**CYBER OPERATIONS**

**Definition**

Use of hacking, viruses, or other methods to conduct information warfare, cause physical damage, disrupt political processes, punish economic competitors, or commit other malicious acts in cyberspace.

---

**Examples of Gray Zone Threat vs. U.S. Interests**

- U.S. national intelligence, intellectual property, and critical infrastructure vulnerable to cyberattacks from multiple actors
  - China’s acquisition of National Security Agency (NSA) hacking tools and repurposing them to attack U.S. allies and private companies
  - Russian cyber breaches during U.S. 2016 presidential election and attempts during 2018 U.S. midterm elections
  - Iran’s attacks on U.S. banks, businesses, government agencies, and dam in New York
  - 2014 North Korean massive cyberattack on Sony; monetary cyber thefts

**U.S. Government Responses**

The Players: Department of Homeland Security (DHS), Intelligence Community (IC), Department of State (DoS), Department of Defense (DoD), Department of Justice (DOJ), Department of Treasury, Department of Commerce, Federal Communications Commission (FCC), Department of Energy, White House (WH)

<table>
<thead>
<tr>
<th>Deterrence &amp; Resilience</th>
<th>Intelligence &amp; Investigation</th>
<th>Cost Imposition</th>
</tr>
</thead>
<tbody>
<tr>
<td>- DHS, FCC, and Commerce set cybersecurity policies, standards, and recommendations; DoS helps set international agreements like the Wassenaar Agreement and the Budapest Convention on Cybercrime</td>
<td>- IC investigates cyber activity and cyberattacks</td>
<td>- DoD’s CYBERCOM (aided by NSA) use a “defending forward” strategy to conduct “persistent engagement”</td>
</tr>
<tr>
<td>- IC leads the protection, investigation, and coordination national security systems; DHS leads U.S. civilian cybersecurity, leads election security, critical infrastructure; DOE, IC, DoD also protect other critical infrastructures in the United States and has expanded to Europe with the Russia Influence Group</td>
<td>- DOJ and the IC’s Cyber Digital Task Force investigates and prosecutes malicious cyber activity</td>
<td>- DOJ’s Cyber Digital Task Force aids and expands U.S. government toolkit for prosecuting malicious cyber activity</td>
</tr>
<tr>
<td>- The Joint Artificial Intelligence Center plans policy for the future of DoD artificial intelligence (AI) operations</td>
<td></td>
<td>- Treasury enforces sanctions like Countering America’s Adversaries Through Sanctions Act (CAATSA); WH, Commerce, and Treasury blocks business with Huawei, ZTE; Trade bans enforced by Commerce and Treasury’s Committee on Foreign Investment in the United States</td>
</tr>
<tr>
<td>- Commerce formulates research on telecom policy and security; FCC’s Communications Security, Reliability, and Interoperability Council sets recommendations for telecom security; WH updated their Artificial Intelligence R&amp;D Strategic Plan</td>
<td></td>
<td>- Naming and shaming (WH, DoS, Commerce)</td>
</tr>
</tbody>
</table>
U.S. Government Assessment

Bureaucratic Structure
- Few opportunities for interagency coordination
- Lack of centralized direction for interagency
- Lack of regulation and evaluation structures within U.S. government
- Insufficient discretionary funding, which harms the flexibility and innovation of U.S. responses

Policy Positions
- Weak international coalitions and partnerships that undermine efforts to coordinate global cyber security efforts (e.g., countering Huawei)
- Underdevelopment of offensive measures and leveraging U.S. strengths like transparency

Operational Limitations
- Intelligence and information sharing hindered by over-classification and bureaucratic stove-pipes
- Inadequate alternatives to China’s 5G technology
- Ineffective tools and tactics
- Few punitive measures to stop cyberattacks
- Few inducements for the private sector to report attacks or to shun potentially harmful technology

Authorities and Purview
- Cyber strategy is unclear on how to create and direct strategic action from policy

Recommendations

Authorities and Resourcing
- Authorize and appropriate resourcing for offensive capabilities, election cybersecurity, and investments in public and private sector research and development (R&D) for advanced technologies
- Appoint a cyber coordinator on the NSC to facilitate interagency collaboration and deconfliction, prioritizing homeland defense

Policies
- Prioritize and align cyber strategy and operations with competitive strategies that account for the domain’s evolving complexity
- Develop a holistic approach and a code of conduct for offensive and defensive capabilities
- Align offensive cyber action with information operations
- Develop a common approach to 5G security
- Develop mechanisms for private sector outreach, building on lessons from Section 9 and Financial Systemic Analysis and Resilience Center
- Buttress cyber alliances and partnerships abroad to coordinate and build resilience

Tools
- Develop capabilities for offensive cyber for the defense of U.S. territory and institutions to deter and prevent hacking