2013-04-29

Embrace Cyber Executive Order

Jasper, Scott

Gannett Co., Inc. by NewsBank, Inc.

Defense News (2013), p. 21
https://hdl.handle.net/10945/48285

Embrace Cyber Executive Order

Defense News - April 29, 2013

- Edition: Domestic
- Section: A
- Page: 21
- Readability: >12 grade level (Lexile: 1530)

The Chinese foreign minister issued a call March 10 for international cooperation on Internet espionage and called accusations of Chinese government involvement in recent hacking incidents an international smear campaign.

Chinese state media similarly condemned suggestions the country was behind the massive global cyber spying campaign (Operation Shady RAT) uncovered in August 2011.

On this occasion, the national security adviser to the US president publicly demanded the Chinese government stop widespread data theft and agree to acceptable norms of behavior.

Recent testimony by the U.S. director of national intelligence warned that the growing use of cyber capabilities is "outpacing the development of a shared understanding of norms of behavior" and raises concern over whether such norms or other means are viable responses.

International conferences on cyberspace held in Budapest in October and London in 2011 stressed the need for international consensus on norms to guide behavior in cyberspace, but little progress has been made.

By contrast, the U.S. Cyber Command is establishing 13 teams of experts capable of carrying out cyber attacks on other nations. Cyber Command's head, in testimony to Congress, said the teams gave him "confidence in our ability to deter major state-on-state attacks in cyberspace" while admitting "we are not deterring the seemingly low-level harassment of private and public sites, property and data."

Attribution remains a huge challenge. Achieving the level of confidence needed to offensively respond to low-level incidents is extremely difficult to attain.

China may have been responsible for attacks on South Korean banks and television networks March 20, based on the discovery of Chinese words and other clues in the destructive malware. However, such indicators are common disinformation techniques used by cyber attack designers and were even used in Stuxnet.

The Darkseoul malware overwrote the Master Boot Record and then wiped content from hard drives.

The malware functioned similar to Shamoon, which infected the oil giant Saudi Aramco in August 2012 and rendered some 30,000 workstations unusable. A self-described activist group, Cutting Sword of Justice, took credit, but analysts suspect the Iranian government commissioned it.

In the U.S., the Industrial Control Systems Cyber Emergency Response Team reported 124 attacks in 2012 against energy, water, chemical and nuclear companies. If U.S. armed forces are ordered to respond, the Pentagon is devising rules of engagement to provide clearer authority.

The line for action could be crossed if the intent is to disrupt or destroy infrastructure. Nonetheless, the lack of timely attribution will complicate the justification for any offensive operation, driving requirements for cyber intelligence that go far beyond issues of vulnerability and software identification.

For example, Chinese hackers used university computers as proxies and switched IP addresses to mask the source of intrusions at The New York Times.

Recently, when Congress failed to enact necessary legislation, President Barack Obama signed the Executive Order entitled "Improving Critical Infrastructure Cybersecurity" on Feb. 12. It sought to establish a partnership with private sector operators of critical infrastructure to improve information sharing and implement risk-based standards.

The order expanded the voluntary Enhanced Cybersecurity Services program of the Department of Homeland Security to all critical infrastructure sectors.

The executive order tasked the director of the National Institute of Standards and Technology to develop a cybersecurity framework that incorporates voluntary consensus standards and industry best practices.

The Critical Security Controls, introduced by the Center for Strategic and International Studies and now guided by the SANS Institute,

answer the call by providing a prioritized, risk-based approach to security based on unclassified threat intelligence.

Knowledge of real attacks that compromise systems influence the design and selection of technical measures, which improve capabilities to monitor networks, detect attack attempts and interrupt infiltration.

The cybersecurity framework would enable critical information sectors to benefit from a competitive market. The continual deployment of solutions to protect multiple threat points, including network, endpoint, Web and email security, would be vital.

The Critical Security Controls identify requirements for commercial tools to detect, track and correct weakness or misuse at threat points.

The executive order on Cybersecurity represents the first step to efficiently share threat information and implement better security practices across critical infrastructure sectors.

As offensive capabilities emerge to deter state-on-state attacks and international norms begin to control lower-level behaviors, embracing this new executive order will improve defensive capabilities to protect critical infrastructure sectors.

By Scott Jasper, lecturer at the Center for Civil-Military Relations at the US Naval Postgraduate School and editor of "Conflict and Cooperation in the Global Commons."

- *Record: def-10498592*