Cybersecurity's next phase—cyber-deterrence

December 13 2016, by Dorothy Denning

Credit: Unsplash/CC0 Public Domain

Cyberattackers pose many threats to a wide range of targets. Russia, for example, was accused of hacking Democratic Party computers throughout the year, interfering with the U.S. presidential election. Then

there was the unknown attacker who, on a single October day, used thousands of internet-connected devices, such as digital video recorders and cameras compromised by Mirai malware, to take down several high-profile websites, including Twitter.

From 2005 to 2015, federal agencies reported a 1,300 percent jump in cybersecurity incidents. Clearly, we need better ways of addressing this broad category of threats. Some of us in the cybersecurity field are asking whether cyber deterrence might help.

Deterrence focuses on making potential adversaries think twice about attacking, forcing them to consider the costs of doing so, as well as the consequences that might come from a counterattack. There are two main principles of deterrence. The first, denial, involves convincing would-be attackers that they won't succeed, at least without enormous effort and cost beyond what they are willing to invest. The second is punishment: Making sure the adversaries know there will be a strong response that might inflict more harm than they are willing to bear.

For decades, deterrence has effectively countered the threat of nuclear weapons. Can we achieve similar results against cyber weapons?

Why cyber deterrence is hard

Nuclear deterrence works because few countries have nuclear weapons or the significant resources needed to invest in them. Those that do have them recognize that launching a first strike risks a devastating nuclear response. Further, the international community has established institutions, such as the International Atomic Energy Agency, and agreements, such as the Treaty on the Non-Proliferation of Nuclear Weapons, to counter the catastrophic threat nuclear weapons pose.

Cyber weapons are nothing like nuclear ones. They are readily developed

and deployed by individuals and small groups as well as states. They are easily replicated and distributed across networks, rendering impossible the hope of anything that might be called "cyber nonproliferation." Cyber weapons are often deployed under a cloak of anonymity, making it difficult to figure out who is really responsible. And cyberattacks can achieve a broad range of effects, most of which are disruptive and costly, but not catastrophic.

This does not mean cyber deterrence is doomed to failure. The sheer scale of cyberattacks demands that we do better to defend against them.

There are three things we can do to strengthen cyber deterrence: Improve cybersecurity, employ active defenses and establish international norms for cyberspace. The first two of these measures will significantly improve our cyber defenses so that even if an attack is not deterred, it will not succeed.

Stepping up protection

Cybersecurity aids deterrence primarily through the principle of denial. It stops attacks before they can achieve their goals. This includes beefing up login security, encrypting data and communications, fighting viruses and other malware, and keeping software updated to patch weaknesses when they're found.

But even more important is developing products that have few if any security vulnerabilities when they are shipped and installed. The Mirai botnet, capable of generating massive data floods that overload internet servers, takes over devices that have gaping security holes, including default passwords hardcoded into firmware that users can't change. While some companies such as Microsoft invest heavily in product security, others, including many Internet-of-Things vendors, do not.

Cybersecurity guru Bruce Schneier aptly characterizes the prevalence of insecure Internet-of-Things devices as a market failure akin to pollution. Simply put, the market favors cheap insecure devices over ones that are more costly but secure. His solution? Regulation, either by imposing basic security standards on manufacturers, or by holding them liable when their products are used in attacks.

Active defenses

When it comes to taking action against attackers, there are many ways to monitor, identify and counter adversary cyberattacks. These active cyber defenses are similar to air defense systems that monitor the sky for hostile aircraft and shoot down incoming missiles. Network monitors that watch for and block ("shoot down") hostile packets are one example, as are honeypots that attract or deflect adversary packets into safe areas. There, they do not harm the targeted network, and can even be studied to reveal attackers' techniques.

Another set of active defenses involves collecting, analyzing and sharing information about potential threats so that network operators can respond to the latest developments. For example, operators could regularly scan their systems looking for devices vulnerable to or compromised by the Mirai botnet or other malware. If they found some, they could disconnect the devices from the network and alert the devices' owners to the danger.

Active cyber defense does more than just deny attackers opportunities. It can often unmask the people behind them, leading to punishment. Nongovernment attackers can be shut down, arrested and prosecuted; countries conducting or supporting cyberwarfare can be sanctioned by the international community.

Currently, however, the private sector is reluctant to employ many active

defenses because of legal uncertainties. The Center for Cyber and Homeland Security at George Washington University recommends several actions that the government and the private sector could take to enable more widespread use of active defenses, including clarifying regulations.

Setting international norms

Finally, international norms for cyberspace can aid deterrence if national governments believe they would be named and shamed within the international community for conducting a cyberattack. The U.S. brought charges in 2014 against five Chinese military hackers for targeting American companies. A year later, the U.S. and China agreed to not steal and exploit each other's corporate secrets for commercial advantage. In the wake of those events, cyber espionage from China plummeted.

Also in 2015, a U.N. group of experts recommended banning cyberattacks against critical infrastructure, including a country's computer emergency response teams. And later that year, the G20 issued a statement opposing the theft of intellectual property to benefit commercial entities. These norms might deter governments from conducting such attacks.

Cyberspace will never be immune to attack – no more than our streets will be immune to crime. But with stronger cybersecurity, increased use of active cyber defenses, and international cyber norms, we can hope to at least keep a lid on the problem.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Cybersecurity's next phase—cyber-deterrence (2016, December 13) retrieved 4 May 2024 from https://techxplore.com/news/2016-12-cybersecurity-phasecyber-deterrence.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.