Naval War College Foundation

Center for Cyber Conflict Studies

U.S. Naval War College

PROCEEDINGS

National Security of U.S. Federal Government Agency Networks

Third Annual Cybersecurity Roundtable Forum
Capitol Hill Club, Washington, D.C.
April 12, 2016

On behalf of the U.S. Naval War College Center for Cyber Conflict Studies, the Naval War College Foundation convened a national group of U.S. leaders, subject matter experts, and practitioners for cybersecurity and federal network resiliency. Distinguished participants included current and former Members of Congress; active duty and retired U.S. military flag and senior officers; senior directors in the Intelligence Community; senior civilian government officials; academic and policy leaders; and cybersecurity executives and information security officers from the finance, information technology, and defense contracting sectors of the business community.

The Forum took place amidst an increasingly mainstream debate in Washington and across the country about the role of government in protecting both federal government and private sector networks from an array of sophisticated cyber threats. Notwithstanding the time constraints of a four-hour format, many key issues and questions were tabled and addressed with preliminary findings and recommendations offered. These are grouped below by the Core Themes considered by the Forum, including for each theme a review of:

- Key Issues
- Overviews of the Discourse
- Key Stakeholders
- Representative Unattributed Quotations
- Preliminary Recommendations

A key purpose of the Forum was to develop actionable recommendations for the incoming President of the United States and Members of the U.S. Congress to address the Nation's cybersecurity vulnerabilities. The Forum recommendations are documented in these Proceedings and reflect the considerable expertise of leaders and subject matter experts in the public and private sectors.

Companies & Organizations Represented

Private Sector Industry & Cybersecurity

Addx Corporation
AECOM Management Services
AGC Partners
Amazon
Beacon Global Strategies
Boeing Defense, Space and Security
CACI International, Inc.
CounterTack
CSRA
General Dynamics Information Technology
Kirby Capital Advisors
Locke Lord, LLP
Lockheed Martin Corporation
NetApp
Northrop Grumman
Palantir Technologies
Palo Alto Networks
RadiantBlue Technologies
Raytheon Company
Schiff Hardin, LLP
SHIELD Capital Partners LLC
Sotera Defense Solutions, Inc.
United Technologies Corporation
U.S. Bank

Military, Intelligence, Government, Policy & Academia

Business Executives for National Security
The Fletcher School of Law and Diplomacy, Tufts University
National Security Agency
Naval War College Foundation
Navy League of the United States
New Jersey Office of Cybersecurity
The Rhode Island Cybersecurity Commission
Security Innovation Network
United States Army Cyber Institute
United States Department of State
United States House of Representatives
United States Naval War College
U.S. Cyber Command
U.S. Fleet Cyber Command, U.S. 10th Fleet, U.S. Navy
United States Senate

NAVAL WAR COLLEGE FOUNDATION

The Core Themes and related findings and recommendations include:

I. Governance, Leadership, and Trust

Key Issues

- Centralizing federal cybersecurity strategy, execution, and organizational structure
- Establishing role and authority for newly-created position of Federal Chief Information Security Officer (CISO)
- Instituting private sector board accountability for cybersecurity
- Restoring an institutional culture of trust between government and private sector companies and citizens

Overview of the Discourse

The Forum discussed leadership and strategy as a broader challenge of U.S. cybersecurity, indicating that the problem is not solely technical or tactical. Coordinated Executive Branch leadership is needed to develop a coherent cyber defense strategy. Presently, there is no clearly defined leader in federal government cybersecurity policy, nor is there consensus about what the government can realistically accomplish.

A positive development is that some silos and barriers within the federal government are coming down, allowing government to collaborate increasingly with the private sector. Informal relationships between agencies and companies have assisted coordination, but must be reinforced with institutional processes.

The Forum expressed concerns about the effectiveness of Department of Homeland Security (DHS) leading national cybersecurity. DHS is by charter responsible for the federal civilian government's cybersecurity. However, DHS has struggled to organize itself to accomplish its cybersecurity mission to secure non-military federal systems, to protect critical infrastructure across the Nation, and to disseminate cyber threat information and analyses.

The Forum's Congressional delegation tabled the suggestion that the incoming President of the United States should establish a mechanism to plan ahead for the future organization of national cyber defense for federal civilian agencies. The Congressional delegation recommended that the next President should review federal cybersecurity strategy and organizational structure to ensure coordination of currently overlapping but uncoordinated authorities. The Office of Management and Budget was noted as having a potentially useful role in this process.

The recently proposed establishment of a Federal CISO is a long-overdue step in the evolution of how government organizes itself for cybersecurity. Next steps will be for White House leadership to decide the authorities this appointee will possess to drive change across government as a whole. A key challenge will be for the CISO to build alliances throughout the federal government. Relatively low government compensation levels (that contrast with the high performance accountability demanded of the position) will challenge recruiting top talent for this position.

As for the private sector, the Forum agreed that cyber expertise is strongly needed at the corporate board level. Boards need informed expertise to evaluate cybersecurity strategies, risk assessments, and investments with measurable scale. Corporate boards have been actively recruiting for cybersecurity expertise in board hiring, but most lack this expertise. The Forum discussed whether legislation or regulation should be enacted to compel publicly traded companies to inform shareholders of the status of cyber expertise present on corporate boards. There was general consensus that the Securities & Exchange Commission (SEC) should require such disclosure at a minimum.

The successes in the Defense Industrial Bureau and the Financial Sector Information Sharing and Analysis Center (FS-ISAC) provide relevant examples of successful information sharing on cyber threats. The Department of Treasury created a cyber intelligence group tailored for information sharing between government and banks, and the financial sector also receives monthly threat briefings from many federal agencies. The FS-ISAC for the financial sector is reputed to be among the most integrated among all ISACs. The Forum agreed that increased information sharing and partnerships strengthen cyberspace security and must be accelerated further for national resilience.

Key Stakeholders

- Federal Government: Executive, Legislative and Judicial Branches
- Military, Intelligence Agencies: NATO, DOD, DIA, NSA, CIA, FBI, Secret Service
- Cabinet Departments: Homeland Security, Treasury, Justice, State
- State and Local Government: National Guard, Law Enforcement
- Private Sector: Information Sharing and Analysis Centers (ISACs)
- Public Policy: Academia, Advocacy
- Foreign Partners: Private and Public

Representative Quotes

"The government must prove that promises can be kept. In this space, there is no amount of energy put into trust that isn't worth it."

"There is a lack of clarity in terms of who is the lead sled dog here… we shouldn't underestimate industry."

“We need focused, intense management of national cybersecurity policy and execution. We need someone in charge to implement with authority.”

“Compliance does not equate to risk management. There is too much focus on compliance.”

“For cyber at the corporate board level, you need measurable and monitorable scale, not another check in the box.”

Recommendations

1) Conduct Presidential review of federal cybersecurity strategy and organizational structure to centralize investigative and policy authorities currently distributed between multiple overlapping and uncoordinated agencies (DHS, DOJ, FBI, Secret Service).

2) Upgrade the Federal CISO position to be a Senate-confirmed position with policy and budget authority, and mandate that all agency CISOs report directly to the Federal CISO to coordinate cybersecurity implementation across all civilian agencies.

3) Establish in a single office a specialized Inspector General for Cybersecurity to evaluate federal agency vulnerabilities with corrective authorities that go beyond compliance certification.

4) Instruct DHS to prioritize the critical infrastructure sectors and provide clearances in order of priority to share threat intelligence and review and test critical infrastructure against the NIST framework.

5) Direct the Securities & Exchange Commission to require businesses to disclose status of board-level cyber expertise via the SEC Form10-K.

6) Promote the FS-ISAC in the financial sector as the model for security and information sharing partnerships for other business sectors.

7) Create market incentives for insurance companies and other industry groups to collaborate with government to develop accurate cyber risk actuarial data that will promote development of a private sector cybersecurity insurance market.

II. Attribution and Deterrence

Key Issues

- Expediting and authenticating attribution of cyber-attacks with USG agencies
- Deterring cyber aggression when retribution risk is low
- Evaluating effectiveness of legalistic versus technical or kinetic responses
- Addressing lack of any deterrence regime between allied countries

Overview of the Discourse

The Forum discussed a recently published finding that state-sponsored cyber activity has increased from one attack every 32 minutes to one attack every 16 minutes from 2014 to 2015. In addition to China, Russia has expanded state-sponsored economic cyber espionage and operations.

Various other state and non-state actors have escalated attack frequencies, sophistication, methods, and techniques. While the U.S. federal government has improved its detection capabilities over time, the private sector is shouldering the majority burden of the Nation's cyber defensive efforts.

One of the primary causes of increased state-sponsored activity is the absence of a deterrence regime led by the United States. Rational state actors (nation states conducting cyber espionage and offensive operations) are operating in cyberspace with nil expectation of retribution. This is due to both technical limitations of attribution and political limitations of national policy and political will.

The United States and allied governments often lack sufficient capabilities to quickly and definitively attribute the source of cyber-attacks. Furthermore, the United States lacks a clear and transparent policy doctrine regarding justifiable responses to cyber aggression against American businesses or government agencies.

The United States has taken modest recent steps to signal a decreasing tolerance for cyber aggression – most notably the recent indictment of Iranian hackers and, in 2014, the indictment of five officers from China's People's Liberation Army (PLA). Such legal actions demand extensive coordination among the Intelligence Community, the Department of Justice, and the White House National Security Council.

The Forum questioned the effectiveness of legal sanctions in deterring cyber attacks by China, Iran or other state actors, noting that a more consequential response will be necessary to alter the strategic calculus of America's cyber adversaries.

Key Stakeholders

- President of the United States and National Security Council
- Department of Defense, U.S. Military, and Intelligence Community
- Department of State
- Department of Treasury
- Department of Justice, FBI, Law Enforcement
- U.S. Congress
- Allied Governments
- Private Sector

Representative Quotes

"Improving the state of our Nation's cyber defenses and giving prosecutors and investigators the tools they need to fight cybercrime have been among our top priorities in Congress."

"We cannot deter if we cannot attribute. Attacks that are prevented should also provide attribution. Then, we must decide how to deal with adversaries."

"Government's most important role in the cybersecurity space is attributing attacks."

"The indictment of Iranian hackers sent a clear message that the U.S. is going after whoever hacks us."

"Legal remedies by the DOJ alone will not protect us from cyber-attacks by China, Iran, North Korea, and Russia."

"There is not enough emphasis on U.S. cyber offensive capabilities."

"We should examine models that let ordinary citizens come to their country's aid…a cyber-adapted form of militias…bringing private sector expertise to bear in times of crisis."

"We need a modern day 'letter of marque' for cyber policy from the President authorizing private interests to attack bad actors."

Recommendations

1) Establish rules of engagement and clarify authorities of Department of Defense, the U.S. Military, and Intelligence Community for cyber offensive operations and deterrence purposes.

2) Direct Department of State to engage allied nations and the U.N. in forming a multilateral cyber deterrence regime.

3) Enact legislation to designate and penalize as federal offenses a) attacks on critical infrastructure, and b) trafficking in botnets & botnet access. Expand DOJ authorities to prosecute and shut down botnet networks.

4) Clarify U.S. policy for private sector rules of engagement for corporate intelligence gathering and self-defense against cyber attacks, to include a detailed response posture.

5) Authorize private companies a modern day "letter of marque" to conduct counter-offensive cyber operations against bad actors.

6) Review and revise communications and surveillance laws (particularly those enacted in a pre-Internet era) to ensure that private companies have legal tools to track network intrusions and locate data stolen from private networks.

III. Enhancing National Cyber Hygiene

Key Issues

- Developing the "gold standard" for best practices
- Managing overlapping frameworks and regulatory regimes
- Defining the role and responsibilities of government versus the private sector
- Developing public-private partnerships and information sharing
- Training human resources for collective resilience

Overview of the Discourse

The Forum noted the importance of establishing a national strategy to promote vigilant cyber hygiene. This includes enhancing user awareness of cyber threats, establishing guidelines for best practices, and adopting universal standards and protocols. Partnerships are critical to building institutional capacity, improving access to training and educational resources, and sharing information. On the latter, new innovations like the Cyber Threat Alliance (a community of competing vendors working to automate intelligence sharing in order to protect all Internet users) is representative of a growing sentiment that cybersecurity is a collective duty and a responsibility shared by both government and industry.

The Forum noted that cyber hygiene is not limited to implementing technical controls or improving awareness. The goal of enhancing America's cyber hygiene is to elevate barriers to entry for cyber threat actors. In this respect, our human resources are our first line of defense, and risk management frameworks are only one piece of the solution. America's academic posture at all levels of education is lagging behind the threat and capabilities of certain nations, notably in cybersecurity engineering and policy fields.

Finally, while industry continues to share cyber threat intelligence within various trusted communities of interest, government must streamline its processes for detecting and rapidly disclosing information on cyber threats and vulnerabilities to empower the public for self-defense. The government will never possess the scale to protect all Americans from each and every cyber attack. However, by serving as a conduit amongst the Intelligence Community, industry, and the general public, federal government agencies can facilitate greater access to cyber threat data.

Key Stakeholders

- Public and Private Sector
- Federal Government, including U.S. Congress & Executive Branch, particularly the Department of Homeland Security, Department of Defense, Military, and the Intelligence Community
- Private Sector ISACs (Information Sharing and Analysis Centers) for Critical Infrastructure Industries
- Information Technology and Cybersecurity Industry
- Academic Leaders

Representative Quotes

"The government has done a poor job communicating the scope and severity of the cyber threat to the American public. An educated public is the first line of defense in preventing cybersecurity incidents."

"We must decide what government can reasonably accomplish."

"We must ensure that future policymakers are armed with what they need and work on our archaic academic curriculum to include a cyber component."

"If there is one thing that government can do it is to make cybersecurity easier for the private sector. It's very difficult for the private sector to partner when they don't know whom to partner with."

"The human dimension of cybersecurity is critical. Endpoint users are the greatest vulnerability, so we must focus responsibility and accountability accordingly."

"Information sharing legislation was an important first step, but the government and the private sector can't solve this alone. There must be collaboration."

Recommendations

1) Establish a *National Cybersecurity Employee Pipeline Project (NCEPP)*, a national level program to address the present cyber skill gap. Such a program would: track the pipeline of potential cybersecurity experts in schools and universities; identify and market all programs within the U.S.; and promote cybersecurity as a career for young American students. NCEPP would be a public-private effort to:

    a) Offer national scholarships to programs that meet certain criteria.
    b) Incentivize commercial organizations to set up scholarships that support the NCEPP goals.
    c) Provide a mechanism for commercial and government organizations to communicate with these potential employees.
    d) Incentivize commercial organizations to recruit interns and employees.
    e) Partner with industry and academia to provide re-training centers for retiring and handicapped veterans.

2) Introduce cybersecurity engineering, technology, and policy courses across the educational continuum (secondary school to post-university graduate schools, including MBA & Executive Education programs for timely private sector implementation in businesses). Upgrade primary and middle school curricula with expanded information technology coursework and cybersecurity awareness.

3) Appoint a senior federal government official in the White House to de-classify and disclose cyber-attacks for the public's awareness in order to bolster cyber hygiene and preparedness for cyber-attacks.

4) Create market incentives for more businesses and industry segments to participate in cybersecurity communities of interest, such as Information Sharing and Analysis Centers (ISACs), in addition to those established for Critical Infrastructure Industries.

IV. Technology Modernization and Innovation

Key Issues

- Transitioning government's costly and vulnerable legacy information technology (IT) infrastructure to cost-effective, secure, scalable platforms in the Cloud
- Defending the expanding attack surface of Internet of Things (IoT)
- Moving beyond IT security and into operational technology (OT) security
- Reforming government acquisition process drastically to enable rapid innovation and technology adoption

Overview of the Discourse

The Forum identified the U.S. federal government's outdated IT infrastructure as a major security vulnerability. Resources are invested in system updates and patches, rather than modernization and upgrades. The $3.1 billion IT Modernization Fund, a component of the White House Cybersecurity National Action Plan, is an important first step towards phasing out obsolete and vulnerable systems across the federal government.

Cyber threats are growing as increasing autonomous systems and the "Internet of Things" (IoT) expand the attack surface and pose unprecedented kinetic threats. Government policy and process trends continue to be too focused on network security and do not account for weapons platform security.

Encryption is a vital security protocol standard for networks around the world. However, there is a lack of thought leadership and initiative in government to leverage the benefits of encryption. Failure to leverage such standards creates major disconnects with the security industry and hinders preparedness.

Finally, government does not move at a pace that is relevant to small businesses and startups. The Forum emphasized that government technology and IT acquisition reform is imperative. The standard requirement for proven past performance of vendors within the acquisition process was cited as a barrier to innovation, as start-up enterprises inherently lack past performance. Separately, there is a supply chain risk management issue with outsourced services, both network and data, that should be a consideration with regards to process and security.

The Defense Innovation Unit Experimental (DIUx) was cited as a new vehicle for innovation within the Department of Defense. The DIUx mission of building relationships between the Pentagon and innovation centers, like Silicon Valley and Boston Route 128, is critical to evolving national security. However, implementation to date has been ineffectual due to policy constraints, a confused mission, and the mismatch of career military personnel assigned to engage with highly entrepreneurial innovators in the marketplace. SECDEF Carter has acknowledged these constraints and recruited a new senior leadership team from Silicon Valley firms including Palo Alto Networks and Google. *(Note: Forum participant, Mr. Raj Shah, was subsequently appointed Managing Partner to lead DIUx in May 2016.)* The Forum recommended overhauling personnel and capital budget resources and governing authorities to allow DIUx to succeed in its mission of identifying partners and funding technology innovation.

In-Q-Tel (IQT) was cited as a model of success of bridging public and private sector innovation and capital. IQT is the Intelligence Community's venture capital firm that was created as an independent 501(3)(c) nonprofit corporation to bridge the gap between technology needs of the IC and emerging commercial innovation. A key success factor has been IQT's structural independence and autonomy in investment decisions and personnel management and its recruitment from the private sector.

Key Stakeholders

- Federal Government: Executive, Legislative, and Judicial Branches
- Military, Intelligence Agencies: DOD, DIA, NSA, CIA, FBI, NATO
- Cabinet Departments: Homeland Security, Treasury, Justice, State
- State and Local Government: National Guard, Law Enforcement
- Private Sector: Defense and Information Technology
- Public Policy: Academia, Advocacy
- Foreign Partners: Private and Public

Representative Quotes

"There are very significant national security ramifications as the digital world is a vector for crime and fraud on an international scale."

"The government should focus on what we stop doing rather than what we start doing."

"*We need a high speed acquisition process to chase a high speed technology process. This is not like buying a ship."*

"DHS bureaucrats should not attempt to learn the venture capital business by establishing a separate fund. DHS should work more effectively with In-Q-Tel."

The sales cycle to government currently takes too long. We need to get DoD to move at a pace that is relevant to small businesses and startups."

"One of the great strengths we have as a nation is venture-backed companies. Small and medium-sized companies will continue to lead in cybersecurity– But it needs to be easier for them to market cyber solutions to government; it generally takes four years."

Recommendations

1) Overhaul the government technology acquisition process and rules. Redesign for speed and time-to-market solutions. Remove barriers such as “past performance” requirement.

2) Revise government procurement and policy to address Operational Technology risks, including platform and weapon technology in cybersecurity strategy and processes.

3) Appropriate funding by Congress to overhaul existing IT infrastructure. Leverage the IT Modernization Fund to transition to new platforms (Cloud-based versus enterprise) rather than continue costly patch updates to outdated infrastructure.

4) Assign the management and accountability of the DHS / In-Q-Tel partnership to senior-most director levels (versus subordinates in the DHS bureaucracy) to ensure that innovative venture-backed technologies are identified and adopted by DHS.

5) Accelerate the transformation begun by SECDEF Carter of DIUx strategy, resource levels, and authorities to adequately empower this DOD initiative to bring innovation to the warfighter.

6) Develop a national cyber range (“sandbox”) with the private sector for R&D, exercises, and testing failures.

7) Employ war gaming simulations with the private sector as a vehicle for training and research, similar to the cyber simulation being hosted by the Naval War College with leading U.S. corporations in July 2016.

V. Concluding Remarks

The Chairman of the Naval War College Foundation Center for Cyber Conflict Studies Task Force, Philip Bilden, concluded the Forum by expressing gratitude to Admiral James Stavridis, USN (Ret.) and LTG Michael Flynn, USA (Ret.) for leading the Roundtable Forum participants through an informative exploration and constructive analysis of the National Security of U.S. Federal Government Agency Networks.

The Chairman expressed appreciation to the assembled leaders, including the entire Rhode Island Congressional Delegation, for their insights and recommendations for establishing a more coherent set of cybersecurity policies, practices, and initiatives. The Chairman thanked the distinguished participants and subject matter experts for contributing to actionable recommendations in service to the Nation's cybersecurity and resilience.

The Chairman noted that the Forum's findings and recommendations would be published in the Proceedings of the Naval War College Foundation Center for Cyber Conflict Studies Task Force and presented to the President of the United States, Members of the U.S. Congress, senior officials in the Department of Defense, U.S. Military and Intelligence Community, and private sector partners.

The Chairman encouraged all participants to continue an ongoing dialog with the Naval War College Foundation and the Center for Cyber Conflict Studies in addressing cybersecurity solutions and policy for their organizations, industry groups, and the Nation.

Subsequent to the Forum, Senator Whitehouse (RI) and Representative Langevin (RI) authored a Congressional letter of support of the NWCF Center for Cyber Conflict Studies Forum, outlining recommendations to be included in the Forum Proceedings. These will be included with Proceedings and presented to the President of the United States, Members of the U.S. Congress, and senior civilian and military officials.

Note: NWCF Center for Cyber Conflict Studies Task Force Proceedings and the Rhode Island U.S. Congressional letter of May 19, 2016 will be posted on The Naval War College Foundation website (http://www.nwcfoundation.org) for broad access by Forum participants and their respective colleagues in their organizations.