In a world of cyber threats, the push for cyber peace is growing

September 3 2019, by Scott Shackelford

Credit: AI-generated image (disclaimer)

Digital conflict and military action are increasingly intertwined, and civilian targets—private businesses and everyday internet users alike—are vulnerable in the digital crossfire. But there are forces at work trying to promote peace online.

It will be a tough challenge: In May 2019, Israel responded to unspecified cyberattacks by Hamas with an immediate airstrike that destroyed the Gaza Strip building where the hackers were located.

The U.S. had done something similar in 2015, launching a drone strike to kill an alleged Islamic State hacker, but that operation was months in the making. In July 2019, the U.S. also reversed the equation, digitally disabling Iranian missile-launching computers in response to Iran shooting down a U.S. military drone over the Strait of Hormuz.

U.S. businesses fear they might be the targets of retaliation for that attack from Iran. Even local nonprofits need to learn how to protect themselves from online threats, potentially including national governments and terrorists. In some ways cyberspace has rarely seemed more unstable, even hostile.

At the same time, dozens of countries and hundreds of firms and nonprofits are fed up with all this digital violence, and are working toward greater cybersecurity for all—and even what might be called cyber peace.

Serious hacking is getting easier

Data and security breaches like the one carried out by the Shadow Brokers, revealed in 2016, released extremely advanced hacking tools to the public, including ones created by the National Security Agency. Cybercriminals are using those programs, among others, to hijack computer systems and data storage in governments across the country.

Some companies have been forced to revert to one-to-one instant-messaging and passing written memos in the wake of ransomware attacks and other cybercrimes.

The U.S. government is taking note. Instead of pushing the technological envelope, it has elected to use tried and true analog technologies to help secure the electricity grid, for example.

A rising international effort

A growing coalition, including the governments of France and New Zealand, is coming together to promote international standards of online behavior, aimed at reducing cyber insecurity. Nonprofits like the Online Trust Alliance, Cyber Peace Alliance, Cybersecurity Tech Accord and ICT4Peace, are joining, as are major funders like the Hewlett Foundation and the Carnegie Endowment for International Peace.

I am the acting director of the Ostrom Workshop at Indiana University that includes the Cyber Peace Working Group, one of several academic groups also working to protect the Internet and its users.

Although it's too soon to say anything certain about long-term results, there are some early indications of success, including the outcome of a Paris meeting in November 2018. More than 60 nations – though not the United States—signed the Paris Call for Trust and Security in Cyberspace, along with more than 130 companies and 90 universities and nonprofit organizations. The document is a broad statement of principles that focus on improving "cyber hygiene," along with "the security of digital products and services" and the "integrity of the internet," among other topics. It doesn't legally bind its participants to do anything, but does lay out some basic points of agreement that could, in time, be codified into laws or other enforceable standards.

Its critics question whether it is too early to establish global commitments given that core issues of sovereignty over the internet remain unresolved. Nevertheless, the Paris Call has helped shape the conversation around the scope and meaning of cyber peace.

Another international effort began in the aftermath of the March 2019 mass shooting at two mosques in Christchurch, New Zealand. The governments of 18 nations—along with more than a dozen well-known technology firms like Google and Facebook—adopted the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online.

This effort has led many of the companies involved to change their policies governing hate speech and disinformation on their platforms. For example, YouTube, owned by Google parent company Alphabet, announced a new hate speech policy prohibiting content "alleging that a group is superior in order to justify discrimination, segregation or exclusion based on qualities like age, gender, race, caste, religion, sexual orientation or veteran status." The Christchurch Call has also helped widen the discussion about cyber peace to include thorny questions about democracy, such as how to balance freedom of speech with limits on extremist content.

A digital Geneva Convention?

A key element remains the need to protect civilians from harm in a future cyber conflict, such as attacks on the electricity grid, dams and other systems that affect daily life for much of the world.

One idea is to fashion an agreement along the lines of the Geneva Conventions, which with their predecessors have sought to protect innocent lives in military conflict for more than a century. An international treaty along the lines of the Outer Space Treaty, Antarctic Treaty or the U.N. Convention on the Law of the Sea may be useful.

There is not yet a grand "Treaty for Cyberspace," though. The relevant international agreement with the highest number of ratifications so far is the 2004 Council of Europe Convention on Cybercrime, also called the Budapest Convention, which guides international prosecution and

extradition of cyber criminals. The U.N. has several groups working on aspects of international cybersecurity.

But as with potential solutions to climate change, there's not a lot of political energy being put into the efforts.

Making progress anyway

In an attempt to avoid leaving people to fend for themselves in a perilous online world, the nonprofit Consumer Reports organization has launched a "Digital Standard" program that will evaluate and rate the privacy and security features of various internet-connected devices and services. Academics are also helping out, such as the Security Planner tool created by Citizen Lab at the University of Toronto, which helps civil society groups and researchers protect their data.

There's much more to be done to protect a digitally centered society, both politically and technically. The key will be focusing on a more positive vision of peace that includes better governance, respect for human rights, making internet access more widely available around the world, and teaching everyone how to protect themselves—and each other—online.

This will not happen overnight, and the path may not be a straight line. Consider that the often-derided 1928 Kellogg-Briand Pact, also called the Pact of Paris, outlawed aggressive war. It didn't work, but did eventually help lay a foundation for the United Nations and a more stable international system.

Similarly, a Cyber Peace Accord—building from efforts such as the Paris Call and the Cybersecurity Tech Accord—could, in time, lead the international community toward greater stability in cyberspace. One possibility could take inspiration from efforts to fight climate change, by

asking individual nations, towns, groups and even individuals to announce "Cyber Peace Pledges," to build momentum toward a more collective solution.

Working together, we may just be able to achieve cyber peace through a mix of shaming, outcasting and inspiring users, firms and policymakers to act.

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

Provided by The Conversation

Citation: In a world of cyber threats, the push for cyber peace is growing (2019, September 3) retrieved 21 June 2024 from https://techxplore.com/news/2019-09-world-cyber-threats-peace.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.