U.S. Government and Private Industry Must Prepare for Cyber-Enabled Economic Warfare Escalations

February 5, 2019

Introduction

In October 2018, the Foundation for Defense of Democracies and The Chertoff Group conducted a cyber-enabled economic warfare (CEEW)[1] tabletop exercise with former senior government officials and private sector leaders. The purpose of the exercise was to identify points of alignment and divergence between what the private sector and government may want, need, and demand from each other in the immediate aftermath of a major cyber incident.

The CEEW exercise simulated a massive cyberattack affecting various U.S. lifeline sectors at the same time that the U.S. military was deploying substantial forces to an overseas theater due to a geopolitical standoff with a peer adversary. As military tensions escalated, the cyberattacks did as well. There were cascading impacts on critical and consumer infrastructure, degrading military capabilities and stoking public fear that access to food, health care, and bank accounts could be jeopardized.

In addition to examining areas of alignment and divergence, the exercise also analyzed decision-making authorities and processes, resilience capabilities, and information-sharing mechanisms.

The most important finding from the discussion is that unless government and private sector decision makers begin developing CEEW-specific procedures and trust now, the United States will find itself flat-footed during a major cyber event.

It is tempting to say that defenses against state actors should simply be left to the U.S. government, but this ignores the very real business disruption and follow-on public panic that can occur in cyber-enabled economic warfare attacks. Banks, logistics firms, and even consumer goods manufacturers are obvious targets.

1. Cyber-enabled economic warfare "refers to a hostile strategy involving attack(s) against a nation using cyber technology with the intent to weaken its economy and thereby reduce its political and military power." Samantha F. Ravich and Annie Fixler, "Framework and Terminology for Understanding Cyber-Enabled Economic Warfare," *Foundation for Defense of Democracies*, February 22, 2017. (https://www.fdd.org/analysis/2017/02/22/framework-and-terminology-for-understanding-cyber-enabled-economic-warfare/)

"What we're looking at here is reshaping the division of labor, the division of responsibility between government and private sector. Because the details of the social contract in physical space do not all transfer and translate up into cyberspace."
–Former senior intelligence official

The tension between a company's fiduciary duties and the U.S. government's national security needs were evident throughout the day. Large multinational companies are essentially able to conduct their own foreign policies. Ensuring that the actions taken by the U.S. private sector are not in direct conflict with the goals of the state during a time of a national security emergency is critical.

U.S. national security and prosperity require resilient enterprises that are capable of withstanding and rapidly recovering from a significant cyber event. This requires pre-clearing select members of the private sector so that the government can share timely, classified, actionable information. Simultaneously, the private sector must be prepared to respond to Washington's demands in a crisis by assessing ahead of time the sensitivity of categories of information potentially requested by the U.S. government. A cyber-enabled economic warfare crisis may lead to critical resource, technology, and personnel shortages necessitating resource prioritization. Washington must therefore consider a national technology reserve for long-lead-time components in the supply chain and a secure cloud for critical infrastructure data as a way to ensure the continuity of the economy. The harder it is for our adversaries to undermine critical infrastructure, the less exposed America will be to cyber-enabled economic warfare.

Key Findings and Recommendations

Key Finding #1: There is disagreement about the importance of attribution of attacks and the relevance of private sector data to attribution. Notwithstanding advances in legal safeguards, challenges, and misunderstandings also persist regarding protections that enable the private sector to share information with the U.S. government.

Private sector organizations prioritized the importance of timely, operationally actionable information about how malware operates and its attack vectors. But among private sector participants, there were conflicting perspectives on the practical value of attribution for defending private networks.

"We're defending our networks 24/7. All the time. Those networks are attacked thousands of times a day. We really couldn't care less if it's state sponsored or organized crime or if it's a lone wolf. At the end of the day, all our customers – and the government is a large customer – rely on our resiliency. The thing we need [to know] is, what is the malware? How do we defend against that as quickly as possible?"
–Chief security officer at a major telecommunications company

That said, several private organizations explained that attribution helps them anticipate future escalations because threat actors have unique tactics, techniques, and procedures. These participants also implored the government to articulate more clearly how information from private sector organizations advances the government's ability to attribute attacks and why this attribution serves the interests of the private sector.

"Many of us have done research and development around what potential tactics we might see out of what actors, and we have playbooks to defend against particular actors."
–Senior vice president at a major financial institution

Government participants emphasized that attribution is important to the ability to execute decisive actions in crisis conditions. In response to debate about how attribution ambiguity would limit the government's ability to respond, one former government official explained that attribution is not an "all or nothing" concept and that the government can take some actions with only circumstantial attribution.

> **"There's also a range of views inside the government as to what confidence level is need to make attribution. The level of confidence needed to make an intelligence assessment is at one level. The level of confidence to begin covert action against the offender is another. To begin Title 10 sorts of activity, which are not covert, is another level of confidence. And then to turn it over to law enforcement is also a distinct level of confidence. And I fear your dialogue only begins when it gets to law enforcement competent, and therefore you've lost the early clues that might be of advantage to you."**
> **–Former senior intelligence official**

Another former official noted that with access to attack data – including perhaps private industry data – attribution is not as difficult as it once was.

> **"Over the last 10 or 15 years, we've seen a good combination of data coming from the private sector and data coming from the government in order to get to attribution. But what the private sector tends to have, that the government cannot assemble quickly, is international data from private sector companies. Because they are on the ground doing incident response and have access to network logs at the enterprise level. The private sector can ask their people, 'What are you seeing on your global networks?' That's not easily attained from the government."**
> **–Former senior FBI official**

The Cybersecurity Information Sharing Act of 2015 provides liability protections to private entities that share cyber threat indicators and defensive measures with other private entities and the government, and it protects the confidentiality of the information shared with the U.S. government. And yet, relatively few companies outside select sectors are proactively sharing cybersecurity threat information with federal entities. Indeed, some companies are unaware of the details of this legislation. During the exercise, there was a robust discussion that even with liability protection, private sector firms fear reputational harm – including concerns about loss of control over ensuing investigations – if they share data with the government.

> **"What we tend to hear repeatedly in the private sector is the belief that there are more legal restrictions on information-sharing than actually exist. When we actually explore what the issues are, it turns out that the legal issues are far easier to get past than people think. It really tends to be, what do people want to get done? … When you're talking about what is the will and what are the incentives and disincentives to put your company forward and risk reputational harm, those are, I think, very significant."**
> **–Former senior FBI official**

Participants acknowledged a meaningful improvement in sector-specific and cross-sector information sharing, but the volume and quality of exchanges remains uneven across industries. Critical infrastructure sectors like electricity and financial services have longstanding mechanisms and channels, including Information Sharing and Analysis Centers (ISACs). Other private entities, however, including large companies whose business crosses multiple sectors, as well as companies with more limited threat intelligence resources, are less equipped to share cybersecurity data. There was a recognition on both sides that if sectors could define for the intelligence community their most critical systems, the intelligence community could collect and provide more targeted, and therefore more useful, information on how cyber actors could try to compromise these systems (as well as the likelihood of attempts to do so).

Finally, while the government has granted security clearances to a number of private sector personnel in core critical infrastructure sectors, a major cyber incident could reveal the need for a much broader group to access specific classified information. Participants discussed the value of pre-clearing a broad set of personnel in the private sector so that clearances could be activated immediately during a national cyber emergency. The U.S. government's current efforts to grant security clearances are perceived as unevenly implemented both across the national security industrial base as well as within each industry.

> **"You've got to remove the legal impediments of communication between the private sector and the government. … You're going to get a lot of government guys who say, 'I can't talk to you about that because that's classified.' Okay, you can clear anybody in. We have to have a mechanism for quickly getting private sector people cleared in the compartments so that there can be open conversation in very short notice."**
> **–Former senior Department of Defense official**

Recommendations

1. **Washington should undertake a more broad-based public awareness campaign** to educate the citizenry – focusing specifically on executives at large – and sector-significant companies **on the importance of the private sector's role in helping to safeguard the nation during a national cyber emergency**. Working with the private sector in the development of this campaign can help address industry concerns about reputational and brand damage.
2. **Washington should educate the private sector on data types most needed to attribute and disrupt CEEW attacks**. This education should be part of a broader effort to explain why attribution is important not only for the government but also for the private sector.
3. **Industry should collaborate on a unified approach to strategic early warning of attacks** on important infrastructure underpinning critical lifeline sectors. An industry-created and -led Analysis and Resilience Center – similar to the one that currently exists for the financial services industry (the FSARC, created by the financial services ISAC), but serving a wider group of critical infrastructure sectors – would provide a broader and more synthesized view of cyber threats and their impacts to critical must-run systems. This organization could also serve as a clearinghouse for closer collaboration with the government through an appropriate Federally Funded Research and Development Center. Such an effort would also enhance the U.S. government's ability to assess and react to cyberattacks on key systems, particularly when those attacks occur below traditional national security thresholds but may still have systemic and widespread impacts on critical national functions.
4. **The U.S. government should "pre-clear" a population from the private sector** whose clearances could be activated for timely and sensitive information sharing as needed. The critical dependencies analysis being undertaken at the Department of Homeland Security's National Risk Management Center (described in more detail below) should inform what additional clearances are needed.
5. **Private sector entities should engage in focused discussions that weigh the relative sensitivity of information categories potentially requested by the U.S. government** so that they can be prepared to respond to U.S. government requests or demands in crisis conditions. These discussions could take place within Information Sharing and Analysis Organizations (ISAOs), which the president has directed the Department of Homeland Security to develop.

6. The U.S. government and private sector entities (or relevant ISAOs) should establish a requirements definition process that enables **private sector organizations across multiple industries to proactively define key information collection and analysis needs**.
7. **Industry information-sharing organizations, including ISAOs, should also consider requiring their companies to contribute threat information** as a condition of membership.

Key Finding #2: The U.S. government possesses response functions, emergency authorities, and powers that can be invoked during a significant cyber event, but the practical implications during severe cyberattack conditions remain unclear. It is critical to build and sustain resilient enterprises now to mitigate future catastrophic impacts.

The group recognized the challenges the U.S. government and private sector will face in prioritizing scarce resources even as the National Cyber Incident Response Plan defines the roles, responsibilities, capabilities, and coordinating structures that support how the United States responds to, and recovers from, a significant cyber incident. The interdependencies across sectors will potentially create cascading impacts if core technology platforms are disrupted.

> **"The folks from the grid will say 'can't run the banks without power,' and Oil and Gas will insist '1/3 of energy is generated by natural gas so pipelines should be prioritized.' Who is going to be first in line, and how do we make that call?"**
> **–Senior leader of a critical infrastructure company**

To be sure, the government has emergency powers to mitigate the crisis and restore critical infrastructure operations. The U.S. government could call upon these authorities to prioritize scarce resources or supplement the private sector where additional skillsets are required or where shortages exist.

The group identified specific authorities that Washington might consider leveraging during crisis conditions. In particular, the Defense Production Act authorizes the president to mobilize the private sector, allocate materials, and ration scarce resources to promote national security and defense. The Stafford Act, meanwhile, authorizes major disaster declarations. The U.S. government would need to create or invoke other authorities to direct critical infrastructure firms to immediately apply technical remediations to constrain an attack. At the same time, the U.S. government may also need to address shortages of qualified personnel to implement the measures.

While the U.S. government has plans, protocols, and support functions to assist companies victimized by cyberattacks, participants recognized that government resources would be heavily constrained given widespread impacts or because of an ongoing overseas contingency. The government does not have the capacity to prevent all attacks on commercial entities, and therefore participants recognized that companies need to independently build and sustain resilience functions to mitigate potential CEEW-based disruptions on their employees, customers, and business operations. Many private sector participants acknowledged that they might be forced to "go it alone" with limited expectations for government assistance.

> **"We sell to pretty much every house in America, and I don't know what we would do. We'd probably call the local FBI office and go to the governor. We'd be head down trying to fix our stuff. But I just have this feeling that we wouldn't be getting much help at all."**
> **–Chairman of the board of directors of a large manufacturing company**

Some industry participants pointed to existing resilience planning activities and redundancies that could support business continuity and recovery objectives. Electricity sector participants, for example, cited North American Electric Reliability Corporation's Spare Equipment Database, and the grid's capacity for manual operations when operational technology fails. That said, participants recognized an urgent need for a much more comprehensive effort to ensure resiliency given supply chain interdependencies.

The scenario for this tabletop exercise involved a malware infection delivered through a software supply chain compromise. Participants acknowledged that as individual customers, they have limited ability to manage broader third-party risk and complex software supply chains.

Recommendations

8. To better understand interdependencies across sectors, **the White House and Congress should properly resource and fund the Department of Homeland Security's National Risk Management Center**, which identifies national critical functions and associated interrelationships and dependencies. The Center also works with other federal agencies and bodies, like the Strategic Infrastructure Coordinating Council, to ensure key sectors are adequately resilient.
9. **The U.S. government should also develop resource prioritization and allocation plans** pursuant to Executive Order 13636, which directs the Department of Homeland Security to create a list of entities upon which a successful cyberattack would likely have catastrophic consequences.
10. **The U.S. government should assess the best mechanisms for a national technology reserve for critical long-lead-time components in the supply chain**. This assessment should also consider the costs and benefits of incentivizing companies – through tax or other favorable consideration – to stockpile these components.
11. Washington should incentivize commercial entities to develop capabilities to anticipate, withstand, contain, and rapidly recover from a significant cyber event. **Immediate consideration should be given to how existing liability limitation programs** such as the SAFETY Act (the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002) could be modified to incentivize resilience.
12. **The U.S. government should begin developing strategies to create a Continuity of the Economy plan** and assess the costs and benefits of creating a secure cloud for critical infrastructure data.
13. **Washington should evaluate existing authorities that mandate the private sector engage in immediate patching and related defensive and containment measures**, recognizing that new authorities may be needed.
14. **Private companies should conduct comprehensive business impact analyses on critical business functions** and the applications, data, and other IT assets that support those functions. They should also ensure that business continuity and disaster recovery plans feature recovery time objectives as well as redundancies and work-arounds to sustain critical operations.
15. **ISAOs should work with their members to enhance software supply chain visibility** to reduce the risk of subversion and compromise. Mitigation initiatives could include software transparency, a secure systems development life cycle (SDLC), more vigilant third-party due diligence, and continuous monitoring.

16. **The government and private sector should also consider how a mature cyber insurance market** (with better actuarial data and mechanisms to measure an organization's resilience) **could help advance private sector resilience**.

Key Finding #3: Private companies may face conflicts between national security imperatives and business objectives. The U.S. government must therefore take steps now to ensure the private sector's conflicting loyalties do not undermine crisis response.

Participants discussed the role that the private sector might play in government decision making. While former government participants welcomed private sector input, industry recognized that Washington is unlikely to provide advance notice to the private sector of actions taken during an escalating overseas contingency even when the escalation may lead to retaliation against the U.S. private sector.

At the same time, industry participants recognized that their primary response would focus on protecting their networks, safeguarding their interests, and restoring customer-facing operations. They also acknowledged the significant economic downside of overt hostility or aggressive action directed against specific adversarial nations with whom U.S. companies do significant business.

> **"I'm glad to hear that we have a lot of patriots around the table who would back a campaign against that country. But I can see the private sector saying, 'What are we doing here?' I mean, are we really going to get into an economic war against a global economic power?"**
> **–Senior vice president of a major American financial institution**

Industry participants anticipated that some prominent CEOs of companies with significant foreign presence or interests could engage in "freelance diplomacy" with their foreign counterparts to preserve business objectives. The group also acknowledged that U.S. companies with C-suites or boards with non-American members may find it more difficult to resolve divergences between the economic interests of their company and the national security of the United States during an escalating overseas contingency.

Recommendations

17. **U.S. companies** with significant foreign ownership, control, or influence **should consider contingency plans for balancing business objectives with potential CEEW conditions** and associated geopolitical tensions.
18. **Washington should consider how the Logan Act** – a 1799 U.S. federal law that criminalizes negotiation by unauthorized persons with foreign governments in a dispute with the U.S. – **might be implemented during a CEEW event** to prevent private industry from engaging in actions that are unhelpful to government objectives. Although the law has rarely been invoked, a public awareness campaign focused on this law could dampen the likelihood of freelance diplomacy by corporate leaders. **Public warnings against interference** and efforts to name-and-shame companies that attempt to meddle for commercial reasons during a major U.S. national security operation **may also dissuade such behavior**.

Key Finding #4: Public perceptions of government inaction are likely to influence both government and private sector responses, and therefore public reactions must be factored into response planning.

Both government and private sector participants acknowledged that public outcry in response to degraded lifeline sector services could limit the U.S. government's maneuvering room. If the American public became convinced

that the damages from the cyberattacks outweighed the importance of the overseas military operation, the U.S. government may be limited to responses that de-escalate the situation. Meanwhile politicians and candidates for public office may exploit the incident for their own policy agendas or political aspirations. Additionally, in a heightened political environment, public trust in government statements about attribution, attack impacts, and responses would likely be viewed through a partisan lens.

> **"You'd have no fuel, you'd have no food, people would be in the streets. People would start hurting each other. There are a lot of guns in this country. [The cyberattack is] an act of war at that point and those in DC would be debating some section of some law."**
> **–Chairman of the board of directors of a large manufacturing company**

In an escalating overseas contingency, an already politically charged environment could be seeded with adversarial media operations to further sow discord. Participants observed that adversarial influence operations using social media could be a powerful tool to affect opinion during crisis conditions.

Recommendations

19. **The U.S. government should actively drill stakeholder relations teams to maintain public confidence during perceived CEEW crisis conditions** by focusing on government transparency and communication. Washington should explore increased Emergency Broadcast System drilling and applications for social media.
20. **Washington should consider how state and local authorities can counsel the public on CEEW awareness and readiness** similar to natural disaster preparedness campaigns.
21. **Washington should continue to strengthen capabilities to identify and counter influence operations** in close partnership with leading social media companies.

Conclusion

The tabletop exercise revealed that both the government and private sector require measures to anticipate, withstand, and recover from a CEEW attack. The recommendations above outline some of the steps the public and private sectors should implement to build resiliency and mitigate attacks.

Policymakers should study the lessons of history. During the Cold War, the United States developed Continuity of Operations/Continuity of Government plans to ensure that the government could execute essential functions in the event of a nuclear attack. These plans continue to be core components of emergency planning, but today's risks extend beyond direct threats to the U.S. government. Today, the private sector is on the battlefield, and strategic planners need to consider how to reconstitute the U.S. economy in the event of a large-scale CEEW campaign through a Continuity of the Economy plan. American innovation and prosperity are our nation's greatest assets. It is incumbent, therefore, that Washington and the private sector to work together to ensure their protection.

Appendix: Anonymized Participant List

Private Industry Participants

- Retired chairman, president, and chief executive officer of a major electric utility holding company and board member of major bank and energy company
- Senior vice president of a major American financial institution
- Vice president and the chief information officer of a major oil and gas company
- Associate general counsel of a major oil and gas company
- Chief security officer at a major American telecommunications company
- Former chief executive officer and president of an American technology company
- Executive vice president and chief legal officer of a leading financial services and insurance organization
- Chairman of the board of directors of a large manufacturing company
- Senior vice president of a large manufacturing company
- President and chief executive officer of a financial services physical and cyberattacks prevention organization
- President of a financial sector cyber and systemic risk mitigation organization
- President and chief executive officer of a professional services organization

Former Government Officials

- Former director of the Central Intelligence Agency and National Security Agency
- Former deputy secretary of defense
- Former under secretary of commerce
- Former chairman of the Federal Communications Commission
- Former deputy secretary of energy
- Former under secretary of homeland security
- Former homeland security advisor and assistant attorney general
- Former deputy national security advisor and assistant secretary of the Treasury
- Former deputy national security advisor to the vice president
- Former deputy assistant director of the FBI's Cyber Division
- Former director of homeland security and emergency management for the State of New Jersey