THIRD WAY
National Security

To Catch a Hacker:

Policy Recommendations

Cybercriminals operate with a sense of impunity as only 0.3% of malicious cyber incidents see an arrest, according to our analysis of FBI reported data. What that means is that the United States is facing a massive cyber enforcement gap just as the cybercrime wave continues and malicious cyber activity that threatens our national security is becoming more common. To close the cyber enforcement gap, we call for a comprehensive, strategic approach to identify, stop, and punish malicious cyber actors. The US maintains robust efforts to secure existing computer networks, but heavily relying on air tight systems and mistake-less human users can only accomplish so much. In our new paper, we call for ten US policy actions (some that build off existing efforts) that can form the contours of such a strategy to go after human attackers.

Domestic Enforcement Reform

1. **A Larger Role for Law Enforcement:** Strengthen capacity building efforts so that law enforcement, enabled by diplomacy, can target the humans behind cyberattacks.
2. **A Cyber Enforcement Cadre:** Address not only workforce shortages, but the way the cyber enforcement workforce is trained, incentivized, and retained.
3. **Better Attribution Efforts:** Increase investments in research and development for attribution technology, better digital forensics, and prioritize efforts to build international alliances that improve timeliness and impact of attribution efforts.
4. **A Carrot and Stick Approach to Fugitives:** Adopt a broader reward-based system to incentivize information sharing that can lead to arrests of malicious cyber actors balanced with the smart use of targeted sanctions.

International Cooperation and Coordination Reform

5. **An Ambassador-level Cyber Quarterback:** Institute an ambassador-level cyber coordinator position at the State Department with a clear mandate and resources on cyber enforcement.
6. **Stronger Tools in the Diplomacy Arsenal:** Expand the number and streamline processes for agreements with other countries that help bring cyber attackers to justice and continue to utilize the multilateral Budapest Convention.
7. **Better International Capacity for Enforcement:** Support efforts to build the capacity of other countries on cybercrime investigations, while ensuring cybercrime and cybersecurity efforts are not used to suppress civil liberties and human rights.

Structural and Process Reform

8. **Better Success Metrics:** Establish mechanisms to measure the scope of the cyber enforcement problem and the effectiveness of government efforts.
9. **Organizational Changes and Interagency Cooperation:** Evaluate further needed policy changes to de-conflict the missions of the agencies responsible for cyber enforcement.
10. **Centralized Strategic Planning:** Institute an overarching, comprehensive strategy for US cyber enforcement led by a senior official at the White House.

The lack of an overarching strategy to deal with this growing threat is ominously analogous to the pre-9/11 US government approach to terrorism. We need a strategy that doesn't just focus on building a better safe, but focuses on catching the safecracker.