PHYS.ORG

3Qs: The rules of cyber-engagement

March 6 2013, by Jason Kornwitz

The Obama administration is reportedly close to approving the nation's first set of rules for how the military can defend or retaliate against a major cyberattack, according to a report last month in The New York Times. Credit: Thinkstock

The Obama administration is close to approving the nation's first set of rules for how the military can defend or retaliate against a major cyberattack, according to a report last month in *The New York Times*. One such new rule would reportedly give the president power to order a pre-emptive strike if the U.S. detects a credible threat from a foreign adversary. Northeastern University news office asked William Robertson, an expert in detecting and preventing Web-based attacks and an assistant professor with dual appointments in the College of Engineering and the College of Computer and Information Science, to assess the potential policy and the growing cyberarms race.

Former Defense Secretary Leon E. Panetta has warned that a cyberattack from a foreign nation or extremist group could be equally as destructive as the terrorist attack of 9/11. What would a cyber-9/11 look like and how does the president's power to order a pre-emptive cyberstrike against a foreign adversary impact the chances of such an attack?

The term "cyber-9/11″ is quite clearly meant to conjure up imagery surrounding the nation's shock in reaction to the airliner hijackings of 2001. One commonality between those attacks and an imagined cyber-9/11 is the element of surprise, where the attackers might very well execute an operation against the nation without advance detection. A strike against the nation's critical infrastructure—such as the power distribution network or air traffic control—could have far-reaching effects that harm or in some other way affect millions of Americans.

One can interpret the recent reported strategizing by the administration on the preemptive use of cyberweapons as a form of deterrence against would-be attackers, in much the same way that our nation's conventional military serves as a deterrent to potential adversaries. Given the history of alleged attacks against American assets by foreign actors located in China and Russia, it is quite possible that the recent decision to allow for preemptive cyberattacks is aimed squarely at nations such as these.

Unfortunately, deterrence only goes so far. It's unlikely to be effective against those adversaries that either do not anticipate experiencing great harm from a preemptive cyberattack—for instance, if attack attribution is difficult or the attackers do not possess significant technological assets—or the attackers have sufficient motivations—e.g., religious or political—that they are willing to risk the consequences.

The Washington Post recently reported the Pentagon is planning to significantly expand the Defense Department's Cyber Command to counter attacks against the nation's computer networks and execute operations on foreign adversaries. From your vantage point as a co-principal investigator of a $4.5 million grant from the National Science Foundation to train the next generation of cyberdetectives, why is the federal government having such a difficult time finding and training qualified cyberspecialists?

One reason for the difficulty in recruiting cyberoperators is simply the scarcity of qualified labor. People with the necessary skills are few and far between, and this shortage is evident in both government and industry circles. A related difficulty is that not every candidate who possesses the requisite technical background has the temperament or inclination for these jobs. Both defensive and offensive roles are stressful and demanding, and as in the case of the conventional military, many choose career paths that do not involve these characteristics.

Another consideration is that convincing top talent to work in a state or federal role can be an uphill battle. Government is competing for a small pool of candidates that can quite easily command large salaries and benefits in the private sector, either by working for any number of established security companies or as freelance consultants.

According to reports, critics have suggested that contractors and consultants looking for a big payday are overstating the cyberthreats to the nation's critical infrastructure. Where should the potential for a catastrophic cyberattack rank on the federal government's list of security concerns?

In my opinion, preparation for catastrophic cyberattacks should be a top priority for government, in cooperation with industry. Those who work in security are all too aware of the fact that our systems are already being attacked, our data is already being exfiltrated, and our infrastructure has already been demonstrated to be "porous" at best. When you consider that bolstering our defenses against catastrophic attacks will also likely translate to a more secure posture against the low-intensity cybercold war that we are already experiencing, as well as stimulate the creation of new jobs and technologies, it would seem to be the forward-thinking direction to move.

Provided by Northeastern University

Citation: 3Qs: The rules of cyber-engagement (2013, March 6) retrieved 26 April 2024 from https://phys.org/news/2013-03-3qs-cyber-engagement.html