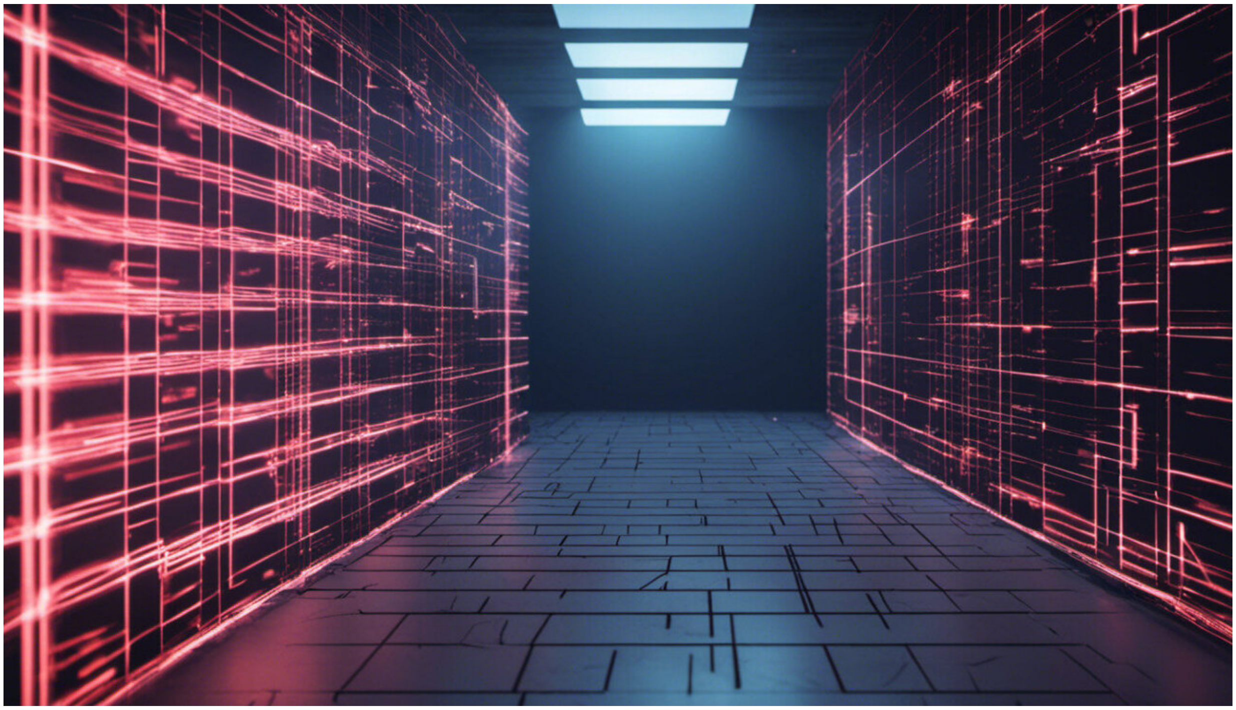
How far should organizations be able to go to defend against cyberattacks?

February 15 2019, by Scott Shackelford



Credit: AI-generated image (disclaimer)

The deluge of cyberattacks sweeping across the world has governments and companies thinking about new ways to protect their digital systems, and the corporate and state secrets stored within. For a long time, cybersecurity experts have erected firewalls to keep out unwanted traffic and set up decoy targets on their networks to distract hackers who do get in. They have also scoured the internet for hints about what cybercriminals might be up to next to better protect themselves and their clients.

Now, though, many leaders and officials are starting to think about stepping up their defensive activities, by taking more active measures. An extreme option within this field of active defense is sometimes called "hacking back" into an adversary's systems to get clues about what they're doing, shut down the attack or even delete data or otherwise damage an attacker's computers.

I have been researching the benefits and drawbacks of various active defense options with Danuvasin Charoen of the Thai National Institute of Development Administration and Kalea Miao, an undergraduate Cox scholar at the Indiana University Kelley School of Business. We have found a surprising number and variety of firms – and countries – exploring various ways to be more proactive in their cybersecurity practices, often with little fanfare.

Getting active

On the surface, it might seem like the proverb is right: "The best defense is a good offense." The damage from cyberattacks can be enormous: In May 2017, a single incident, the WannaCry cyber attack, affected hundreds of thousands of systems around the world and caused more than US$4 billion in lost productivity and data recovery costs. One month later, another attack, called NotPetya, cost global shipping giant Maersk $300 million and reduced the company to relying on the Facebook-owned WhatsApp messaging system for official corporate communications.

Faced with this scale of loss, some companies want to step up their defenses. Firms with sophisticated technology systems know what's needed to protect their customers, networks and valuable trade secrets. They also likely have employees with the skills to track down hackers and penetrate the attackers' own systems. But the ethics and implications of justifying a cyberattack as defensive get very complicated very quickly.

It's often unclear, for example, exactly who is behind an attack – uncertainty that can last for days, months or even years. So who should the hack-back target? What if a privately owned U.S. company believed that it was under attack from a firm owned by the Chinese government? If it hacked back, would that be an act of war between the countries? What should happen to repair corporate and international relations if the company was wrong and its attacker was somewhere else? Companies shouldn't be empowered to start global cyber conflicts that could have dire consequences, but online and offline.

Of course, it's also important to think about what might happen if other countries allow their companies to hack back against U.S. government or corporate efforts. More U.S. firms could fall victim to cyberattacks as a result, and might find little legal recourse.

Engaging with the law

At the moment, hacking back is illegal, in the U.S. and in many nations around the world. In the U.S., the Computer Fraud and Abuse Act makes it a crime to access another computer without authorization. Every member of the G-7, including the U.S., as well as Thailand and Australia, has banned hacking back. In 2018, more than 50 countries – but not the U.S. – signed an agreement that private firms based in their nations are not allowed to hack back.

However, supporters of active defensive tactics are pushing their message hard. The Republican Party's 2016 presidential platform promised to ensure "users have a self-defense right to deal with hackers as they see fit." In March 2018, the Georgia state legislature passed a bill to permit "active defense measures that are designed to prevent or detect unauthorized computer access." Two months later, then-Gov. Nathan Deal vetoed it, at the urging of technology firms concerned about its "national security implications and other potential ramifications."

Had it become law, Georgia's bill would still likely have run afoul of federal law. However, lawmakers in Washington have also proposed letting companies engage in certain types of active defense. In 2017, U.S. Rep. Tom Graves, a Georgia Republican, proposed the Active Cyber Defense Certainty Act, which would let companies engage in certain active defense measures, including conducting surveillance on prospective attackers, provided that the firm informed the FBI first and that the action did not threaten "public health or safety." The bill died and has not yet been reintroduced; it's not likely to get far in the new Democratic House.

Active defense remains illegal in the U.S. and much of the world. But the bans are not being enforced at home or abroad.

Going global

Not every country has banned hacking back. Singapore, for example, has been permitting local firms to engage in active defense measures in an effort to prevent, detect, or counter specific threats to its critical infrastructure, including the financial industry. Other nations, such as France, do not wish to see the private sector out front, but are still keen to keep active defense as an option for governments.

The more countries allow active defense, the more likely everyone – in the U.S. and around the world – is to become a cyberattack victim. Instead of deterring attacks, aggressive active defense increases the possibility of the lights going out, or American voting machines returning inaccurate results.

Organizations can and should be encouraged to take passive defense measures, like gathering intelligence on potential attackers and reporting intrusions. But in my view they should be discouraged – if not prevented – from acting aggressively, because of the risk of destabilizing corporate and international relations. If the quest for cyber peace degenerates into a tit-for-tat battle of digital vigilantism, global insecurity will be greater, not less.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: How far should organizations be able to go to defend against cyberattacks? (2019, February 15) retrieved 6 May 2024 from https://phys.org/news/2019-02-defend-cyberattacks.html