Asymmetric Threats in an Era of Great Power Competition

Sponsored by CACI International Inc, The Center for Security Policy, and the Institute for the Study of War

Escalating Cyber Warfare: Risks and Recommendations

The U.S. is involved in a cyber war that is aimed at the whole of our society and our interests. China and Russia have been attacking and exploiting U.S. government, industry, and private information networks for decades. Their cyber forces continually probe financial networks, public infrastructure, technology companies, and government networks using deception – often through proxy actors – to cover their tracks.

Both China and Russia have been highly successful at penetrating and exfiltrating massive amounts of sensitive data, from consumer records to U.S. government personnel files and highly classified technology. They have embarked on aggressive military modernization projects, producing weapon systems and technologies that bear suspiciously close resemblance to our own. China's fifth-generation stealth aircraft, for example, is modeled after U.S. technology that cost millions of dollars to develop and test.

China has made no secret of its ambitions to dominate the Pacific region, and cyber operations are a key element of its plans. Most of its regional neighbors and their militaries have underinvested in cybersecurity, exposing themselves and their allies and partners – including the U.S. – to increased risk of technology and information theft. Backed by an increasingly powerful military with a broader footprint than ever, China can intimidate regional neighbors with the threat of cyber attacks on their infrastructure and financial systems that could potentially be followed by military intervention.

While the U.S. and its partner nations attempt to define authorities and policies that enable information sharing yet adequately protect national sovereignty and the privacy of their citizens in cyberspace, countries like China, Russia, and others freely disregard international norms. The popularity of the Internet of Things is making cyber defense even more difficult. Household appliances, industrial controls, garage door openers, cars, drones – nearly everything seems to have WiFi or Bluetooth connectivity. This level of networking is about to be amplified by the introduction of 5G mobile technology: it is estimated that 20 billion devices will be connected. This exponentially increases the threat surface, and 5G's ability to connect point-to-point will make it much more difficult to trace bad actors.

China has invested heavily in 5G technology through Huawei and other companies. As U.S.-friendly nations snap up Chinese equipment and devices, exploitation becomes a significant risk. It is difficult to ascertain what sort of backdoors or malware might be in that equipment. Even more troubling, a significant percentage of Internet traffic will be routed through that equipment, leaving sensitive information open to potential capture by Chinese military and intelligence teams.

> The challenge in cyberspace is that speed, not size, is the source of strength. Adversaries can operate much quicker, since they are not burdened by the ethical, privacy, and sovereignty considerations that the U.S. and its partner nations must work through.

There is zero unemployment for people with deep cyber skills. The challenge is that even if every American man, woman, and child were a cybersecurity warrior, the U.S. would still be vastly outnumbered. This is why the U.S. must make better use of analytics, artificial intelligence, and machine learning as force multipliers to distinguish anomalies from normal behavior and automate responses.

The cyberspace domain is not confined to the military, so responding adequately to cyber operations will require a broad response, especially when it comes to the rampant theft of intellectual property. There must be much stricter standards with nations that steal technology. It should be considered a "showstopper" before we sign any trade agreements.

NOTE: The content of this report reflects the invocation of the Chatham House Rule for the symposium as non-attributable.