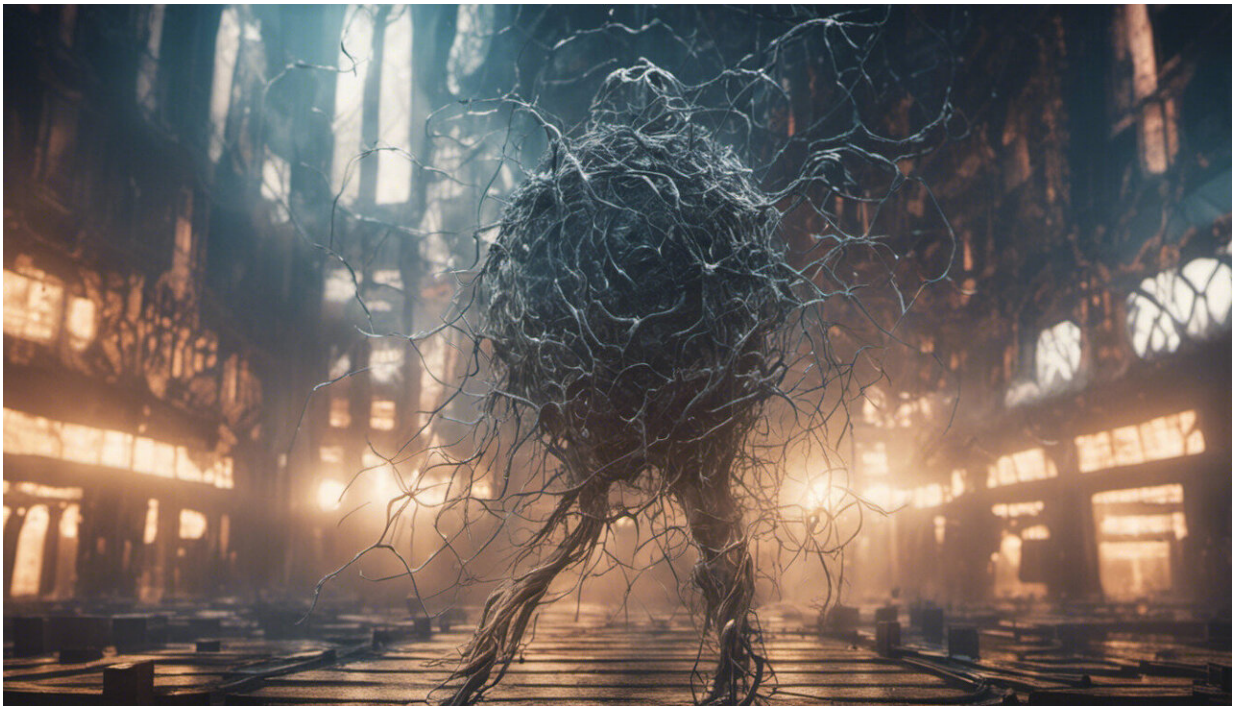
Should cybersecurity be a human right?

February 14 2017, by Scott Shackelford



Credit: AI-generated image (disclaimer)

Having access to the internet is increasingly considered to be an emerging human right. International organizations and national governments have begun to formally recognize its importance to freedom of speech, expression and information exchange. The next step to help ensure some measure of cyber peace online may be for cybersecurity to be recognized as a human right, too.

The United Nations has taken note of the crucial role of internet connectivity in "the struggle for human rights." United Nations officials have decried the actions of governments cutting off internet access as denying their citizens' rights to free expression.

But access is not enough. Those of us who have regular internet access often suffer from cyber-fatigue: We're all simultaneously expecting our data to be hacked at any moment and feeling powerless to prevent it. Late last year, the Electronic Frontier Foundation, an online rights advocacy group, called for technology companies to "unite in defense of users," securing their systems against intrusion by hackers as well as government surveillance.

It's time to rethink how we understand the cybersecurity of digital communications. One of the U.N.'s leading champions of free expression, international law expert David Kaye, in 2015 called for "the encryption of private communications to be made a standard." These and other developments in the international and business communities are signaling what could be early phases of declaring cybersecurity to be a human right that governments, companies and individuals should work to protect.

Is internet access a right?

The idea of internet access as a human right is not without controversy. No less an authority than Vinton Cerf, a "father of the internet," has argued that technology itself is not a right, but a means through which rights can be exercised.

All the same, more and more nations have declared their citizens' right to internet access. Spain, France, Finland, Costa Rica, Estonia and Greece have codified this right in a variety of ways, including in their constitutions, laws and judicial rulings.

A former head of the U.N.'s global telecommunications governing body has argued that governments must "regard the internet as basic infrastructure – just like roads, waste and water." Global public opinion seems to overwhelmingly agree.

Cerf's argument may, in fact, strengthen the case for cybersecurity as a human right – ensuring that technology enables people to exercise their rights to privacy and free communication.

Existing human rights law

Current international human rights law includes many principles that apply to cybersecurity. For example, Article 19 of the Universal Declaration of Human Rights includes protections of freedom of speech, communication and access to information. Similarly, Article 3 states "Everyone has the right to life, liberty and security of person." But enforcing these rights is difficult under international law. As a result, many countries ignore the rules.

There is cause for hope, though. As far back as 2011, the U.N.'s High Commission for Human Rights said that human rights are equally valid online as offline. Protecting people's privacy is no less important when handling paper documents, for instance, than when dealing with digital correspondence. The U.N.'s Human Rights Council reinforced that stance in 2012, 2014 and 2016.

In 2013, the U.N. General Assembly itself – the organization's overall governing body, comprising representatives from all member nations – voted to confirm people's "right to privacy in the digital age." Passed in the wake of revelations about U.S. electronic spying around the globe, the document further endorsed the importance of protecting privacy and freedom of expression online. And in November 2015, the G-20, a group of nations with some of the world's largest economies, similarly

endorsed privacy, "including in the context of digital communications."

Putting protections in place

Simply put, the obligation to protect these rights involves developing new cybersecurity policies, such as encrypting all communications and discarding old and unneeded data, rather than keeping it around indefinitely. More firms are using the U.N.'s Guiding Principles to help inform their business decision-making to promote human rights due diligence. They are also using U.S. government recommendations, in the form of the National Institute for Standards and Technology Cybersecurity Framework, to help determine how best to protect their data and that of their customers.

In time, the tide will likely strengthen. Internet access will become more widely recognized as a human right – and following in its wake may well be cybersecurity. As people use online services more in their daily lives, their expectations of digital privacy and freedom of expression will lead them to demand better protections.

Governments will respond by building on the foundations of existing international law, formally extending into cyberspace the human rights to privacy, freedom of expression and improved economic well-being. Now is the time for businesses, governments and individuals to prepare for this development by incorporating cybersecurity as a fundamental ethical consideration in telecommunications, data storage, corporate social responsibility and enterprise risk management.

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

Provided by The Conversation