REACTION

PLANNING RESPONSES AND DEFINING ATTACKS IN CYBERSPACE

Evan F. Kohlmann[*] *and Rodrigo Bijou*[**]

In the past year, the United States has experienced an alarming explosion of cyberattacks aimed at public- and private-sector targets. From small businesses to U.S. government agencies and security contractors, a surprisingly broad range of systems have been compromised by increasingly sophisticated attacks attributed to both criminal and state actors alike. While the country's leadership continues to make references to a "cyber-Pearl Harbor," a "digital 9/11," and even "Cybergeddon," the reality is that the most severe cyberattacks are below a conventionally understood military threshold. The most severe threats lie in attacks against critical infrastructure like banks, energy companies, and telecommunications firms. Unfortunately, it is often these sorts of attacks that are the most socially disruptive and yet rarely subject to any form of clear punitive sanction.

While the FBI would never tolerate a sustained physical attack on a conventional bank branch by rifle-toting assailants, the U.S. government allows serious cyberattacks to go unpunished. In recent months, the government has stood by and watched a shadowy group that calls itself the "Izz ad-Din al-Qassam Cyber Fighters" mount destructive electronic assaults again and again on virtually every major American bank — purportedly in retribution for a YouTube video the group deems blasphemous to Islam. U.S. government officials have fingered Iran in connection with the attacks, yet have waffled on any definitive response. Indeed, this cyberthreat is fundamentally different from past challenges in its ability to cause significant economic or social damage without physical operations. A lack of established international legal procedures, a hazy public understanding of the mechanics of electronic intrusions, and cyberterrorists' exponentially faster operational tempo (all combined with the extreme challenges involved in definitively identifying perpetrators on the Internet) have allowed some lawless actors to operate with a surprising sense of impunity.

[*] Evan F Kohlmann is a Senior Partner at Flashpoint Global Partners, a New York-based cybersecurity consulting firm. He has served as a private consultant on cyberterrorism and cybersecurity to the U.S. Justice Department and the FBI.

[**] Rodrigo Bijou is an analyst on issues related to cybersecurity and counterterrorism. He is currently pursuing research in advanced persistent threats, and advising the private sector on emergent security issues.

With these distinctions in mind, the federal government must establish policies that firmly signal a commitment to protect American businesses and warn hostile actors that they cannot inflict critical damage on the U.S. economy without consequence. Instead of promoting catchy slogans, the federal government should first establish clear thresholds for what constitutes an actionable cyberattack using such criteria as (a) physical harm, (b) significant disruption to critical infrastructure, and (c) prolonged damage to GDP. Establishing such thresholds would allow the government to stop focusing exclusively on military expertise and start considering the trade expertise of the Office of the United States Trade Representative or the financial crimes expertise of the FBI, where applicable. Clearly defining different thresholds would help ground the cyberterrorism debate in a way that helps the government craft a response doctrine based on legality and domain expertise, and in a manner that respects the unique characteristics of cyberattacks.

While analogies to Pearl Harbor may be a bit misguided, the law of just warfare is very much relevant to such an analysis. The "just war" doctrines of *jus ad bellum* and *jus in bello* may be applicable once attack thresholds are properly defined. In deciding whether to respond to attacks, the federal government can turn to existing legal norms, such as international law governing preemptive strikes against imminent threats, to build a cybersecurity escalation model where the United States is not in the untenable role of initial aggressor. Once it has decided to engage, the federal government can use the principle of "offensive countermeasures" to select a justifiable response. For example, launching an offensive action like forcibly disabling systems responsible for a denial of service attack against the financial sector would be well within the boundaries set by existing legal norms since it would be used reactively. By contrast, degrading foreign systems without even the suspicion of an impending attack would lack legal justification.

Cyberterrorism also raises the issue of proportional response. The U.S. government can ensure proportionality by giving the appropriate agency the power to respond. Carefully allocating response authority would help avoid any legally troubling issues arising from agencies working outside their statutory authority, and instead provide more credible response vehicles based on existing missions. For example, if an attack caused economic damage, the responsibility to respond in justified manner through proportional actions like sanctions would fall to the Office of the United States Trade Representative, the State Department, and the Department of Justice. Conversely, if an attack is more directly damaging — even potentially resulting in loss of life — or is the unambiguous work of a state-sponsored actor, then the federal government would have a more obvious justification to invoke a proportional military response using appropriate authorities like the Department of Defense Cyber Command. The federal government can thus apply proportionality in a manner that not only gives operations better legal standing, but also strengthens those operations by ensuring responses align with the domain expertise of a particular agency. Cyberattacks are aimed at a comprehensive set of targets and therefore need to be addressed in a comprehensive manner.

Any successful cybersecurity strategy will undoubtedly require further investment in the country's ability to reliably track and attribute responsibility for attacks when they occur — whether those attacks target government agencies or private companies. Spending added dollars on cybersecurity at a time of government sequester and budget-trimming may not be a particularly popular policy, but the government cannot afford to let the situation continue to devolve: private actors may become tempted to take independent offensive measures in a desperate effort to protect themselves. The Internet can remain free without being an online Wild West — and it is in America's immediate interest to reassure both its friends and its adversaries of the country's commitment to consistently uphold law and order across the digital domain.