Active self-defense strategy best deterrent against cyber-attacks

June 27 2011

With the threats of cybercrime, cyberterrorism and cyberwarfare looming over our hyper-connected world, the best defense for the U.S. might be a good offense, says new research by a University of Illinois expert in technology and legal issues.

Law professor Jay P. Kesan warns that an active self-defense regime, which he terms "mitigative counterstriking," is a necessity in cyberspace, especially to protect critical infrastructure such as banking, utilities and emergency services.

"The threats from cyber-attacks are real, and the harm of a potential attack can be far greater than what we can currently combat," Kesan said.

Kesan's analysis, co-written with former U. of I. law student Carol M. Hayes and published in a forthcoming issue of the *Harvard Journal of Law and Technology,* concludes that mitigative counterstriking against attacks instead of simply relying on passive defense options (firewalls, patches and anti-virus software) is legally justifiable as self-defense, although a more exhaustive legal framework needs to be implemented.

"The principles of mitigative counterstriking are legally justifiable under several areas of domestic and international law, and can be made consistent with other areas of law by amending or reinterpreting the law," he said.

Kesan says an active defense regime consists of three distinct elements: detecting intrusions, tracing the attack back to the attacker, and executing a counterstrike.

A counterstrike can be characterized in one of two ways: retributive counterstrikes, which punish the attacker; and mitigative counterstrikes, which minimize the damage to the victims' information-technology infrastructure.

According to the authors' study, there currently is no effective domestic or international legal apparatus to deter cyber-attacks. Criminal law enforcement is complicated by the lack of a consistently enforced international law, jurisdictional issues and the difficulty of identifying an attacker in a manner specific enough to justify criminal prosecution. Resorting to civil litigation would likely be slow and impractical.

"Cyber-attacks are fundamentally different from crime," Kesan said. "The person may be physically very far away from you, and you may not be able to use traditional legal remedies against that person, since civil and criminal remedies require jurisdiction over a person. In those circumstances, what do you do?"

Kesan suggests that a government-affiliated agency, preferably a public-private partnership, should be responsible for an active defense program, including providing resources for private parties to detect and trace intrusions, and executing counterstrikes.

"We're at a particularly interesting moment in time because the technologies available to do this are getting better," Kesan said. "Trace-route and trace-back technologies – where we pinpoint where certain intrusions are coming from, even if they're going through intermediaries – are getting better. The swiftness of the technologies is getting better, which itself might be a deterrent."

Kesan says the confluence of better technology and inadequate legal protection provides a unique opportunity to think through the issues associated with creating new legal policy.

"Obviously, some sort of self-defense in cyberspace is justifiable," he said. "But how far do we go? Do we just block packets, or do we send them back? That's something we need to think carefully about."

Active defense, however, has been and continues to be a controversial subject. Kesan says the reason the government has been tentative is that, in some quarters, an active defense is viewed as tantamount to vigilantism. It also carries the risk of inflicting significant collateral damage.

"There will be consequences to engaging in that kind of conduct, so we don't want to take actions that are perceived as being lawless or could potentially cause lots of collateral harm," Kesan said. "Technologies are never 100 percent perfect or foolproof."

But if the U.S. is subject to an attack, "then we should have the ability to enact some measures to at least minimize the damage," he said. "Additionally, I would argue that a system to promote active defense and permit mitigative counterstriking should also include a liability rule to protect innocent third party intermediaries whose systems are compromised by attackers and counterstrikers."

Kesan says it's vital that formal policy is finalized soon, while there is still time for thoughtful deliberation and analysis of all of the potential implications of an attack.

"We rely on our online infrastructure for just about everything," he said. "That represents a good choke point, one that might be an attractive target for people who wish to do harm to us. If they were successful, it

would have the potential to cause a great deal of economic hardship. That's why we need to be prepared before we are faced with the fallout from an attack."

More information: The paper, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace," is available online.

Provided by University of Illinois at Urbana-Champaign