FDD FOUNDATION FOR DEFENSE OF DEMOCRACIES | The Chertoff Group

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

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.
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**.

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**.

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.