" could take the form of offensive cyberattacks that disrupt an adversary's capabilities, influence operations, heightened surveillance to provide warning of a pending attack, or other initiatives that undermine adversaries' ability to launch effective cyberattacks before such assaults begin.[1] Offensive retaliatory measures could include counter-attacks against an aggressor and private actors' efforts to recover stolen data.

Private sector networks have been the target of many cyberattacks. Some cause minor disruptions to corporate operations; others take capabilities offline for extended periods of time. Some attacks – particularly those designed to steal information – affect only the targeted organization, while attacks on critical infrastructure can disrupt energy supplies, healthcare, and other essential services on which civilians depend.

The United States has more than 12 million technology workers, with more than 1.1 million working specifically in cybersecurity.[2] Commercial companies across the U.S. economy employ millions of cyber experts who are able to secure their information technology infrastructure and understand threats against it. Companies in the Defense Industrial Base (DIB), which provide the military and other national security agencies with critical equipment and services, are high-profile targets for foreign adversaries. They also have extensive in-house cyber expertise, which they provide to government agencies for a wide range of missions.

Given their significant cyber workforce, DIB companies and other commercial corporations are well positioned to assist the government in executing offensive operations, implementing retaliatory cyber actions, or facilitating information-sharing with public and private organizations. Providing such assistance to the government could help prevent attacks on their own networks and enhance government's ability to recover stolen data, mitigate damage, and restore critical services in the wake of an attack. How might industry help bolster U.S. government cyber capabilities given statutory limitations, legal authorities, and risks?

While the cyber community has extensively debated the wisdom of, and options for, industry involvement in offensive cyber operations against cyber actors, clear options have not (yet) materialized. INSA recommends several options for industry engagement, principally through public-private collaborative efforts led by multiple government agencies. Specifically, INSA proposes:

- Augmented Cyber National Guard and Reserve forces, or even a centralized Cyber National Guard, to help the military and state and local governments with incident response;
- A Defense Department National Digital Reserve Corps to augment the capabilities of federal agencies, as proposed by legislation in the House of Representatives;
- A Corporate Cyber Reserve that would allow companies to contribute cyber capabilities and resources to government-led incident response efforts;
- A private sector advisory council to help U.S. Cyber Command and its components understand foreign network targets; and
- A whole-of-nation "Cyber Manhattan Project" to harness technical innovation and help the United States stay ahead of its adversaries' cyber capabilities.

AN EXPANDING CYBER THREAT

Cyber threats are increasing on a global scale – from nation states to hacktivists. Threat actors have access to easily accessible offensive toolkits on the dark web and use highly sophisticated supply chain cyber operations, as demonstrated by the Solarwinds and Log4j attacks. Coupled with the exponential growth in potential attack vectors due to the proliferation of digital technologies and the internet-of-things, the United States must increase its capability to anticipate and counter a wide breadth of cyber threats, especially against civilian critical infrastructure.

These response efforts are complicated by states' use of cyberattacks to advance national security objectives in conflict and the shift from "traditional" combat to warfighting that involves both kinetic and cyber weapons. The Russia-Ukraine War offers a glimpse of the future of such hybrid warfare. As Sergey Shykevich, Threat Intelligence Group Manager at Check Point, a U.S.-based cybersecurity firm, said of the Ukraine war, "for the first time, we've seen coordination between cyberattacks and kinetic military assaults."[3] Mykhailo Federov, Ukraine's deputy prime minister and minister for digital transformation, stated in September 2022 that the conflict engulfing his nation "is the world's first cyber war."[4]

Data supports these claims. Check Point noted that the first three days of the Ukraine war in February 2022 coincided with a "196% increase in cyberattacks on Ukraine's government and military sector," and that the number of attacks doubled again in the subsequent six months.[5] In April 2022, Microsoft reported that Russian cyber operations in Ukraine in the first six weeks of the conflict attacked hundreds of targets in both government organizations and civilian critical infrastructure, and that Russian cyber operations were undertaken to complement kinetic action.[6]

HOW CAN THE UNITED STATES RESPOND?

Countering existing, emerging, and innovative cyber threats requires a whole-of-nation effort in which civilian government agencies, the U.S. military, and the private sector provide resources and capabilities. The United States needs a "toolkit" that includes both defensive and offensive capabilities to mitigate debilitating attacks on private U.S. companies – both commercial companies that develop highly valuable technologies of interest to U.S. adversaries and the privately owned and operated critical infrastructure that provides services vital to health, safety, and economic activity.

IS "HACKING BACK" A VIABLE STRATEGY?

Some companies advocate "hacking back" against attackers – either to retaliate or to reclaim the data that was stolen – but such steps are unlikely to achieve their goals and are, under current law, illegal. The Computer Fraud and Abuse Act of 1986 imposes criminal penalties for accessing another entity's computer network.[7] U.S. legislators have introduced bills that would modify this law's provisions to allow hacking back, but none have passed into law. One example, the Active Cyber Defense Certainty Act (ACDC), would have empowered companies to use beacons to track and recover stolen data. The bill failed to pass in both the 115th and 116th Congress. In June 2021, two senators introduced a bill – the Study on Cyber-Attack Response Options Act – directing the Department of Homeland Security to conduct a study on the risks and benefits of allowing private companies to respond proportionately to an unlawful network breach, subject to federal oversight; the bill died in Committee.[8]

Most companies would be averse to hack into the networks of likely perpetrators for fear of retribution and concerns about both civil and criminal liability. For example, a victim company hacking back could target the wrong entity, given the difficulty of accurately attributing culpability for cyberattacks. Furthermore, such a company could (even inadvertently) illegitimately acquire information of value, damage networks or data, or violate the laws of the United States or the country in which the adversary's network is based, any of which would expose the company to legal liability. Even if a victim company's sole goal is to take back its stolen data, it cannot guarantee that the data hasn't already been copied, stored elsewhere, sold, or disseminated. Companies' best chance of recovering stolen data or resources is to collaborate with federal law enforcement agencies, which have a range of legal authorities to track down and recoup the lost assets.[9]

RECOMMENDATIONS

How can U.S. industry's cyber workforce and expertise help the United States bolster offensive capabilities whose existence deters cyberattacks? In many ways, the best way for the private sector to contribute to cyber offense is to contribute to defensive measures like enhanced cyber resiliency and robust incident response capabilities. Such steps would help free up federal government resources for other initiatives (including offensive operations). Furthermore, enhanced capabilities to restore critical infrastructure services could deter attacks on U.S. infrastructure by reducing the impact – and thus the value – of disruptive attacks.

Under certain configurations, private sector cyber experts could also assist offensive cyber operations, defensive cybersecurity, and incident response as needed. Just as citizen-soldiers in the National Guard contribute, under different circumstances, to civil support missions at the state level and combat operations at the federal-level, cyber experts could similarly be mobilized by different levels of government for different missions, depending on the need.

The range of companies in the American economy with assets worth protecting and skilled workers who could be brought to the task is enormous. Some may be willing to be proactive, while others will not; some will be willing to take risks, while others will not. Given this diversity of approaches to a shared threat, some government coordination will be needed to provide both a policy framework and structure to private sector efforts. In addition, since offensive cyber activities are generally illegal for private actors to undertake, government sponsorship of private citizens' contributions through government institutions will provide a legal framework for their engagement.

INSA recommends several options for consideration:

- **EXPANDING CRITICAL INFRASTRUCTURE VULNERABILITY ASSESSMENTS:** Under the auspices of the Cybersecurity and Infrastructure Security Agency (CISA), private infrastructure operators and sector-specific Information Sharing and Analysis Centers (ISACs) already assess weaknesses in U.S. networks that need to be patched or protected. To apply infrastructure expertise to offensive goals, U.S. Cyber Command (CYBERCOM) should expand its "Under Advisement" program, in which members of the Command's Cyber National Mission Force (CNMF) share threat information with companies,[10] from a purely defensive focus to one that uses U.S. companies' experiences to identify vulnerabilities and points of failure in foreign countries' critical infrastructure. While it is unlikely CYBERCOM would target a foreign country's agricultural or healthcare sectors to advance national security goals, critical infrastructure that supports an adversary's military capabilities – such as energy or transportation – could be legitimate targets in a conflict. Participating companies would require legal indemnification for their support – both from the risk of lost business if a company's ties to CYBERCOM were to be revealed and from the risk that a U.S. company could be sued for damages caused by U.S. military actors who benefited from the company's assistance.

- **EXPANDING NATIONAL GUARD AND RESERVES CYBER FORCE STRUCTURE:** The Secretary of Defense and Secretary of Homeland Security should expand the cyber force resident in the National Guard and Reserves that would be responsive to cyber needs across the United States. Many Guardsmen and Reservists have critical cyber skills from their day jobs that can enhance the military's cyber defense and response capabilities. Alternatively, the government could establish a new stand-alone Cyber National Guard with authorities modeled after those of the U.S. Coast Guard, which operates under the Department of Homeland Security (DHS) but can transfer under the Defense Department's command during wartime. A Cyber National Guard under DHS could use DHS legal authorities to assist with domestic needs, such as bringing critical infrastructure back online after a cyberattack, and transfer to the Department of Defense in time of war to bolster its cyber missions. As with the existing National Guard and Reserves, companies would be required to preserve the jobs of employees who are activated for duty. The National Guard Bureau currently oversees Cyber Protection Teams in 31 states and territories[11] who are positioned to help state and local officials restore critical services.[12] However, as cyberattacks can often have multi-state impacts, a nationwide cyber response capability would provide greater capacity to surge wherever needed.

- **CREATING A NATIONAL DIGITAL RESERVE CORPS:** Whereas a Cyber National Guard could draw on civilian expertise to augment military capabilities and assist state and local authorities, a civilian cyber reserve corps could augment federal government capabilities. In January 2023, two House members introduced bipartisan legislation to create a National Digital Reserve Corps whose members could be mobilized for 30 days or more annually to augment the cybersecurity capabilities of federal agencies.[13] Such experts, who would receive additional training and certification under the program, could help agencies develop and implement cybersecurity services, education and training, data triage, and technical solutions, and – given their full-time roles in the civilian sector – bridge public needs and private sector capabilities. Such a proposal would enable civilians with needed cyber skills to assist the federal government with minimal inconveniences to their employers, who are already accustomed to military reservists taking short absences for deployments These civilians could serve in supporting roles to the military personnel who "pull the trigger" on offensive cyber operations; they could also be assigned to support defensive missions as well.

- **LAUNCH A CORPORATE CYBER RESERVE:** CISA could coordinate a Corporate Cyber Reserve capability in which companies could designate a portion of their network capabilities and cyber workforce to be made available to the government during crises. Such a model would be based on the Government's Civil Reserve Air Fleet (CRAF), which allows the U.S. government to requisition planes from commercial airlines when additional aircraft are required.

- **REVOLUTIONIZE INNOVATION THROUGH A CYBER MANHATTAN PROJECT:**
  The National Defense Strategy calls for integrating U.S. and allied capabilities across all warfighting domains, a concept called Integrated Deterrence (ID). However, ID does not include the private sector even though a large portion of the 21st century battlespace consists of private sector networks. Industry must be part of the ID solution. As new technologies like artificial intelligence, machine learning, and quantum computing change the nature of cyberwarfare, the United States and its allies must bring together its leading computer scientists, cyber strategists, and hackers to create new, innovative solutions that enable coalition partners to stay ahead of adversaries on both cyber defense and cyber offense. In a geographically-distributed Cyber Manhattan Project, government and industry experts could apply lessons from past cyber successes and insights into emerging technologies to exceptionally challenging problems.[14] Leading technology companies would need to provide financial, technical, and human capital support to such an effort.

CONCLUSION

The global digital revolution has increased the cyber vulnerabilities of private sector entities in the United States. Ensuring the resiliency of U.S. critical infrastructure is necessary to protect Americans' health, safety, and economic activity. Protecting U.S. companies' valuable intellectual property preserves jobs and financial investments and prevents advanced technologies from being stolen by military adversaries and economic competitors. In short, the defense of critical infrastructure and commercial networks is a national imperative for maintaining the United States' economic prosperity and national security.

But defense is not enough. While no legal framework exists to allow private corporations or individual citizens to engage in offensive cyber operations on their own, contributions made under the rubric of new policies, legislation, and organizational frameworks could help enhance the nation's offensive cyber capabilities. In augmenting government capabilities, the U.S. private sector can secure its own assets, increase the country's cyber deterrence capability, and protect U.S. technological and economic competitiveness.

REFERENCES

[1] Thanks to guest speaker Dr. John Arquilla, Distinguished Professor and Department Chair at the US Naval Postgraduate School and renowned cyber expert and author, for sharing his views at the August 1, 2022, meeting of INSA's Cyber Council.

[2] Steve Morgan, "Cybersecurity Jobs Report: 3.5 Million Openings in 2025," Cybercrime Magazine, November 9, 2021. At https://cybersecurityventures.com/jobs/. Also see CyberSeek, Cybersecurity Supply/Demand Heat Map, as of October 25, 2022. At https://www.cyberseek.org/heatmap.html.

[3] Serena Haththotuwa, "Weaponized Cybercrime: Learning from the Conflict in Ukraine," Business Leader, September 12, 2022. At https://www.businessleader.co.uk/weaponized-cybercrime-learning-from-the-conflict-in-ukraine/.

[4] Jaspreet Gill, "Ukraine, Rushing Into 'Digital Transformation,' Prepares for More Russian Cyber-Attacks: Officials," Breaking Defense, September 12, 2022. At https://breakingdefense.com/2022/09/ukraine-rushing-into-digital-transformation-prepares-for-more-russian-cyber-attacks-officials/.

[5] Haththotuwa, September 12, 2022.

[6] Microsoft, Special Report: Ukraine – An Overview of Russia's Cyberattack Activity in Ukraine, April 27, 2022, pp. 2, 4, 10. At https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

[7] Computer Fraud and Abuse Act, 18 USC § 1030 (1986). At https://www.congress.gov/bill/99th-congress/house-bill/4718/text.

[8] See Corey Nachreiner, "The Pros and Cons of the Proposed Hack Back Bill," SC Media, January 28, 2022. At https://www.scmagazine.com/perspective/policy/the-pros-and-cons-of-the-proposed-hack-back-bill.

[9] Speakers with senior-level experience in intelligence, law enforcement, and military organizations shared these insights at a meeting of INSA's Legal Affairs Roundtable on April 19, 2019.

[10] Mark Pomerleau, "Cyber Command Creates Forum with Industry to Share Threat Information," FedScoop, May 5, 2022. At https://fedscoop.com/cyber-command-creates-forum-with-industry-to-share-threat-information/.

[11] Capt. Clarissa Estrada, "Virginia National Guard Brigade Makes History at Cyber Shield 2022, the DoD's Largest Unclassified Cyber Defense Exercise," DVIDS, June 15, 2022. At https://www.dvidshub.net/news/423114/virginia-national-guard-brigade-makes-history-cyber-shield-2022-dods-largest-unclassified-cyber-defense-exercise.

[12] Sgt. 1st Class Jon Soucy, "Guard Set to Activate Additional Cyber Units," National Guard Bureau News, December 9, 2015. At https://www.nationalguard.mil/News/Article/633547/guard-set-to-activate-additional-cyber-units/. See also National Guard Bureau Office of Public Affairs, "National Guard Defends the Cyber Front," June 14, 2022. At https://www.ang.af.mil/Media/Article-Display/Article/3061816/national-guard-defends-the-cyber-front/. See also Alex Ebrahimi, et. al., "National Guard Cyber Protection Teams as a Response to Cybersecurity Threats," unpublished paper, June 2020. At https://cci.calpoly.edu/sites/default/files/2021-05/NGCPT_6.30.20.pdf.

[13] See Rep. Robin Kelly, "Representatives Robin Kelly, Tony Gonzales Introduce Bill to Form National Digital Reserve Corps," press release, January 11, 2023. At https://robinkelly.house.gov/media-center/press-releases/representatives-robin-kelly-tony-gonzales-introduce-bill-form-national. Proposals to create the National Digital Reserve Corps were included in the versions of the FY2022 and FY2023 National Defense Authorization Acts (NDAA) passed by the House but were dropped both times before the bills were signed into law. See Lamar Johnson, "FY2022 NDAA Passes House with a Number of Tech Amendments," MeriTalk, September 24, 2021. At https://meritalk.com/articles/fy2022-ndaa-passes-house-with-a-number-of-tech-amendments/. See also Lauren C. Williams, "A Look at Tech Amendments in the FY2023 House NDAA," DefenseOne, July 15, 2022. At https://www.defenseone.com/defense-systems/2022/07/look-tech-amendments-2023-house-ndaa/374555/.

[14] Arquilla, INSA Cyber Council meeting, August 1, 2022.

INSA

INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

ACKNOWLEDGEMENTS

INSA expresses its appreciation to the INSA members and staff who contributed their time, expertise, and resources to this paper.

INSA MEMBERS

Jim Keffer, *Cyber Council Chair*

Steve Orrin, *Cyber Council Vice Chair*

Harry Brooks, *Guidehouse*

Moon Yousif Sulfab, *Virginia Polytechnic Institute*

Laura Yoeckel-Kelly, *Booz Allen Hamilton*

Samuel Visner, *MITRE*

INSA STAFF

Suzanne Wilson Heckenberg, *President*

John Doyon, *Executive Vice President*

Larry Hanauer, *Vice President for Policy*

Peggy O'Connor, *Director of Communications and Policy*

Om Narayanan, *Intern*

Hans Kuppers IV, *Intern*

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit trade association dedicated to advancing collaborative, public-private approaches to intelligence and national security priorities. Through the application of industry expertise, leading-edge academic research and commercial best practices, INSA seeks to make the Intelligence Community more effective and efficient. INSA's 160+ member organizations and 4,000+ individual and associate members include senior executives and intelligence experts in the public, private and academic sectors.

ABOUT INSA'S CYBER COUNCIL

INSA's Cyber Council seeks to fuse knowledge from industry, government, and academic experts in order to provide authoritative and influential insights regarding the national security challenges present in the cyber domain. The Council works to promote a greater understanding of cyber threats, challenges, and opportunities that can be addressed effectively through public-private collaboration.