NAVAL WAR COLLEGE FOUNDATION

CENTER FOR CYBER CONFLICT STUDIES

U.S. NAVAL WAR COLLEGE

PROCEEDINGS

Cybersecurity of U.S. Financial Infrastructure

Cybersecurity Roundtable Forum
Army and Navy Club, Washington, D.C.
November 5th, 2014

The Naval War College Foundation (NWCF) convened its inaugural Cybersecurity Roundtable Forum on behalf of the Center for Cyber Conflict Studies at the U.S. Naval War College to address cyber threats to America's financial infrastructure and institutions. The Forum was attended by senior leaders from key stakeholder organizations across the public, private, and academic sectors. The Forum was chaired by NWCF's Center for Cyber Conflict Studies Task Force Chairman, Mr. Philip Bilden, and moderated by Admiral James Stavridis, U.S. Navy (Ret.) and Lieutenant General Michael Flynn, U.S. Army (Ret.).

More than forty distinguished attendees participated, including U.S. Senator Sheldon Whitehouse; former Massachusetts Governor and U.S. Presidential Candidate, Mitt Romney; Superintendent of the U.S. Naval Academy, Vice Admiral Walter E. "Ted" Carter; several active, reserve, and retired Flag and General Officers from three branches of the U.S. military; former senior officials from the National Security Agency, the Defense Intelligence Agency, and the Federal Bureau of Investigation; and senior executives and leaders, including company Founders, Chairmen, CEOs, and Chief Information Security and Risk Officers, from leading American corporate institutions across banking, credit unions, insurance, asset management, payments systems, capital markets exchanges, private equity, trade associations, cybersecurity, information technology & data systems, academia, and law.

The Forum marked the beginning of a national dialog on cybersecurity under the convening authority of the Naval War College Foundation. 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:

- Key issues and questions
- An overview of the discourse
- Key stakeholders identified
- Representative unattributed quotes
- Preliminary recommendations for further consideration by key stakeholders

The Core Themes and related findings include:

I. THREATS TO CYBERSPACE

Key Issues and Questions

- Defining the threats, the targets, and the bad actors
- Differentiating threats: cyber-attack; cyber-espionage; cyber-crime; cyber-terrorism
- Defensive measures: financial industry self-defense versus governmental shield across the continuum of preparation, active defense, mitigation, and recovery
- Offensive measures: proportionality, practicality, lethality, and legality

Overview of the Discourse

The Forum noted that cyberspace has become far more than the technology that gave rise to it, necessitating a consideration of the people and critical processes that are inextricably woven into it. Cyberspace has been called a domain in military terminology, differentiated from other physical domains of land, sea, air, and space. Cyberspace may be alternatively viewed as a globally-connected substrate, or medium, containing the wealth and treasure of individuals, sectors and nation-states. Regardless of its physical description, it is certain that cyberspace is, and will continue to be, both an object and a venue for conflict.

Cyberspace undermines at least three traditional barriers to conflict that defined nations' security frameworks for several centuries, notably: scale, proximity, and precision. Now with few resources and from a great distance, actors alone or in groups can determine at will the ***scale*** that they will use to attack or penetrate a target. These actors can overcome the ***proximity*** obstacle that used to limit serious conflict to neighbors or superpowers, and gather top quality intelligence or cause high value damage with minimal effort. Moreover, they can easily tailor their operations because the costly ***precision*** obstacle of industrial age conflict does not apply.

Cyberspace affords bad actors an unprecedented freedom of maneuver relative to the four traditional military domains of land, sea, air, and space. High thresholds in non-cyber domains encourage malicious exploitation of the fifth domain: cyberspace. Cyberspace's low barriers to entry allow, but do not require, commensurately low thresholds for responding to cyber aggression. Kinetic military force against a state or non-state cyber attacker may be an appropriate response of self-defense or retaliation to a cyber attack. The scale and severity of the cyber damage would likely influence the response, whether through cyberspace offensive action or through traditional military force. Data manipulation, for example, might call for a retaliatory use of kinetic force, especially if the victim serves vital national interests. Strategy and doctrine should account for the cumulative adverse effects of cyber-attacks that sometimes

escape the eye-grabbing attention of kinetic attacks. Few domestic or international norms govern the emerging, deeply-digitized world.

There is currently a significant disconnect between the threat to the Nation's critical infrastructure and the level of preparedness to protect and respond to sophisticated bad actors. Today's cyber threat landscape overwhelms existing responses, and the default resort to the use of force is too narrow and too simple. Physical damage or loss of human life is too often the principal measure of a national security reaction to top tier threats, thereby leaving many other forms of damage, and other perpetrators or other victims, out of consideration. National security requires more collective, public-private, coordinated strategies that define what is a legitimate use of force in cyberspace by government actors versus what is self-defense by victimized organizations. Equally needed are the coordinated programs to implement systemic cyber resilience within and across key public and private sectors and communities of the Nation. The Forum discussed the importance of departing from conventional notions of force and its limitations, and adopting new standards that reflect the cyber domain's unique characteristics.

Key Stakeholders

- Federal Government: Executive, Legislative & Judicial branches
- Military, Intelligence Agencies, Law Enforcement: DOD, DIA, NSA, CIA, FBI, NATO
- Cabinet Departments: Homeland Security, Treasury, Justice, Department of State
- State and Local Government: National Guard, law enforcement
- Private Sector: multiple industries, banking, finance, payments systems, capital markets
- Public Policy: academia, advocacy
- Foreign Partners: private and public

Representative Quotes

"We are at war in Cyberspace. It is time we recognize this reality and alert the Nation."

"Cyber threats today greatly exceed America's level of preparation."

"We will need collaboration. The public and private sector must come together nationally and internationally."

"The Naval War College is uniquely positioned as a national convening authority to bring the government and the private sector together for U.S. cybersecurity policy leadership."

"We have terrestrial, admiralty, aviation, even nuclear laws and norms. What about cyberspace? We need cyber law and norms laid out clearly to understand our scope of action."

RECOMMENDATIONS

1. Government and private sector leaders must develop initiatives for national-level awareness and education, preventative measures and countermeasures, and cybersecurity doctrine and policy.

2. Partnerships must be formed at the highest levels of government and the financial industry to collaborate and cooperate on mitigating a dynamic threat landscape. Planning, training, and exercises should be undertaken to better define and leverage complementary roles across individuals, sectors, and nations.

3. Policymakers should establish baseline definitions of cyber-attack versus cyber-crime for domestic and international application of law (civil and criminal) and defense.

II. PROTECTION OF U.S. AND GLOBAL FINANCIAL INFRASTRUCTURE

Key Issues and Questions

- Role of government in protecting U.S. private sector institutions
- Role of international institutions (NATO, global central banks, capital markets exchanges) in safeguarding international capital system
- Free rider / laggard dilemma and the role of regulation
- Interconnectivity of financial system: vulnerability and dependency of networks

Overview of the Discourse

The Forum discussed the vulnerability of the global financial system to cyber threats in any one country's financial system due to interconnected capital and technology linkages. Financial institutions have become highly dependent on cyberspace in order to transact across geographies and constituencies with scale efficiencies. The U.S. and global financial system is premised on the existence of, and collective confidence in, assured security for financial data transactions. Trust and confidence are critical elements in the global financial system and are therefore closely aligned with security in cyberspace. Conversely, lack of trust in security can yield powerful adverse economic forces across multiple geographies and constituencies.

The cyber threat to our financial institutions threatens the trust and confidence in the financial system. The increased scale and frequency of cyber attacks facing leading American banks, for example, undermines confidence in the safety of our system and the security of our assets and

national treasure. The cybersecurity of U.S. financial institutions and infrastructure is existentially critical to America's long-term economic security.

America's financial infrastructure and iconic institutions and market exchanges are increasingly targets in cyber attacks for economic and ideological motivations by bad actors. Cyber threats are diverse, ranging from state-on-state warfare, to financial crimes, theft of intellectual property, cyber-espionage, and preparation of the battlefield for future action. Cyber threats are constantly evolving and adapting to seek out and exploit vulnerabilities in our financial architecture.

Significant investment in the Nation's cybersecurity, by both the public and private sectors, is needed to preserve the security of cyberspace. Maintaining the security of cyberspace is critical to the functioning of the U.S. and global financial system and economies. America's interests require the surety of cybersecurity in our financial system.

The Forum introduced the ambitious notion of a cyber strategic equivalent to the Marshall Plan to mobilize the requisite U.S. and allied resources to promote shared security and prosperity in the twenty-first century cybered world. A comprehensive national cybersecurity strategy might begin with a strictly U.S. focus before expanding globally in concert with our allies. Such a strategy would require the difficult political achievement of developing a strategic consensus to strengthen, adapt, and integrate several factors, including: baseline technologies; U.S. domestic laws; regional agreements; enforceability of international norms; cross-sector national programs; and people, processes, and technology (PPT). In short, enlightened and effective political leadership would be required to develop and implement a strategic framework of U.S. national cybersecurity within and beyond our geographic borders.

Key Stakeholders

- Broadest scope of inter-connected governments & economies
- U.S. public and private sectors
- U.S. financial institutions and industry
- Developed and developing nations
- International financial infrastructure
- Global and regional financial entities and hubs

Representative Quotes

"If any one financial institution is at risk, then all financial institutions are at risk, and so is the broader American economy and society."

"The larger banks and institutions can afford the investment in cybersecurity, and cannot afford to ignore it. The large may need to protect the small."

"We have a huge burden as an iconic American company, because we are asked to take on the security of the United States."

"Exercises are key. The military trains through exercises and war-gaming (such as those at the U.S. Naval War College). Why not cybersecurity exercises for the banking sector?"

RECOMMENDATIONS

1. Financial sector firms must continue to cooperate and share information with one another, government agencies, law enforcement, and cybersecurity firms via established mechanisms, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), for common protection of U.S. financial infrastructure. Many of the larger firms already share extensively with each other and federal government entities. The continuous push from trade associations, regulators, and the Treasury Department for smaller financial firms to join the FS-ISAC should be further supported and encouraged.

2. America's largest financial institutions must continue to lead in protecting the industry and smaller institutions. Concrete actions include: a) investing in cybersecurity resources; b) adopting stringent cyber procedures; c) encouraging use of the National Institute of Standards and Technology-Cybersecurity Framework (NIST-CF); d) sharing data with the FS-ISAC so that threat information can be distributed to smaller firms; and e) investing in analytical infrastructure, like the recently developed software platform created by FS-ISAC and NIST-CF, "Soltra Edge", that enables automated threat indicator sharing.

3. The financial industry should continue to address the “free rider / institutional laggards" problem by promoting: a) industry standards of conduct like the NIST-CF; and b) accounting control standards, Service Organizational Controls (SOC2); and c) a risk-based approach and best security practices with regulators.

4. Financial institutions should broaden participation in war-gaming simulation exercises to prepare for coordinated individual and institutional cyber-attack responses. This builds on the sector’s experience in exercises like CyberFire (2008), Quantum Dawn 1 (2011), Quantum Dawn 2 (2013), and the Cyber TTX Series (2014). Plans for additional multi-year exercises should include a broadening scope of constituencies in government and private sector and financial organizations. The U.S. Naval War College is a national resource in war-gaming that could potentially host cybersecurity simulation exercises for U.S. financial sector firms.

5. Federal and state governments should continue to collaborate with the private sector to remove barriers to the sharing of threat data between and among stakeholders. While specific

initiatives are being coordinated with Treasury, Homeland Security, and Executive authorities to establish information sharing processes with the financial sector, the challenging scope of integration will require focus and leadership to achieve systematic implementation.

III. CYBER DOCTRINE & LAW

Key Issues and Questions

- Countering threats in cyberspace: by whom, in what jurisdiction, and under what authority?
- Formulating a national defense doctrine for cyberspace
- Developing a legal framework for cyberspace under U.S. and international law
- Differentiating between cyber offense and cyber defense in national security

Overview of the Discourse

The Forum agreed that it would be preferable to establish definitive attribution as a pre-requisite for any cyber response, but acknowledged that this level of accuracy is rarely possible. Cyberspace's inherent anonymity and decentralized posture complicates attribution enormously, thus the reality of too often relying solely on law enforcement response after the attack has occurred. Several factors are essential in disrupting cyberspace's safe havens and shedding light on malicious cyber actors, including: a) increased investments in pre-event threat intelligence; b) more effective sharing of incident data; c) more gaming through rapid reaction responses across industry partners; and d) further developing technologies in the area of advanced heuristics (problem solving) and anomaly detection.

Cyber responses should be governed by proportionality and not necessarily limited to actions only within cyberspace itself. For assaults amounting to major national events, cyber-attacks could be countered with non-cyber mechanisms by sea, air, space, and land forces. Responses should be proportionate. A possible guide to justifiable retaliation response has been outlined in the recently completed Tallinn Manual on the International Law Applicable to Cyber Warfare, 2013, in which a member of the Naval War College faculty was a contributing scholar.

The Forum discussed the applicability of the principle of collective defense in the context of Article 5 of the NATO Treaty, which declares an armed attack against one member-state to be an armed attack against all member-states. A similar construct should exist for cyber-attacks. Key elements of this construct are emerging from the discussions of the Tallinn Manual and a number of bi-lateral and multi-lateral discussions on applying the Law of Armed Conflict to cyberspace.

These international laws, however, are products of a bygone era in which states were the only major actors able to cause or contain major harm to other states. Given the 'everyman' nature of cyber conflict today identified by the Forum's participants, such laws are difficult to both apply and enforce, particularly given the blurred lines between some traditional state actors and non-state actors (ranging from nationalistic sympathizers to outright proxies) in cyber conflict.

Nation-states are now beginning to enact virtual territorial controls piece-by-piece, from requiring that data be located within their physical territory (several nations) to ruling that the national police can monitor all Internet traffic crossing national territory (Sweden, 2008). The debate about what is called a "re-territorialization" or a rising "Cyber Westphalian" process is highly contentious. The longer-term emergent consensus will have major impact on the future relevance of current international law about justifiable force and self-defense. As the responsibilities and latitudes of states solidify over the coming years, a strategy rooted in definitive attribution and proportionality could (given the appropriate technological transformation) ultimately support an international cyber deterrence regime and succeed in disrupting cyber-attackers' business models and their cost-benefit calculus about the probability of success.

Key Stakeholders

- Federal Government: Executive, Legislative & Judicial branches
- Military, Intelligence Agencies, Law Enforcement: DOD, DIA, NSA, CIA, FBI
- Cabinet Departments: State, Homeland Security, Justice, Treasury
- Allied Nations: NATO, existing U.S. alliances
- State and Local Government: law enforcement
- Private Sector: multiple industries; banking, finance, payments, capital markets
- Public Policy: academia, advocacy

Representative Quotes

"It may be time for the creation of a separate Cyber Force within the Department of Defense, just as the Air Force was created out of the Army to focus on a new domain of warfare."

"American corporations are relentlessly attacked by our adversaries. We don't fire back. We must be willing to do so."

"The role of law enforcement responding to cyber attacks today is analogous to that of the Emergency Medical Teams arriving to treat an injured patient. In both cases, the damage has already been done. We need to move toward a preventative cybersecurity model."

"Companies are protecting themselves (through retaliatory cyber countermeasures, in some cases) because they have to. It's not against the law, because the law doesn't exist."

"Government has to move faster or pass authority and grant permission to act."

"This is an 'all hands on deck' problem that is moving too fast for government regulation."

RECOMMENDATIONS

1. Collectively develop comprehensive strategy, legal framework, and cyber self-defense expectations for U.S. national cybersecurity policy.

2. Delineate clearly and systematically the difference between cyber offense and cyber defense operations permitted for U.S. national security institutions, including the outcomes considered acceptable politically, economically, and ethically.

3. Codify legal jurisdiction for cyber defense to assign authorities and permissions to act by government, military, sanctioned consortia, and private sector interests.

4. Establish cyber law enforcement norms and ensure adequate resources at state and national levels.

5. Promote mutually assured cyber resilience across public and private institutions, emphasizing collaboration in threat identification, remediation, and deterrence through policy, incentives, and resource sharing.

IV. THE HUMAN ELEMENT

Key Issues and Questions

- Recognition of vulnerability to cyber-intrusions through exploitable and exploitative human behavior
- Cyber hygiene: standards of understanding, training, and responsible behavior to mitigate risk of cyber threats in networked systems
- Preparing the next generation to secure the future of cyberspace

Overview of the Discourse

The human element is the indispensible component of cybersecurity. People are at the core of cyber threats, both as bad actors or unwitting accomplices. Our policies need to: a) pursue and punish the former, and b) educate, protect, and improve the performance of the latter.

Most cyber-attackers have "bosses and budgets." Raising the economic barriers to entry will help stem the tide of cyber-attacks. Adopting simple best practices and technical standards ("cyber hygiene") can significantly reduce cyber risk by increasing the financial cost to hackers and removing low-level actors from the threat pool. Doing so begins with good cyber hygiene and a cyber-savvy culture. Cybersecurity is a shared responsibility: both the public and private sectors play a role in promoting awareness.

Closely related, America's cybersecurity talent pool is qualitatively and quantitatively deficient relative to our asymmetrically-advantaged cyber rivals with nexus in Russia, China, North Korea and Iran, among other cyber centers of adversarial intent and expertise. Robust education and training curricula are necessary to grow America's level of preparation to a level commensurate with the threat. The next generation cybersecurity practitioner will reside at the intersection of technical and non-technical disciplines.

Key Stakeholders

- Any person with a computer, smartphone, or Internet connection
- Federal and State governments
- Private and public sector networked organizations
- Department of Education and academia
- Public policy and advocacy groups

Representative Quotes

"To err in cyberspace is human; to exploit, malicious."

"Insiders and employees are letting the bad actors gain access to networks. Organizations must hold their people accountable for the technology they use."

"We know the bad actors are going to get in; that's a given. What we have to do is protect the data once they are inside our network."

"Future cyber warriors will require a blend of skills ranging from computer geek to poet, where technical IT skills are joined with lateral-thinking problem-solving."

"We need a 'Smokey the Bear of cybersecurity' in our educational media."

RECOMMENDATIONS

1. Actively promote education of cyber risk and cyber hygiene in school curricula.

2. Actively promote cyber awareness and best practices to employees in public and private sector.

3. Develop national campaign to capture the attention of broad population of the necessity of cyber awareness practices.

4. Develop the theory and practice of cybersecurity – the integrated application of technology, human factors, and policy to create a more resilient and defensible cyberspace.

V. CYBER THREAT INTELLIGENCE SHARING

Key Issues and Questions

- Disseminating threat intelligence to take countermeasures and avert contagion
- Cross-sector collaboration: federal, state, law enforcement
- Financial sector collaboration: trade associations, lead institutions, Treasury and FBI
- "Cyber speed" versus government response time

Overview of the Discourse

The Forum highlighted the critical importance of sharing cyber threat information with multiple stakeholders and authorities at “cyber speed,” while noting that government response time is challenged under the best of circumstances. Jurisdictional authorities complicate accountability and responsiveness for cyber sharing. "Stove-piping" in government restricts access to silos of information from other government entities or personnel who could benefit from timely access to that information.

Cybersecurity legislation and considerable funding at the state and federal level are necessary to connect the actors across sectors and authorities to ensure robust cross-sector collaboration on cyber threats and resilient responses. Despite widespread support for information sharing, insufficient accommodations for privacy and liability protection have thus far hindered legislative movement. The cyber threat landscape is dynamic and can overwhelm current established regulatory regimes. Market incentives can contribute by bringing to the table many stakeholders

not yet recognizing their long-term self-interest in joining public-private partnerships, especially those commercial entities whose concern about costs and the loss of competitive advantages keep them from fully participating today. Tax breaks, rules that affect everyone equally, and legal immunity are examples of how legislation can foster a better information sharing environment.

Information sharing also requires technical solutions that enable real-time, secure, and trusted collaboration. Finance industry trade organizations, for example, have developed the aforementioned innovative analytical platform, Soltra Edge, that facilitates shared situational awareness of cyber threats across the financial industry and government. Other sectors should join this platform to facilitate cross-sector, machine-to-machine sharing and develop similar strategies to mitigate cyber-attacks in a timely manner.

Finally, information sharing demands vertical integration as much as it requires horizontal integration. Cross-sector collaboration is key. In the digital age, cybersecurity demands executive-level attention. Public and private institutions must practice cyber risk management from the IT Department up to the C-Suite.

Key Stakeholders

- Federal Government: Executive, Legislative & Judicial branches
- Military, Intelligence Agencies, Law Enforcement: DOD, DIA, NSA, CIA, NATO, FBI
- Cabinet Departments: Homeland Security, Treasury, Justice, State
- State and Local Government: law enforcement
- Global Financial Institutions: U.S. and global counterparts
- Private Sector: multiple industries, banking, finance, payments systems, capital markets
- Public Policy: academia, advocacy

Representative Quotes

"Information sharing needs to be at real time speed within minutes or seconds."

"Law enforcement operates at the speed of the law, not at the speed of cyberspace."

"We don't need more regulation! Compliance regulation does not equal improved security."

"The observation of one leads to the defense of many."

“There is no cybersecurity without information sharing.”

"Cybersecurity has moved out of the data server room and into the corporate board room."

"CEOs are now accountable for the cybersecurity of their organizations. Expect more CEOs to be replaced by corporate boards due to ineffectual cybersecurity policy and practice."

RECOMMENDATIONS

1. U.S. financial industry should expand and institutionalize real-time threat dissemination protocols and methods within the financial sector.

2. U.S. financial industry and federal government agencies and the Treasury Department should incentivize and institutionalize threat sharing methods and operations with a focus on speed-to-response time.

3. Congress should not regulate financial institutions for cybersecurity compliance given the need for speed, tactical flexibility, and room for maneuver by information security and risk managers.

4. Congress and state legislatures should promote collaboration in public-private partnerships through coordinated legislation with tax and other incentives to address increased costs, privacy, and liability of financial institutions.

CONCLUDING REMARKS

The Forum Chairman and distinguished Moderators concluded the proceedings with gratitude for the time and talent of the assembled leaders participating. The Chairman noted that findings and recommendations would be circulated to all attendees for use in their respective organizations in the form of Forum Proceedings. 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.