A Playbook for Winning the Cyber War

By Emily Harding, Julia Dickson, and Aosheng Pusztaszeri

KEY TAKEAWAYS

- State-affiliated cyberattacks against the United States are increasing in sophistication and severity, yet Washington remains dangerously unprepared. CSIS proposes a new playbook to prepare for this era of cyber conflict.
- CSIS wargames tested responses to a deadly Chinese, Russian, or Iranian cyberattack on the U.S. homeland. The results revealed the likely disastrous confusion that would occur in a cyber-first conflict, as policymakers lack shared frameworks and a coherent view on what constitutes an act of war or a proportional response.
- China is now the top cyber threat. Beijing is well-resourced and persistent, excelling in espionage and operational preparation of the environment (OPE). Chinese threat actors have aggressively targeted U.S. critical infrastructure (CI), likely prepositioning to conduct disruptive attacks.
- Russia's cyber campaign in Ukraine may give a false sense of security about the threat Russian cyberattacks pose. Russian attacks have been persistent and comprehensive, but Ukraine has proven resilient. The United States lacks similarly hardened systems.
- Iran is a rising, aggressive cyber actor. Though less advanced than China or Russia, Tehran has targeted civilian CI and is likely to pursue further destructive cyber activities.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

BACKGROUND & CONTEXT

China, Russia, and Iran have used increasingly aggressive attempts to disrupt, delay, and harass the United States and its allies in the cyber domain. Russia blazed a trail in this domain, and China followed with a sweeping campaign of intellectual property theft. Iran is a rising cyber actor and has demonstrated a brazen willingness to attack civilian CI. As these adversaries build their capabilities, cyberattacks against the United States are increasing in frequency and sophistication. For instance, Chinese threat actor Volt Typhoon embedded itself in the networks of multiple civilian CI networks, likely prepositioning to sabotage civilian CI and hinder U.S. military mobilization during a Taiwan contingency.

Despite repeated wake-up calls, U.S. government efforts to bolster cyber defense have broken on the rocks of well-intentioned but deleterious opposition. At the same time, the United States is generally regarded as one of the world's most capable offensive cyber actors. This offensive skill, however, is counterbalanced by its large attack surface and weak domestic defense, resulting in hesitation to utilize the available tools and a reluctance to retaliate against attackers.

A dramatic change is needed in the cyber domain. Washington urgently needs to integrate cyber into its broader foreign policy toolkit and determine how cyber activity aligns with larger foreign policy actions, including deterrence, proportional response, and international norms. In other words, the United States needs a new playbook to respond to increasingly disruptive and aggressive cyberattacks.

LEGISLATIVE OR POLICY IMPLICATIONS

Congress is currently considering several bills that tackle aspects of cyber defense, but no single bill offers a comprehensive framework.

The Senate draft of the National Defense Authorization Act (S. 2296) includes specific measures to address defense-related cybersecurity gaps, including measures to protect military infrastructure and formulate nationwide cyber defense strategies. The House version (H.R. 3838) maintains current cyber programs and funding levels, with fewer new cybersecurity initiatives.

Other bills focus on CI protection. The Strengthening Cyber Resilience Against State-Sponsored Threats Act (H.R. 2659) aims to enhance understanding of and response to Chinese state-sponsored cyberattacks by establishing an interagency task force. The Cybersecurity for Rural Water Systems Act (H.R. 2109) expands funding opportunities under the Department of Agriculture for rural water systems to upgrade their cybersecurity capabilities.

CHALLENGES & RISKS

By failing to fully integrate cyber into its foreign policy toolkit and to strengthen its defenses, Washington has unintentionally created an environment where:

- **Critical infrastructure is exposed.** Chinese actors like Volt Typhoon and Iranian actors have demonstrated both the will and capability to disrupt U.S. civilian CI.
- **Washington has failed to establish deterrence in the cyber domain, and adversaries control the escalation ladder.** Historically, U.S. foreign policy has rested on deterrence, with implied escalation dominance in any domain. But that foundation has failed in the context of cyber. U.S. responses to cyberattacks have been muted, and escalation dominance does not exist.

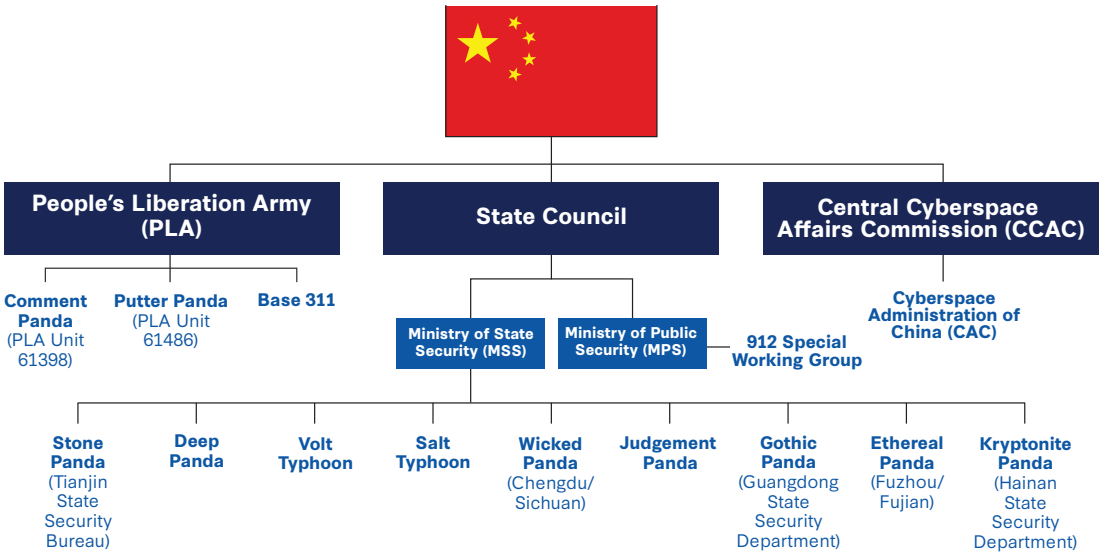
RECOMMENDATIONS

We recommend five specific congressional actions to address these challenges:

- **Fund cybersecurity:** Congress should consider funding much-needed capital upgrades in government networks, allow more flexible spending for cybersecurity improvements, and require improved reporting and greater accountability for weak cyber defense inside government. They should also consider creating a combination of funding streams (carrots) and consequences (sticks) for CI providers to significantly improve their resilience against attacks.
- **Create and fund a new Cyber Force:** The cyber domain needs its own service, heavily weighted toward reserve forces, to recruit and retain the best cyber talent from the private sector. The House and Senate Armed Services Committees should consider using the next NDAA to initiate the first steps.
- **Protect industry cyber fighters:** Treat the private sector as real partners. Put in place protections for cyber operators who act in conjunction with the U.S. government, as so many from the private sector did in Ukraine.
- **Give the Cybersecurity and Infrastructure Security Agency (CISA) additional authorities:** Congress should consider granting CISA the authority to hold agencies accountable for their cybersecurity defenses and deploy intervention teams to take over cyber defense efforts if agencies repeatedly fail cybersecurity audits.
- **Codify "Secure by Design":** The U.S. government has made this program requiring secure coding largely voluntary. Congress should consider passing legislation to require Secure by Design in all software products. After two years, software should display a security label; after five, producers of unlabeled products should be liable for security flaws.

GRAPHICS/CHARTS

Chinese Cyber Actors



Source: CSIS research.

ADDITIONAL RESOURCES

- Tech Recs: A one-stop shop reference site, designed for Congress, highlighting CSIS's best recommendations for policies around reforms in seven critical technologies.
- Seven Critical Technologies for Winning the Next War: This report identifies the seven technologies critical to maintaining an edge against near-peer adversaries—secure and redundant communications, quantum technology, bioengineering, space-based technology, high-performance batteries, AI and machine learning, and robotics. Congress should prioritize investment in these areas.
- "The United States Needs a New Way to Think About Cyber": This piece proposes three steps the U.S. government can take to establish clear norms and deterrence in the cyber domain.
- China's Strategy of Political Warfare: A comprehensive report for Congress that covers Chinese political warfare activities, including China's main actions and goals as well as U.S. options for countering Beijing.

For more information, contact: **Chloe Himmel** at 202.775.3186 or **chimmel@csis.org**.