

Society's dependence on the internet: 5 cyber issues the coronavirus lays bare

March 30 2020, by Laura Denardis and Jennifer Daskal



AI will serve to develop a network control system that not only detects and reacts to problems but can also predict and avoid them. Credit: CC0 Public Domain

As more and more U.S. schools and businesses shutter their doors, the rapidly evolving coronavirus pandemic is helping to expose society's dependence—good and bad—on the digital world.

Entire swaths of society, including [classes we teach at American University](#), have moved online until the coast is clear. As vast segments of society are temporarily forced into isolation to achieve [social distancing](#), the internet is their window into the world. Online [social events](#) like virtual happy hours foster a sense of connectedness amid social distancing. While the online world is often portrayed as a societal ill, this pandemic is a reminder of how much the [digital world](#) has to offer.

The pandemic also lays bare the many vulnerabilities created by society's dependence on the internet. These include the dangerous consequences of censorship, the constantly morphing spread of disinformation, supply chain vulnerabilities and the risks of weak cybersecurity.

1. China's censorship affects us all

The global pandemic reminds us that even [local censorship can have global ramifications](#). [China's early suppression of coronavirus information](#) likely contributed to what is now a worldwide pandemic. Had the doctor in Wuhan who spotted the outbreak been able to speak freely, public [health](#) authorities might have been able to do more to contain it early.

China is not alone. Much of the world lives in countries that impose [controls on what can and cannot be said about their governments online](#). Such censorship is not just a free speech issue, but a public health issue as well. Technologies that circumvent censorship are increasingly a matter of life and death.

2. Disinformation online isn't just speech—it's also a matter of health and safety

During a public health emergency, sharing accurate information rapidly is critical. Social media can be an effective tool for doing just that. But it's also a source of disinformation and manipulation in ways that can threaten global health and personal safety—something tech companies are desperately, yet imperfectly, trying to combat.

Facebook, for example, has banned ads selling face masks or [promising false preventions or cures](#), while giving the World Health Organization unlimited ad space. Twitter is placing links to the Centers for Disease Control and Prevention and other reliable information sources atop search returns. Meanwhile, Russia and others [reportedly are spreading rumors](#) about the coronavirus's origins. Others are using the coronavirus to spread [racist vitriol](#), in ways that put individuals at risk.

Not only does COVID-19 warn us of the costs—and geopolitics—of disinformation, it highlights the roles and responsibilities of the private sector in confronting these risks. Figuring out how to do so effectively, without suppressing legitimate critics, is one of the greatest challenges for the next decade.

3. Cyber resiliency and security matter more than ever

Our university has moved our work online. We are holding meetings by video chat and conducting virtual courses. While many don't have this luxury, including those on the front lines of health and public safety or newly unemployed, thousands of other [universities](#), [businesses](#) and other institutions also moved online—a testament to the benefits of technological innovation.

At the same time, these moves remind us of the importance of strong encryption, reliable networks and effective cyber defenses. Today

network outages are not just about losing access to Netflix but about losing livelihoods. Cyber insecurity is also a threat to public health, such as when [ransomware attacks disrupt entire medical facilities](#).

4. Smart technologies as a lifeline

The virus also exposes the promise and risks of the "internet of things," the globe-spanning web of always-on, always-connected cameras, thermostats, alarm systems and other physical objects. Smart thermometers, blood pressure monitors and other medical devices are increasingly connected to the web. This makes it easier for people with pre-existing conditions to manage their health at home, rather than having to seek treatment in a medical facility where they are at much greater risk of exposure to the disease.

Yet this reliance on the internet of things carries risks. Insecure smart devices can be co-opted to disrupt democracy and society, such as when the [Mirai botnet hijacked home appliances](#) to disrupt critical news and information sites in the fall of 2016. When digitally interconnected devices are attacked, their benefits suddenly disappear—adding to the sense of crisis and sending those dependent on connected home diagnostic tools into already overcrowded hospitals.

5. Tech supply chain is a point of vulnerability

The shutdown of Chinese factories in the wake of the pandemic interrupted the supply of critical parts to many industries, including the U.S. tech sector. Even Apple had to temporarily [halt production](#) of the iPhone. Had China not begun to recover, the toll on the global economy could have been even greater than it is now.

This interdependence of our supply chain is neither new nor tech-

specific. Manufacturing—medical and otherwise—has long depended on parts from all over the world. The crisis serves as a reminder of the global, [complex interactions](#) of the many companies that produce gadgets, phones, computers and many other products on which the economy and society as a whole depend. Even if the virus had never traveled outside of China, the effects would have reverberated—highlighting ways in which even local crises have global ramifications.

Cyber policy in everything

As the next phase of the pandemic response unfolds, society will be grappling with more and more difficult questions. Among the many challenges are complex choices about how to curb the spread of the disease while preserving core freedoms. How much tracking and surveillance are people willing to accept as a means of protecting public health?

As Laura explains in "[The Internet in Everything](#)," cyber policy is now entangled with everything, including health, the environment and consumer safety. Choices that we make now, about cybersecurity, speech online, encryption policies and product design will have dramatic ramifications for health, security and basic human flourishing.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: Society's dependence on the internet: 5 cyber issues the coronavirus lays bare (2020, March 30) retrieved 19 April 2024 from <https://techxplore.com/news/2020-03-society-internet-cyber-issues-coronavirus.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.