SCHOLARS
STRATEGY NETWORK

How Cybercrimes Challenge Law Enforcement

Diana S. Dolliver, University of Alabama

The cyber-world brings global connections to local settings, transforming the ways we interact with one another. The benefits are many for each person and society. Barriers are bridged, and people have an easier time gaining access to information, connections, and a full range of legitimately offered goods and services. But there is a concerning downside to the cyber-world as well, because it spreads illegitimate goods and services and makes it easier for criminals to operate across national boundaries as well as within them.

Cybercrimes add new dimensions to illegality and violent threats that law enforcement officials and policymakers struggle to address. Such crimes can be especially worrisome because they are often asymmetrical – in that one person or small group can wreak as much damage as it once took an entire army to cause. What is more, the offender does not have to be physically anywhere near the victim. When the crime happens, the offender may be thousands of miles or continents away and thus very hard to track down.

What are Cybercrimes?

Cybercrime is a broad term encompassing acts committed or facilitated by the use of computer technology. In some instances, the perpetrator must have special knowledge of the Internet to commit the crime, while in others computer programs are used to achieve criminal goals.

- Some cybercrimes are simply new variants of traditional forms of wrongdoing – such as theft and fraud – where computers are used to steal personal identifications, passwords, and credit card information.

- In more sophisticated cybercrimes, computers may be sabotaged – as in denial of service attacks – or turned into agents of espionage. Viruses or other devices are often hidden in seemingly legitimate emails or advertisements on the web, which infect a computer once a user clicks on an email or link. After the computer has been infected, victims may be unable to use their computers or gain access to certain websites or documents.

- In the case of "Trojan horse" attacks, the criminal hacker may be able to gain remote access to the computer system and view the user's screen or web camera, or even take control of the entire computer from a remote location. Hackers typically use methods such as these to gain access to government computer systems, commercial databases, and other large targets containing information they can use for illicit purposes.

Cybercrimes can also involve illicit trade or the commissioning of criminal acts. Cybercriminal child pornography rings are currently expanding, used by organized crime groups around the world. Extremely serious crimes like murder for hire and killing to harvest organs are sometimes facilitated by the use of the "Deep Web," which is also sometimes referred to as the "Dark Net."

The Deep Web refers to information that a standard Internet search engine like *Google.com* or *Yahoo.com* cannot find. Anonymity is the name of the game, and special software is often needed to gain access. To find what they seek, individuals using this approach must know exactly what they are looking for and how to find it. Some researchers have termed the Deep Web the "secret Internet for bad guys." Much more remains to be learned about the extent to which organized criminal groups use the Deep Web to expedite and spread longstanding illegal activities such as drug trafficking, human trafficking, and manufacturing counterfeit products.

Special Concerns for Law Enforcement

The asymmetrical nature of cybercrime calls out for new approaches to combating crime. If one person can become as powerful as an entire army, countries can no longer rely solely on more reactive methods. Traditionally, threats to national borders lead to the concentration of law enforcement agents or military

personnel at border crossings and points of entry. Similarly, many criminal threats are met with the deployment of extra police in a neighborhood. Now, given the access and ease of the Internet, every person who has a computer, a Smartphone, or any other device that can connect to the Internet is a potential point of entry into a country. As organizations like the United Nations emphasize, transnational organized crime spans national and ethnic boundaries; and local police jurisdictions must also be alert to cybercriminals operating across state and regional lines. Security officials and law enforcement agencies alike must place a new emphasis on preventive intelligence to locate sources of potential cyber threats to the organizations and people they are supposed to protect.

Fragmented Policy Responses

Because cybercrimes are relatively new, so are the responses by legislators and law enforcement authorities. Policy responses are in their infancy, under development at all levels of government. In the United States alone, there are more than fifty federal statutes that directly or indirectly address different aspects of cyber-security and cybercrime. Examples include the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, the Cyber Security Research and Development Act of 2002, and the E-Government Act of 2002. Tellingly, there is no single piece of comprehensive U.S. legislation that encompasses all aspects of cyber-related crime. Also, various federal agencies have created centers to address threats. The Department of Defense has its "Defense Cyber Crimes Center," while the Federal Bureau of Investigation has the "Internet Crime Complaint Center," and Immigration and Customs Enforcement has its "Cyber Crimes Center." Other federal agencies pursue investigations of particular kinds of cybercrime – such as the Drug Enforcement Administration's attempt to tackle the problem of illegal online sales of prescription drugs through fake pharmacies. Both laws and enforcement efforts are scattered.

Searching for the Right Balance

Policymakers struggle with what to do about dangerous or illicit information on the web. For instance, terrorists have learned how to construct crude bombs from information on the Internet, and drug addicts have found new ways to purchase illegal substances. But does this mean national governments should limit their citizens' access to the Internet? Authoritarian countries such as China have already taken such steps, but democratic societies must find a more appropriate balance between personal freedoms and crime control. How this can be done remains to be seen, but there is no question that cybercrimes including terrorism are at the forefront of concern for governments and law enforcement agencies around the world.