Congressional Research Service
Informing the legislative debate since 1914

Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement

Kristin Finklea
Specialist in Domestic Security

Catherine A. Theohary
Specialist in National Security Policy and Information Operations

January 15, 2015

Congressional Research Service
7-5700
www.crs.gov
R42547

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Twenty-first century criminals increasingly rely on the Internet and advanced technologies to further their criminal operations. These criminals can easily leverage the Internet to carry out traditional crimes such as distributing illicit drugs and sex trafficking. In addition, they exploit the digital world to facilitate crimes that are often technology driven, including identity theft, payment card fraud, and intellectual property theft. Cybercrimes have economic, public health, and national security implications, among others. For over three decades, Congress has been concerned about cybercrime and its related threats. Today, these concerns often arise among a larger discussion surrounding the federal government's role in ensuring U.S. cyber security.

Conceptualizing cybercrime involves a number of key elements and questions that include *where* do the criminal acts exist in the real and digital worlds (and what technologies are involved in carrying out the crimes), *why* are malicious activities initiated, and *who* is involved in carrying out the malicious acts?

- One way of viewing cybercrimes is that they may be digital versions of traditional, real world offenses. They could be considered traditional, or "real world," crimes if not for the incorporated element of virtual or cyberspace. In some instances, however, it may seem that law enforcement struggles to keep up with developments in the virtual world, which transform routine activities once driven by paper records in the real world. As a result, criminals are often prosecuted using laws intended to combat crimes in the real world.
- The distinction between cybercrime and other malicious acts in the virtual realm is the actor's motivation. Cyber criminals can exhibit a wide range of self interests, deriving profit, notoriety, and/or gratification from activities such as hacking, cyber stalking, and online child pornography. Without knowing the criminal intent or motivation, however, some activities of cyber criminals and other malicious actors may appear on the surface to be similar, causing confusion as to whether a particular action should be categorized as cyber*crime* or not. When referring to cybercrime incidents, terms such as cyber attack, cyber espionage, and cyber war are often loosely applied, and they may obscure the motives of the actors involved.
- Criminal attribution is a key delineating factor between cybercrime and other cyber threats. When investigating a given threat, law enforcement is challenged with tracing the action to its source and determining whether the actor is a criminal or whether the actor may be a terrorist or state actor posing a potentially greater national security threat. This is highlighted by examining the online collective known as *Anonymous*. Some refer to Anonymous as a group of online activists, others see the collective as a group of criminal actors, and still others have likened it to online insurgents.

The U.S. government does not appear to have an official definition of cybercrime that distinguishes it from crimes committed in what is considered the real world. Similarly, there is not a definition of cybercrime that distinguishes it from other forms of cyber threats, and the term is often used interchangeably with other Internet- or technology-linked malicious acts. Federal law enforcement agencies often define cybercrime based on their jurisdiction and the crimes they are charged with investigating. And, just as there is no overarching definition for cybercrime,

there is no single agency that has been designated as the lead investigative agency for combating cybercrime.

Congress may question whether it is necessary to have a clear definition of what constitutes cybercrime and what delineates it from other real world and cyber threats. On one hand, if the purpose of defining cybercrime is for investigating and prosecuting any of the various crimes under the broader cybercrime umbrella, it may be less critical to create a definition of the umbrella term and more imperative to clearly define which specific activities constitute crimes—regardless of whether they are considered real world crimes or cybercrimes. On the other hand, a distinction between cybercrime and other malicious activities may be beneficial for creating specific policies on combating the ever-expanding range of cyber threats. If government agencies and private sector businesses design strategies and missions around combating cybercrime, it may be useful to communicate a clear definition of cybercrime to those individuals who may be involved in carrying out the strategies.

The United States does not have a national strategy exclusively focused on combating cybercrime. Rather, there are other, broader strategies that have cybercrime components (a selection of which are presented in the **Appendix**). Policy makers may question whether there should be a distinct strategy for combating cybercrime or whether efforts to control these crimes are best addressed through more wide-ranging strategies such as those targeting cyber security or transnational organized crime. Congress may also question whether these broader strategies provide specific cybercrime-related objectives and clear means to achieve these goals.

Comprehensive data on cybercrime incidents and their impact are not available, and without exact numbers on the current scope and prevalence of cybercrime, it is difficult to evaluate the magnitude of the threats posed by cyber criminals. There are a number of issues that have prevented the accurate measurement and tracking of cybercrime. For one, the lack of a clear sense of what constitutes cybercrime presents a barrier to tracking inclusive cybercrime data. Additionally, much of the available data on cybercrime are self-reported, and individuals or organizations may not realize a cybercrime has taken place or may elect—for a host of reasons—not to report it. Policy makers may debate whether to direct a thorough evaluation of the threats posed by cyber criminals.

Contents

Appendixes

Contacts

Background

Twenty-first century criminals increasingly rely on the Internet and advanced technologies to further their criminal operations. According to Europol's Organized Crime Threat Assessment, "Internet technology has now emerged as a key facilitator for the vast majority of offline organised crime activity."[1] For instance, criminals can easily leverage the Internet to carry out traditional crimes such as distributing illicit drugs and sex trafficking. In addition, they exploit the digital world to facilitate crimes that are often technology driven, including identity theft, payment card fraud, and intellectual property theft. The Federal Bureau of Investigation (FBI) considers high-tech crimes to be the most significant crimes confronting the United States.[2] Policy makers have shown an increasing interest in ensuring the federal government has the tools and capabilities to combat modern day crime—particularly those with cyber components—while safeguarding privacy rights.[3]

Today's cyber criminals "have evolved their practices to make their crimes more profitable.... [T]hey choose specialties, master their skills, create networks of colleagues, and organize their crimes."[4] These criminals can victimize individuals and organizations alike. They are motivated by self interest and profit. One estimate has placed the annual cost of cybercrime to adults in 24 countries across the globe at $113 billion.[5] In addition to the economic impact, cybercrimes can have public health and national security consequences, among others.

U.S. officials face the challenging task of identifying the perpetrators of malicious cyber incidents in which victim and criminal can be far removed from one another. The person or persons behind an incident can range from lone actors to expansive criminal networks or even nation states. This challenge of actor attribution is further compounded by the anonymity afforded by the digital realm. It can sometimes be difficult to determine the actor's motivation—is the criminal driven by greed or glory in the form of recognition among fellow criminals in the cyber world, or does the criminal have broader ideological motives? Finding the answers to these questions is key to distinguishing between cybercrimes and other cyber threats such as cyber attacks, cyber espionage, and cyber warfare. Relevant distinctions exist between these various malicious activities in the cyber domain just as lines have been drawn between their real world counterparts.

For over three decades, Congress has been concerned about cybercrime and its related threats.[6] Today, these concerns often arise among a larger discussion surrounding the federal government's

[1] Europol, *EU Internet Organized Threat Assessment: iOCTA 2011*, File No. 2530-274, April 28, 2011, p. 6.

[2] See remarks by James B. Comey, Director, Federal Bureau of Investigation before the RSA Cyber Security Conference, San Francisco, CA, February 26, 2014. Hereinafter: Comey, RSA Cyber Security Conference.

[3] See, for example, U.S. Congress, Senate Committee on the Judiciary, *Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime*, 113th Cong., 2nd sess., February 4, 2014.

[4] Steven R. Chabinsky, Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation, GovSec/FOSE Conference, Washington, DC, March 23, 2010. Hereinafter: Chabinsky, GovSec/FOSE Conference.

[5] Norton, Symantec Corporation, "2013 Norton Report: Cost per Cybercrime Victim Up 50 Percent," press release, October 1, 2013. This $113 billion is the self-reported direct financial losses to cybercrime.

[6] The original version of the Computer Fraud and Abuse Act was passed as part of the Comprehensive Crime Control Act of 1984 (P.L. 98-473). Prior to this, hearings were held over several Congresses. For more information, see CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle.

role in ensuring cyber security. This report discusses the concept of cybercrime and related cyber threats such as cyber espionage and cyber warfare. While it touches on these related threats, this report only does so in the context of framing the discussion of cybercrime.[7] It questions whether—and under what circumstances—clear distinctions between the various threats should be delineated. The report also outlines how current federal strategies may address cybercrime. It raises issues surrounding the measurement and tracking of cybercrime. Throughout, it discusses whether a clearer understanding of what constitutes cybercrime as well as its prevalence and harm could better equip policy makers to debate the sufficiency of federal law enforcement resources available to counter cybercrime and to conduct oversight in this arena.

Conceptualizing Cybercrime

A singular, agreed-upon definition of cybercrime does not exist. Various definitions have been offered by industry experts and scholars, and several have been formulated within the federal government. Definitions have varied in their levels of specificity and breadth. For instance, one of the largest computer security companies, Symantec Corporation, defines cybercrime as "any crime that is committed using a computer or network, or hardware device."[8] Irrespective of the definition, conceptualizing cybercrime involves a number of key elements and questions, including *where* do the criminal acts exist in the real and digital worlds (and what technologies are involved), *why* are malicious activities initiated, and *who* is involved in carrying out the malicious acts? In the sections below, the questions of where, why, and who are discussed as they relate to cybercrime. This is followed by a discussion of government definitions of cybercrime and a debate on whether or when a common definition of cybercrime may be useful.

Where: Location of Criminal Activities, Actors, and Victims

The notion of location as it relates to cybercrime involves both the physical and digital domains. The relatively clear borders and locations within the physical world, however, are not replicated in the virtual realm. Of course, some distinct boundaries separate the physical and the cyber worlds; keyboard, mouse, screen, and password can all mediate between these physical and virtual realms.[9] Within cyberspace, however, the notion of a border is much more nebulous. This is, in part, because the same geographic borders that exist in the real world do not exist in the cyber world.[10]

Even without distinct borders, the digital world is linked to the physical world—as is crime involving the digital world. Take, for instance, point-of-sale (POS) skimming. This high-tech financial fraud involves placing a device over (or sometimes replacing) an existing card slot on a credit card reader or ATM. The device "relies on sophisticated data-reading electronics to copy the magnetic stripe information from [the] credit card or debit card. It can capture both [the]

[7] For more information on cyberwarfare and other cybersecurity issues, see CRS Report RL31787, *Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues*, by Catherine A. Theohary.

[8] Symantec Corporation, *What is Cybercrime?*, http://us.norton.com/cybercrime-definition.

[9] David R. Johnson and David Post, "Law and Borders - The Rise of Law in Cyberspace," *Stanford Law Review*, vol. 48 (May 1996), p. 1379.

[10] Ibid., p. 1370.

credit card number and [the] PIN."[11] Fraudsters can then retrieve the stolen information by physically collecting the skimming device or by programming the device to broadcast the data to thieves over a network.

Researchers have proposed that some cybercrimes may require more technological expertise or heavier use of digital technologies to perpetrate than others.[12] For example, phishing,[13] identity theft, and distributed denial of service (DDoS)[14] attacks necessitate a greater understanding of computing and digital technologies than others, such as cyber stalking and online child pornography, that can be thought of as "point and click" crimes. Those crimes requiring more technological expertise may also be more firmly rooted in the virtual world than others. Regardless, the cyber component may delineate them from traditional crimes. Computers and other advanced technologies may be components of cybercrime through a variety of roles:

- in some cybercrimes, computers themselves—or data contained therein—are the victims or targets of crime;
- in other instances, computers or other digital technologies are used as tools for carrying out crimes (victimizing individuals, organizations, or government); and
- technological devices may serve as repositories for evidence of a cybercrime.[15]

All of these issues underscore the salience of location in any conceptualization of cybercrime.

Technology: Cyber vs. Real World Crime

Perhaps one way of viewing cybercrimes is that they are digital versions of traditional offenses.[16] It appears that many cybercrimes could be considered traditional, or real world, crimes if not for the incorporated element of virtual or cyberspace. Indeed, many of these so-called cybercrimes can be easily likened to traditional crimes. For instance, identity theft can occur in both physical and cyber arenas. While these crimes may occur through differing mechanisms, in both circumstances the criminal intent (profit) and outcome (stolen personally identifiable information) are the same.

---

[11] Robert Vamosi, "Keep Your Credit Cards Safe From Skimmers," *PC World*, December 8, 2010.

[12] Sarah Gordon and Richard Ford, "On the definition and classification of cybercrime," *Journal of Computer Virology*, vol. 2 (July 2006), pp. 15 – 19.

[13] Phishing "is a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses. These authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers and passwords, credit card numbers and Social Security numbers," Computerworld, January 19, 2004, http://www.computerworld.com/s/article/89096/Phishing.

[14] A denial-of-service attack attempts to prevent legitimate users from accessing a resource – in this case a network or website. This is most commonly done by "flooding" a network with information and overloading the server with so many requests for information that it cannot process other, legitimate requests. A distributed denial-of-service (DDoS) attack utilizes other computers—often from unwitting individuals—to assist in flooding a network. For more information, see the U.S. Computer Emergency Readiness Team, http://www.us-cert.gov/cas/tips/ST04-015.html.

[15] According to the Homeland Security Newswire, "[t]he ubiquity of this [electronic] technology [such as cell phones and computer files] has often provided investigators with an electronic trail that gives prosecutors concrete analytical evidence for nearly every crime." "An Electronic Trail for Every Crime," *Homeland Security Newswire*, April 19, 2011, http://homelandsecuritynewswire.com/electronic-trail-every-crime.

[16] Susan Brenner, "Thoughts, Witches and Crimes," *CYB3RCRIM3: Observations on Technology, Law, and Lawlessness*, May 6, 2009, http://cyb3rcrim3.blogspot.com/2009/05/thoughts-witches-and-crimes.html.

- In the real world, a criminal can steal a victim's wallet or mail including documents containing personally identifiable information. In one case from March 2014, two defendants were charged for their role in a conspiracy to "steal mail containing credit debit cards.... The defendants then used the stolen debit cards to obtain cash, without the knowledge or authorization of the identity theft victims."[17] In another case, two men were sentenced for leading a criminal enterprise that stole credit and debit cards from mailboxes in affluent neighborhoods in South Florida. The thieves then used the cards to make large purchases and cash withdrawals from the cards, costing victims $786,000.[18]
- In the cyber world, a computer hacker can easily steal this same PII—electronically rather than physically. In September 2013, two Romanian nationals were sentenced for "participating in an international, multimillion-dollar scheme to remotely hack into and steal payment card data from hundreds of U.S. merchants' computers." Defendants remotely hacked into POS systems and then, also remotely, installed "keystroke loggers." These devices illegally captured victims' credit card information when the cards were swiped by the merchants, and then this information was transferred electronically to the fraudsters. The defendants stole information from more than 100,000 victims and sold this information for a profit.[19]

In some instances, it may seem that law enforcement struggles to keep up with developments in the virtual world, which transform routine activities once driven by paper records in the real world. As a result, criminals are often prosecuted using laws intended to combat crimes in the real world. As Department of Justice (DOJ) officials have pointed out, federal laws to prosecute computer-related crimes are not necessarily as ample or broad as those used to confront their traditional counterparts.[20] For instance, computer fraud (18 U.S.C. §1030) is not currently considered a predicate offense for racketeering under the Racketeer Influenced Corrupt Organizations (RICO) Act—one of the primary tools used to prosecute organized crime.[21] As noted, organized criminals are increasingly using the Internet and other advanced technologies to carry out their operations. Yet, the range of crimes carried out by organized crime encompasses both traditional and cybercrimes. The Obama Administration has recommended revising RICO provisions (which can be applied to both criminal and civil cases) so that computer fraud would be considered a predicate offense.[22] Cyber criminal organizations have been targeted under civil

[17] U.S. Attorney's Office, Southern District of Florida, "Twenty-Five Defendants Charged in Separate Schemes That Resulted in Thousands of Identities Stolen and Millions of Dollars in Identity Theft Tax Filings," press release, April 3, 2014.

[18] U.S. Department of Justice, "Two Wellington Men Sentenced in Mail and Aggravated Identity Theft Ring," press release, April 26, 2011; Wayne K. Roustan, "Two Plead Guilty to ID Theft That Cost Victims $786,000: They Admit Stealing Credit and Debit Cards from Mailboxes," February 12, 2011.

[19] U.S. Department of Justice, "Two Romanian Nationals Sentenced to Prison for Scheme to Steal Payment Card Data," press release, September 14, 2013.

[20] Statement for the Record of James A. Baker, Associate Deputy Attorney General, Department of Justice before the U.S. Congress, House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, *Cybersecurity: Innovative Solutions to Challenging Problems*, 112th Cong., May 25, 2011, http://judiciary.house.gov/hearings/pdf/Baker05252011.pdf.

[21] For more information on RICO, see CRS Report 96-950, *RICO: A Brief Sketch*, by Charles Doyle. The predicate offenses for racketeering include a host of state and federal crimes listed in 18 U.S.C. §1961.

[22] The White House, *Law Enforcement Provisions Related to Computer Security*, May 12, 2011, p. 2, http://www.whitehouse.gov/omb/legislative_letters. Legislation (e.g., the Cyber Crime Protection Security Act, S. (continued...)

RICO, citing predicate offenses such as wire fraud, bank fraud, and access device fraud.[23] It is unknown whether or how adding computer fraud to the list of predicate offenses would further these investigations and prosecutions.

- In June 2014, the GameOver Zeus botnet,[24] was disrupted through an international law enforcement effort led by the FBI. Law enforcement was authorized to sever communication between infected computers and criminal servers.[25] GameOver Zeus is the most recent variant of the Zeus Botnet, which would steal online banking information and transfer funds to money mules, or U.S. residents with bank accounts, who would move the money out of the United States. Officials also indicted an alleged administrator of GameOver Zeus, "charging him with conspiracy, computer hacking, wire fraud, bank fraud, and money laundering."[26]

Borders and Cyberspace

Criminals operate in the cyber world partly to circumvent more conventional, established constructs such as international borders.[27] In the virtual realm, criminals can rely on relative anonymity and a rather seamless environment to conduct business. High-speed Internet communication has not only facilitated the growth of legitimate business, but it has bolstered criminals' abilities to operate in an environment where they can broaden their pool of potential targets and rapidly exploit their victims. Between December 2000 and June 2014, the estimated number of Internet users grew from almost 361 million to nearly 7.2 billion—an increase of more than 741%.[28] Frauds and schemes that were once conducted face-to-face can now be carried out remotely from across the country or even across the world. Despite criminals exploiting virtual space, the criminal actor and the victim(s) are located in the real world—though often in different cities, states, or even countries. Similarly, the digital technologies used to facilitate these crimes, such as Internet servers and digital communication devices, are located in physical locations that may not coincide with the locations of the criminal actors or victims. As such, law enforcement faces not only technological but jurisdictional challenges in investigating and prosecuting cyber criminals.

(...continued)

2111) introduced in the 112th Congress would, among other things, make computer fraud and related crimes under 18 U.S.C. §1030 predicate offenses under RICO.

[23] "Microsoft Takes Down Dozens of Zeus, SpyEye Botnets," *Krebs on Security*, March 26, 2012. See also *Microsoft Corp., FS-ISAC, Inc., and National Automated Clearing House Association v. John Does 1-39*, (U.S. District Court, Eastern District of New York), http://www.zeuslegalnotice.com/images/Complaint_w_Appendices.pdf.

[24] Botnets are groups of computers that are remotely controlled by hackers. They have been infected by downloading malicious software and are used to carry out malicious activities on behalf of the hackers.

[25] U.S. Department of Justice, "U.S. Leads Multi-National Action Against GameOver Zeus Botnet and Cryptolocker Ransomware, Charges Botnet Administrator," press release, June 2, 2014.

[26] U.S. Department of Justice, "U.S. Leads Multi-National Action Against GameOver Zeus Botnet and Cryptolocker Ransomware, Charges Botnet Administrator," press release, June 2, 2014.

[27] For more information on the issue of borders in cyberspace, see CRS Report R41927, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, by Kristin Finklea.

[28] Internet World Stats, *Internet Usage Statistics, The Internet Big Picture, World Internet Users and Population Stats*, http://www.internetworldstats.com/stats.htm.

Conceptualizing Cyberspace

In determining what constitutes cybercrime, it may be beneficial to outline what constitutes cyberspace. After determining what constitutes the cyber realm, then boundaries for permissible behavior—as it intersects with this space—can be outlined.

The National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) defines cyberspace as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." In other words, cyberspace is the "virtual environment of information and interactions between people."[29] The U.S. military has adopted a definition of cyberspace consistent with that laid out in NSPD-54/HSPD-23. A recently published document of the Department of Defense defined cyberspace as "[a] global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."┐ It is unknown whether federal law enforcement also utilizes the definition of cyberspace—as outlined in NSPD-54/HSPD-23—in its conceptualization of what constitutes cybercrime and for purposes of cybercrime investigations and prosecutions.

As noted by one expert, cyberspace "is not a fixed, predetermined reality operating according to principles and dynamics that cannot be controlled or altered by man. The cyberworld is a constructed world, a fabrication. Because it is a construct, cyberspace is mutable; much of it can be modified and transformed."[30] Criminal actors do not exist in cyberspace. Rather, they exist in the physical world and their actions traverse the real world as well as cyberspace, impacting victims in the real world. In this vein, criminals may rely upon cyberspace as a marketplace to help carry out malicious activities, but they—and their victims—remain in the physical world.

Why: Motivation

The distinction between cybercrime and other cyber-based malicious acts such as terrorism or state sponsored espionage is the actor's *motivation*. Cyber criminals can exhibit a wide range of self interests, deriving profit, notoriety, and/or gratification from activities such as hacking, cyber stalking, and online child pornography. As one FBI agent specializing in cybercrime has reportedly stated, "[h]acking into a company, whether it's to put information on the web for everyone to see or if you're going to make money, is still hacking, it's still a crime."[31] Without knowing the criminal intent or motivation, however, some activities of cyber criminals and other malicious actors may appear on the surface to be similar, causing confusion as to whether a particular action should be categorized as cyber*crime* or not. As noted in the National Strategy to Secure Cyberspace, "[t]he speed and anonymity of cyber attacks makes distinguishing among the

[29] National Security Agency, *Statement for the Record, Lieutenant General Keith Alexander, Commander, Joint Functional Component Command for Network Warfare*, Before the House Armed Services Committee, Terrorism, Unconventional Threats, and Capabilities Subcommittee, May 5, 2009, http://www.nsa.gov/public_info/speeches_testimonies/5may09_dir.shtml.

[30] Susan W. Brenner, "Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships," *North Carolina Journal of Law & Technology*, vol. 4, no. 1 (Fall), p. 37.

[31] Dominic Rushe, "FBI Fights Back Against Cybercrime," *The Guardian*, August 24, 2011, http://www.guardian.co.uk/technology/2011/aug/24/us-agency-fights-back-against-cybercrime.

actions of terrorists, criminals, and nation states difficult, a task which often occurs only after the fact, if at all."[32] This challenge of attribution is discussed in detail in the section "Who: Attribution."

The FBI has noted three primary categories of cyber threat actors:

> [1] organized crime groups that are primarily threatening the financial services sector, and they are expanding the scope of their attacks; [2] state sponsors—foreign governments that are interested in pilfering data, including intellectual property and research and development data from major manufacturers, government agencies, and defense contractors; and [3] increasingly there are terrorist groups who want to impact this country the same way they did on 9/11 by flying planes into buildings. They are seeking to use the network to challenge the United States by looking at critical infrastructure to disrupt or harm the viability of our way of life.[33]

Of these three categories outlined by the FBI, the first—organized crime groups—focuses on cybercrime. However, this category appears limited to those crimes that target the financial services sector. While the second category includes the theft of intellectual property and other activities that may be considered cybercrimes, this category is more roughly aligned with state-sponsored espionage. As such, the FBI's conceptualization of cybercrime surrounds the activities—primarily financial—of organized crime groups. This may exclude lone actors including hackers, stalkers, and online child predators. The FBI considers these malicious activities under the umbrella of cybercrime, as discussed in the "Government Definitions and Agency Focus" section of this report, but the classification noted above suggests that the FBI may prioritize investigation of criminal organizations engaging in cybercrime over lone actors.

While there is a clear distinction that organized crime groups are motivated by profit and terrorists are motivated by ideologies, the motivation of state sponsored cyber threat actors may be more difficult to categorize and determine. This may be in part because different state sponsored actors may have different motivations, as is implied by the FBI description of the range of state sponsored cyber threats. For instance, some actors targeting the intellectual property of manufacturers and corporations may aim to gain a competitive advantage for businesses based in a particular country. Others actors seeking data from government agencies and contractors may desire to utilize this information to undermine the integrity and security of a rival nation. This is the distinction between the theft of trade secrets and the theft of state secrets. Nonetheless, in some cases, state actors' actions look much like those of profit-driven criminals.

Blurring Lines Between Cybercrime and Related Threats

When referring to cybercrime incidents, terms such as cyber attack and cyber war are often loosely applied, and they may obscure the motives of the actors involved. Blurring of concepts occurs in other areas as well. The terms cyber espionage or exploitation and cyber attack are often used interchangeably, although they may refer to distinct sets of activities that are governed by different laws, regulations, or strategies. However, there are areas where these activities may overlap, causing confusion over the applicable governing structure. Experts have cautioned that

[32] Department of Homeland Security, *National Strategy to Secure Cyberspace*, February 2003, p. viii, http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

[33] Federal Bureau of Investigation, *The Cyber Threat: Part 1: On the Front Lines With Shawn Henry*, March 27, 2012, http://www.fbi.gov/news/stories/2012/march/shawn-henry_032712/shawn-henry_032712.

overuse of the term cyber war or information warfare when referring to cybercrime may sensationalize certain cybercrimes that are threats to public security but not necessarily threats to national security.[34]

Organized Criminals in Cyberspace—A National Security Threat

Significant threats posed by cybercrime may be considered matters of national and economic security. For instance, the White House, through the Strategy to Combat Transnational Organized Crime (Strategy), has indicated that cybercrime "costs consumers billions of dollars annually, threatens sensitive corporate and government computer networks, and undermines worldwide confidence in the international financial system."[35] Criminal networks rely on cyber technologies to carry out sophisticated frauds costing individuals and businesses billions of dollars. The Strategy notes that over the course of one year, Central European cybercrime networks alone have defrauded U.S. persons and businesses of about $1 billion.[36]

- In one case, members of a cybercriminal network (spanning countries including Romania, the Czech Republic, the United Kingdom, and Canada) are alleged to have participated in a cyber fraud scheme defrauding individuals making large purchases on Internet marketplaces. The co-conspirators would reportedly post items for sale, including "cars, motorcycles, boats, and other high-value items generally priced in the $10,000 to $45,000 range. Unbeknownst to the buyers, however, the merchandise did not exist."[37] They are suspected of duping their victims out of more than $3 million.
- In another case, one network of hackers—from countries including Estonia, Russia, and Moldova—reportedly hacked the RBS WorldPay computer network. These individuals allegedly defeated the encryption used by RBS WorldPay to protect customer information associated with the payroll card processing system. Using counterfeit payroll debit cards—cards that allow employees to withdraw their regular salaries from ATMs—the hackers and their associates withdrew more than $9.4 million from over 2,100 ATMs across at least 280 cities around the globe—including in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan, and Canada. Notably, the over $9 million loss occurred in under 12 hours. In October 2014, a leader of this network was sentenced "for conspiracy to commit wire fraud and computer intrusion."[38]

[34] David L. Speer, "Redefining Borders: The Challenges of Cybercrime," *Crime, Law and Social Change*, vol. 34, no. 3 (October 2000), p. 260.

[35] The White House, *Strategy To Combat Transnational Organized Crime: Addressing Converging Threats to National Security*, July 2011, p. 7, http://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf.

[36] Ibid., p. 7.

[37] U.S. Department of Justice, "Romanian National Aurel Cojocaru Extradited From Czech Republic To United States To Face Charges Related To Multimillion Dollar International Cyber Fraud Scheme," press release, November 7, 2013.

[38] U.S. Department of Justice, "International Hacker Sentenced," press release, October 24, 2014.

Cyber Espionage—Profit vs. State Direction

Espionage conducted in cyberspace is in many ways akin to traditional forms of espionage, the unauthorized access to confidential information by an individual or government. Illicit exfiltration of networked information can be conducted for intelligence gathering purposes, financial gains, or a combination of the two. Cyber espionage—particularly that which targets trade secrets—can pose similar threats to national security. According to the Office of the National Counterintelligence Executive, "[f]oreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation's prosperity and security."[39] Cyber espionage targeting trade secrets can be considered either distinct from, or a form of, cybercrime depending upon the actor and the actor's motivation. Economic[40] and industrial espionage[41] (or theft of trade secrets) financially burden U.S. companies that lose valuable intellectual property and incur costs in remediating the damage from the theft.

The use of technology for these purposes is nothing new; spying in cyberspace is a criminal activity as it is in other domains. However, the tools used to conduct cyber spying can be the same as those used to commit a host of disruptive or destructive acts that could range from online activism to criminal activity, and conceivably even an act of war.

- Consider the reported hacking of computer systems used in the design of the U.S. military's multipurpose fighter jet, the Joint Strike Fighter.[42] In some ways, this represents a typical case of industrial espionage in which plans for a company's product are illegally obtained and replicated. However, as a military platform it is difficult to ascertain whether its computerized operating systems were hacked in order to understand and replicate them or to plant malicious software that could conduct military surveillance, or potentially disrupt or destroy the platform's ability to function. Complicating this is the lack of clear attribution for the perpetrators. Although the security breach appeared to have origins in China, without an understanding of whether it was sponsored by a foreign government or military, it is difficult to categorize whether the hacking was merely a criminal

[39] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, October 2011, p. i.

[40] 18 U.S.C. §1831. Economic espionage is "(a) In General—Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly – (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in any of paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy."

[41] 18 U.S.C. §1832. Theft of trade secrets is when an individual "knowingly – (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; (4) attempts to commit any offense described in paragraphs (1) through (3); or (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy."

[42] First reported in The Wall Street Journal, Siobhan Gorban, August Cole, and Yochi Dreazen, *Computer Spies Breach Fighter Jet Program*, April 21, 2009.

activity or part of what could be considered an economic espionage campaign.[43] For its part, officials from the People's Republic of China have denied responsibility, stating that all forms of computer hacking are illegal in China, and that the government has difficulty in controlling computer crime within its own borders.

Cyber Warfare

Three international incidents involving Estonia, Georgia, and Iran have influenced discussions of what distinguishes cyber warfare from related cyber threats. In 2007, a series of distributed denial of service (DDOS) attacks were launched on Estonian websites and networked services. Although it appeared that the attacks may have come from Russia, some of the IP addresses involved were traced to ethnic Russians living within Estonian borders.[44] Without a definition of what constitutes an "armed attack" in cyberspace and where territorial boundaries exist, and without attribution to a nation state, some considered the Estonian cyber attacks to be more of a cyber riot than a war. Some considered it the electronic equivalent to a real world sit-in, in that traffic to particular sites was analogously slowed down or blocked by organized citizens wishing to make a political statement or influence events. Others have likened it to a form of cyber terrorism, another term for which no consensus definition exists.[45] Ultimately, although various groups have claimed credit for the attacks, investigations led to only one conviction in an Estonian criminal court of an ethnic Russian student.

Soon after the Estonian incident, there was a series of strategic cyber attacks that disabled Georgian command and control systems in 2008. This coincided with a Russian military incursion across the Georgian border. As the cyber disruption occurred simultaneously with a kinetic event, some considered this to be a form of network warfare. Some questioned whether this disruption was an act of cyber warfare by the Russians or a separate cyber threat. Investigations later determined that the attacks began with online Russian hacking forums, who distributed lists of Georgian Internet sites as targets.

In July 2010, a malicious software worm called Stuxnet attacked the operations of nuclear centrifuges in Iran.[46] Some assumed that only a nation state or states would have the intelligence apparatus and testing beds necessary to develop and deploy this malware. In addition, as the worm was designed to target and destroy particular systems without any financial or intelligence gain, Stuxnet may be considered a form of cyber weaponry rather than a different form of cyber threat such as cyber espionage or cybercrime.

[43] "Moonlight Maze" and "Titan Rain" are examples of cyber campaigns conducted against unclassified Department of Defense targets and directed by other governments. Probes may be used to test network defenses as well as to extract sensitive information, and may coincide with a country's interest in weakening U.S. command and control systems.

[44] For a country so wired that it is colloquially known as E-stonia, the attacks had such a crippling effect that Estonian government officials considered it a national security crisis. At the time, Estonia appealed to the Russian government for help under a Mutual Legal Assistance treaty, but was denied.

[45] For information on terrorist use of the Internet, see CRS Report R41674, *Terrorist Use of the Internet: Information Operations in Cyberspace*, by Catherine A. Theohary and John W. Rollins.

[46] See CRS Report R41524, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, by Paul K. Kerr, John W. Rollins, and Catherine A. Theohary.

Who: Attribution

The preceding section suggests that blurry lines between various types of malicious activity in cyberspace may make it difficult for investigators to attribute an incident to a specific individual or organization. Criminal attribution is a key delineating factor between cybercrime and other cyber threats. When investigating a given threat, law enforcement is challenged with tracing the action to its source and determining whether the actor is a criminal or whether the actor may be a terrorist or state actor posing a potentially greater national security threat.

Take, for example, the July–September 2011 attacks on private companies primarily involved in the chemical industry. In what has been dubbed the "Nitro" attacks, hackers sent phony emails to members of Fortune 100 companies, businesses developing advanced materials for military vehicles, and companies developing manufacturing infrastructure for the chemical industry.[47] The emails contained attachments with a malicious Trojan[48] called PoisonIvy, which ultimately allowed hackers access to other computers in the company workgroup as well as to needed passwords. They could then navigate to the targeted intellectual property, copy the content, and upload the information to servers external to the compromised organization. Because the victimized companies were involved in the research, development, and manufacture of chemicals and advanced materials, it may have initially been unclear whether the attacker was a terrorist attempting to procure chemicals or a hacker seeking corporate secrets. According to Symantec, the purpose of the attacks was likely industrial espionage, and the attackers appear to have been seeking intellectual property, including design documents, formulas, and manufacturing processes, for competitive advantage. The source of the attack was identified as a computer system owned by an individual—dubbed Covert Grove—in China.[49]

The attribution issue is highlighted in the November 2014 revelation of a breach at Sony Pictures Entertainment (SPE) by actors known as the "Guardians of Peace." The FBI, in its investigation of the breach, notes that it "consisted of the deployment of destructive malware and the theft of proprietary information as well as employees' personally identifiable information and confidential communications. The attacks also rendered thousands of SPE's computers inoperable, forced SPE to take its entire computer network offline, and significantly disrupted the company's business operations."[50] There has been debate among officials, scholars, reporters, and others about the true source of the breach. As of December 2014, the FBI—leading an interagency effort—had attributed the hack to North Korea. In its attribution, the FBI cites malware linked "to other malware that the FBI knows North Korean actors previously developed," "significant overlap between the infrastructure used in this attack and other malicious cyber activity the U.S. government has previously linked directly to North Korea," and tools similar to those used in a

[47] Eric Chien and Gavin O'Gorman, *The Nitro Attacks: Stealing Secrets from the Chemical Industry*, Symantec Security Response, 2011, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf.

[48] A Trojan is a type of malware. It is a type of software that, once activated, can damage the host and provide back doors for malicious users to access the computer system. For more information on the various types of malware, see Cisco, *What Is the Difference: Viruses, Worms, Trojans, and Bots?*, http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html.

[49] Eric Chien and Gavin O'Gorman, *The Nitro Attacks: Stealing Secrets from the Chemical Industry*, Symantec Security Response, 2011, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf.

[50] Federal Bureau of Investigation, "Update on Sony Investigation," press release, December 19, 2014.

2013 North Korean cyber attack against South Korean banks and media outlets.[51] Nonetheless, experts critical of this attribution note that the evidence linking North Korea to the SPE breach is not definitive.[52]

Attribution continues to be a challenge in identifying both public security and national security threats. In the 2012 Worldwide Threat Assessment of the U.S. Intelligence Community, James Clapper, Director of National Intelligence noted the challenges in cyber actor attribution. More specifically, he noted that

> [t]wo of our greatest strategic challenges regarding cyber threats are: (1) the difficulty of providing timely, actionable warning of cyber threats and incidents, such as identifying past or present security breaches, *definitively attributing them* [emphasis added], and accurately distinguishing between cyber espionage intrusions and potentially disruptive cyber attacks; and (2) the highly complex vulnerabilities associated with the IT supply chain for US networks.[53]

The FBI, for one, has bolstered its efforts to better attribute cyber threats to specific sources and motives. Through the Next Generation Cyber Initiative, the FBI is developing agents to connect with critical infrastructure components and computer scientists to "extract hackers' digital signatures" and determine their identities, all to help concretely attribute a specific malicious actor to a particular cyber incident.[54] Similarly, the Department of Defense has reportedly "made significant investments in forensics to address this problem of attribution."[55]

Attribution, however, may be more important for government and law enforcement than for private sector organizations. Law enforcement, through their investigations, may strive for attribution so that the actual perpetrator may be prosecuted. Industry organizations, however, may be less concerned and may focus more on damage control and prevention—regardless of the actor or his motivations.[56]

Case Study: Anonymous

The online collective known as "Anonymous" is a decentralized group operating in cyberspace. While scholars, theorists, law enforcement, and policy makers may not always agree on how to conceptualize or categorize the Anonymous entity, it is generally agreed that it operates with two

[51] Federal Bureau of Investigation, "Update on Sony Investigation," press release, December 19, 2014.

[52] See, for example, Andy Greenberg, "FBI Director: Sony's 'Sloppy' North Korean Hackers Revealed Their IP Addresses," *Wired: Threat Level*, January 7, 2015; Pierluigi Paganini, "Sony Pictures Hack: Is North Korea Innocent or Guilty?," *InfoSec Institute*, January 11, 2015; and Michael Sexton, "Accurately Attributing the Sony Hack is More Important than Retaliating," *Georgetown Security Studies Review*, January 13, 2015.

[53] Office of the Director of National Intelligence, *Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence*, January 31, 2012, p. 8.

[54] Federal Bureau of Investigation, "Cyber Security: Focusing on Hackers and Intrusions," press release, October 26, 2012, https://www.fbi.gov/news/stories/2012/october/cyber-division-focusing-on-hackers-and-intrusions/cyber-division-focusing-on-hackers-and-intrusions.

[55] U.S. Department of Defense, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," news transcript, October 11, 2012.

[56] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, October 2011, p. 1.

broad tenets: (1) personal anonymity and (2) the free flow of information.[57] Anonymous is a loosely formed organization to the extent that it cannot be easily categorized. For instance, membership may be fluid; the Anonymous structure—or lack thereof—allows for participation in a single campaign or in a variety of protest activities. Further, members may have different interests and motivations for participation, and may use differing forms of tactics—both legal and illegal. As such, some refer to Anonymous as a group of online activists, others see the collective as a group of criminal actors, and still others have likened it to online insurgents.[58]

Anonymous came into the spotlight in 2008 with its first united act of "hacktivism"[59] to protest the Church of Scientology. The church reportedly attempted to pressure Internet websites to remove a leaked video of actor Tom Cruise endorsing Scientology—a video that had only been intended for church viewing.[60] In response, Anonymous members banded together to make distributed denial-of-service (DDoS) attacks, amongst other things (such as prank calling, hosting proprietary church documents online, and sending excessive faxes to waste paper and ink) against the church.[61] This online protest later transitioned to physical protest, with masked activists gathering outside of Scientology compounds.[62] In another notable display of online hacktivism, Anonymous initiated DDoS attacks against PayPal, Mastercard, Amazon, and others in December 2010. This was in response to these companies pulling support and services for Wikileaks, which had publicly released a cache of diplomatic cables.[63]

The first instance of Anonymous hacking networks for the purpose of exposing data was against the security firm HBGary.[64] HBGary had reportedly uncovered the identities of Anonymous leaders and was planning to release this information to the FBI. Anonymous hacked into HBGary's servers and published the company's email online, exposing sensitive proprietary information.[65] Anonymous has since been involved in numerous incidents of data exposure to advance both political and social stances. In October 2011, Anonymous targeted online child pornography sites; after the Freedom Hosting server ignored Anonymous's warnings to remove links to illegal child pornography sites, the hacker collective infiltrated the server, took down over 40 child pornography websites, and exposed the names of nearly 1,600 active members of these sites.[66]

Some have even likened Anonymous to "the non-state insurgents the U.S. has faced in Iraq and Afghanistan—small groups of non-state actors using asymmetric means of warfare to destabilize

[57] From remarks by Gabriella Coleman, Professor, New York University, at The Brookings Institution, *Hacktivism, Vigilantism and Collective Action in a Digital Age*, November 9, 2011.

[58] From remarks by Paul Rosenzweig, Lecturer in Law, George Washington University, at The Brookings Institution, *Hacktivism, Vigilantism and Collective Action in a Digital Age*, November 9, 2011.

[59] Hacktivism is a term often used to refer to the use of computers and online networks to conduct politically or socially-motivated protest.

[60] E. Gabriella Coleman, "Anonymous: From the Lulz to Collective Action," *The New Everyday*, April 6, 2011.

[61] Ryan Singel, "War Breaks Out Between Hackers and Scientology—There Can Be Only One," *Wired: Threat Level*, January 23, 2008.

[62] James Harrison, "Scientology Protestors Take Action Around World," *The State News*, February 12, 2008.

[63] E. Gabriella Coleman, "Anonymous: From the Lulz to Collective Action," *The New Everyday*, April 6, 2011.

[64] From remarks by Gabriella Coleman, Professor, New York University, at The Brookings Institution, *Hacktivism, Vigilantism and Collective Action in a Digital Age*, November 9, 2011.

[65] "HBGary Federal Hacked by Anonymous," *KrebsOnSecurity*, February 7, 2011.

[66] "Anonymous Targets Child Porn Sites, Releases Names of 1,500 Members," *Homeland Security News Wire*, October 25, 2011.

and disrupt existing political authority."[67] Whereas traditional insurgencies may desire to weaken the control or legitimacy of an established government, some have suggested that the goals of the Anonymous "insurgents" may be slightly different. It has been posited that Anonymous actors—as insurgents—may desire independence from the government in the sense that government should not control the cyber domain.[68]

How groups like Anonymous are conceptualized may drive the policies and strategies adopted to address their actions. Is Anonymous a group of online activists, a collection of hacker criminals, or a cyber insurgency? And, because Anonymous is known to be a loosely connected organization, can all members and actors be assimilated into the same category? Members' differing goals and activities may require that a variety of conceptualizations be applied to Anonymous and that a range of strategies be employed to counter any illegal activities. In its counter-Anonymous activities to date, the U.S. government has primarily treated the collective as a criminal entity and has indicted and arrested individuals associated with specific hacking and data breach incidents.

- Individuals associated with Anonymous have been charged and sentenced for their roles in a distributed denial of service attack against the website of Angel Soft bathroom tissue, a subsidiary of Koch Industries. The defendants reportedly used a "'low orbit ion cannon' designed to flood the Angel Soft server with traffic with the intention of disrupting the website's service."[69] The attack supposedly cost the Koch Industries several hundred-thousand dollars in losses.
- In March 2012, the Department of Justice indicted six individuals in the United States and abroad for hacking and other crimes related to their participation in Anonymous and related groups.[70] The indictment cited the December 2011 hacking of Stratfor and theft of confidential information of about 860,000 individuals. It also referenced the January 2012 hacking of international law enforcement email and subsequent accessing of a conference call between Ireland's national police, the FBI, and other law enforcement agencies. At least one defendant has since been sentenced to prison.[71]
- In December 2013, 13 individuals pleaded guilty in federal court to charges related to their role in Anonymous's DDoS attack on PayPal. After WikiLeaks released the trove of State Department cables in November 2010, PayPal suspended WikiLeaks' account such that it could no longer receive donations via PayPal. This spurred "Operation Avenge Assange," where Anonymous coordinated DDoS attacks against PayPal's (and other companies') servers.[72]

[67] Paul Rosenzweig, *Lessons of WikiLeaks: The U.S. Needs a Counterinsurgency Strategy for Cyberspace*, The Heritage Foundation, Backgrounder #2560, May 31, 2011, http://www.heritage.org/research/reports/2011/05/lessons-of-wikileaks-the-us-needs-a-counterinsurgency-strategy-for-cyberspace.

[68] Ibid.

[69] Federal Bureau of Investigation, "Iowa Man Sentenced in Federal Court for Cyber Attack on Koch Industries Subsidiary ," press release, February 13, 2014.

[70] These groups include Internet Feds, LulzSec, and AntiSec. Federal Bureau of Investigation, "Six Hackers in the United States and Abroad Charged for Crimes Affecting Over One Million Victims," press release, March 6, 2012.

[71] Federal Bureau of Investigation, "Jeremy Hammond Sentenced to 10 Years in Prison for Hacking into the Stratfor Website and Other Company, Federal, State, and Local Government Websites ," press release, November 15, 2013.

[72] U.S. Department of Justice, Federal Bureau of Investigation, "Thirteen Defendants Plead Guilty for December 2010 Cyber-Attack Against PayPal," press release, December 6, 2013.

Government Definitions and Agency Focus

The U.S. government does not appear to have an official definition of cybercrime that distinguishes it from crimes committed in what many consider the real world. Similarly, there is not a definition of cybercrime that distinguishes it from other forms of cyber threats, and the term is often used interchangeably with other Internet or technology-based malicious acts such as cyber warfare, cyber attack, and cyber terrorism.[73] Rather, government officials, law enforcement, and policy makers have often described cybercrime in terms of a number of computer, Internet, or advanced technology-related offenses. It has been an umbrella term, encompassing a range of crimes and malicious activities that may differ depending upon who is asked.

Federal law enforcement agencies often define cybercrime based on their jurisdiction and the crimes they are charged with investigating. And, just as there is no overarching definition for cybercrime, there is no single agency that has been designated as the lead investigative agency for combating "cybercrime." For instance, a range of federal law enforcement agencies, including the Federal Bureau of Investigation (FBI), U.S. Secret Service (Secret Service, USSS), and others, investigate crimes that have high-tech elements or that may be considered cybercrimes.

- The FBI is the primary investigative agency within DOJ charged with combating a variety of crimes that may be considered under the broader category of cybercrime. The FBI works cases ranging from computer hacking and online intellectual property rights violations to child exploitation via the Internet and a range of online frauds such as advance fee fraud (AFF), identity theft, and healthcare scams—all elements of what the FBI considers cybercrime.[74] The FBI has a Cyber Division that is involved in investigating these crimes as well as other cyber threats. However, because of the multi-faceted nature of many of these crimes, other divisions are likely involved in their investigation as well.
- The Internet Crime Complaint Center (IC3)—a partnership between the FBI and the National White Collar Crime Center (NW3C)[75]—views cybercrime as a term encompassing "online fraud in its many forms including Intellectual Property Rights (IPR) matters, Computer Intrusions (hacking), Economic Espionage (Theft of Trade Secrets), Online Extortion, International Money Laundering, Identity Theft, and a growing list of Internet facilitated crimes."[76]
- Within the Department of Homeland Security (DHS), the Secret Service is one of the primary agencies combating what may be considered cybercrime. The USSS does not, however, have a publicly available definition for what it considers cybercrime. The USSS is charged with protecting the nation's financial infrastructure and payment systems to safeguard the economy. As such, it has established a Cyber Intelligence Unit, 45 Financial Crimes Task Forces, and 33

[73] McAfee provides examples of cybercrime, hacktivism, cyber war, and cyber terrorism at http://blogs.mcafee.com/wp-content/uploads/2010/10/CybercrimeAndHactivismFocus2010.pdf.

[74] For more information on the full range of the FBI's cyber investigations, see http://www.fbi.gov/about-us/investigate/cyber.

[75] The NW3C is supported by a grant from the Bureau of Justice Assistance. For more information on the Center, see http://www.nw3c.org/.

[76] Internet Crime Complaint Center, http://www.ic3.gov/about/default.aspx.

Electronic Crime Task Forces that investigate a range of crimes, including those with a cyber component.[77]

- The Council of Europe Convention on Cybercrime,[78] to which the United States is a signatory, defines cybercrime as a range of malicious activities that fall into four broad categories of computer-related crimes: (1) security breaches such as hacking, illegal data interception, and system interferences that compromise network integrity and availability; (2) fraud and forgery; (3) child pornography; and (4) copyright infringements. While the United States has signed the Convention, it has not necessarily adopted the exact definition of cybercrime as laid out in the Convention.

In prosecuting cases with a cyber component, DOJ does not explicitly define cybercrime or comprehensively list all offenses that may be considered cybercrimes. Data on cybercrime prosecutions tend to reflect cases prosecuted under the computer fraud statute,[79] 18 U.S.C. Section 1030, as well as those statutes related to stored wire and electronic communications, 18 U.S.C. Section 2101-2711.[80] DOJ does indicate, however, that other cybercrimes are prosecuted under federal fraud, identity theft, illegal intercept of electronic communications, access device fraud, illegal access to stored communications, copyright infringement, and counterfeit products/trademark infringement statutes.[81]

Is a Definition Needed?

Some may question whether it is necessary to have a clear definition of what constitutes cybercrime and what delineates it from other real world and cyber threats. And the answer may depend on the purpose of defining it.

On one hand, if the purpose of defining cybercrime is for investigating and prosecuting any of the various crimes under the broader cybercrime umbrella, it may be less critical to create a definition of the umbrella term and more imperative to clearly define which specific activities constitute crimes—regardless of whether they are considered real world crimes or cybercrimes. For instance, identity theft (18 U.S.C. §1028(a)(7)) is a crime whether it is committed solely in the real world or carried out via cyber means. The statute does not distinguish between the means by which the crime is carried out.

On the other hand, a distinction between cybercrime and other malicious activities may be beneficial for creating specific policies on combating the ever-expanding range of cyber threats. Indeed, some have argued that the prevention and remediation of cybercrime hinge on

[77] U.S. Secret Service, *U.S. Secret Service Annual Report 2013*.

[78] A copy of the Convention is available at http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.

[79] The federal computer fraud and abuse statute protects computers in which there is a federal interest—federal computers, bank computers, and computers used in or affecting interstate and foreign commerce. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud. For more information, see CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle.

[80] U.S. Department of Justice, *United States Attorneys' Annual Statistical Report, Fiscal Year 2010*, pp. 26-27, http://www.justice.gov/usao/reading_room/reports/asr2010/10statrpt.pdf. The more recent reports do not contain specific information on cybercrime.

[81] Ibid, p. 27.

definitional clarity.[82] If government agencies and private sector businesses design strategies and missions around combating "cybercrime," it may be useful to communicate a clear definition of cybercrime to those individuals who may be involved in carrying out the strategies. For instance, if Congress receives an appropriations request for agency funds to combat cybercrime, policy makers may find it beneficial to understand what is meant by the term *cybercrime* as well as what activities would be implemented to combat the threat before deciding whether or not, as well as the extent to which, appropriations may be warranted. Similarly, if Congress chooses to conduct oversight on agencies' efforts to combat cybercrime, a consensus definition of cybercrime and its distinction from various cyber threats may aid in making a sound evaluation of cybercrime policies and strategies.

If, for policy implications, Congress is interested in evaluating the extent or impact of cybercrime—or the countermeasures aimed at thwarting cyber criminals—a definition may be necessary. More information on the issues surrounding "Measuring and Tracking Cybercrime" is provided later in this report.

Strategies and Cybercrime

The United States does not have a national strategy exclusively focused on combating cybercrime. Rather, there are other, broader strategies that have cybercrime components. Policy makers may question whether there should be a distinct strategy for combating cybercrime or whether efforts to control these crimes are best addressed through more wide-ranging strategies, such as those targeting cybersecurity or transnational organized crime. Congress may also question whether these broader strategies provide specific cybercrime-related objectives and clear means to achieve these goals.

The framework within which cybercrime is conceptualized may provide a backdrop for evaluating what type of strategy—existing or otherwise—may be best leveraged to counter the modern day cybercrime threats. For instance, if cybercrime is thought of more as a national security threat than a public security threat, a strategy focused on countering national security threats (including cyber threats) may be more appropriate than a public security-focused strategy for confronting cybercrime, and vice versa. However, categorically clumping the collection of cybercrime activities under the umbrella of "national security threat," "economic security threat," "public security threat," etc. may prove challenging because of the range of crimes and variety of malicious actors. As such, another means of examining what form of strategy to employ regarding cybercrime may be to take an "all threats" approach specific to the cyber domain. This type of strategy would focus on the cyber space (as opposed to the physical space) through which the criminal activity takes place, regardless of the security level of the threat.

Some have suggested that the starting point for any strategy addressing cybercrime should focus on actor attribution and that "greater attribution and clearer rules for responding to both non-attributed and attributed attacks would enable the development and implementation of better strategies and tactics for responding to cyber threats."[83] Existing methods for responding to

[82] Sarah Gordon and Richard Ford, "On the definition and classification of cybercrime," *Journal of Computer Virology*, vol. 2 (July 2006), p. 13.

[83] Scott Charney, *Rethinking the Cyber Threat: A Framework and Path Forward*, Trustworthy Computing Group, Microsoft Corporation, 2009, p. 12.

attacks in the physical world differ based on the identity and motivation of the actor. For example, legal frameworks direct that law enforcement responds to criminal actors, the intelligence community engages in counterintelligence, and the military addresses threats posed by nation-states.[84] In the cyber world, however, these different actors may use similar techniques. As such, attributing a given incident to a particular individual or entity—and responding within the appropriate legal framework—may be challenging.

The **Appendix** presents a selection of current U.S. strategies and international conventions in which the United States participates. Policy makers may evaluate the effectiveness of these existing tools in enhancing actor attribution and countering the spectrum of evolving cybercrime threats. While any one given strategy may be insufficient to address the array of cybercrime threats, the interplay between several strategies may provide a framework for effective crime fighting in the digital domain. Congressional oversight may highlight any gaps in strategies and may be able to evaluate whether the strategies are designed (and carried out) to work with one another.

Measuring and Tracking Cybercrime

According to one expert, "the threat of cybercrime is largely being ignored, and that [threat] is greater than most people believe."[85] Indeed, malicious actors exploiting cyberspace have been identified by the intelligence community as a top threat.[86] However, comprehensive data on cybercrime incidents and their impact are not available, and without exact numbers on the current scope and prevalence of cybercrime, it is difficult to evaluate the magnitude of the threats posed by cyber criminals.

There are a number of issues that have prevented the accurate measurement and tracking of cybercrime. Firstly, the lack of a clear definition of what constitutes cybercrime presents a barrier to tracking comprehensive cybercrime data. This is compounded by the facts that (1) the range of cybercrimes is ever expanding in the globalized world and (2) cyber crimes often overlap with more traditional, non-cyber crimes—thus providing challenges in gauging the true scope of cybercrime. Various agencies and researchers have put forth estimates of the prevalence and costs of cybercrime. However, these often measure a different range of criminal activities and base estimates on differing victim populations.

- The Ponemon Institute, through its *2014 Cost of Cyber Crime Study: United States*, estimates that the median cost of cybercrime to select organizations is $9.7 million annually.[87] Further, the study's findings suggest that this median cost increased from nearly $9.1 million in 2013. The median cost is based on a self-report survey of 59 U.S.-based organizations across various industry sectors. In its report, the Ponemon Institute did not provide a definition of cybercrime as

[84] Ibid., p. 6-7.

[85] "Attackers Have Advantage in Cyberspace, Says Cybersecurity Expert," *Homeland Security Newswire*, August 12, 2011.

[86] Office of the Director of National Intelligence, *Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community* for the Senate Select Committee on Intelligence, January 29, 2014, p. 1.

[87] Ponemon Institute, *2014 Cost of Cyber Crime Study: United States*, October 2014, p. 5. Annual losses ranged from $1.6 million to $61 million per organization. The Ponemon Institute is a research and strategic consulting group.

used in the survey or report of the findings. Further, no information was provided on whether survey documents provided to the study participants included a definition of "cybercrime" that was to be used throughout the survey.

- Results from the 2014 Global Economic Crime Survey—polling 5,128 respondents across 99 countries—indicate that 7% of U.S. organizations lost at least $1 million to cybercrime in 2014.[88] Further, 19% of U.S. organizations reportedly lost $50,000-$1 million from cybercrime. Similar to other studies measuring cybercrime-related losses, this survey does not appear to use a specific, measurable definition of cybercrime.
- McAfee and the Center for Strategic and International Studies have also estimated the losses from cybercrime. In their report, *Net Losses: Estimating the Global Cost of Cybercrime*, they recognize that defining cybercrime is challenging, and any definition will ultimately impact loss estimates. They also note that data on cybercrime are lacking and this "means that any dollar amount for the global cost of cybercrime is an estimate based on incomplete data."[89] Nonetheless, they estimate that cybercrime accounts for about 0.8% of global GDP and about 0.64% of the United States' GDP.[90]

Some surveys of cybercrime measure a specific aspect of what may be considered cybercrime, such as phishing attempts or data breaches. Indeed, the prevalence of data breaches is an often-cited statistic, related to an unknown—and by no means comprehensive—range of cybercrimes. The number of data breaches, as well as the number of records affected by these breaches, has fluctuated over the past several years.

- The Identity Theft Resource Center (ITRC) tracks data breaches across the nation, and their statistics indicate that the total number of reported data breaches increased in 2014 (n = 783) after generally fluctuating over the previous five years. This is the largest number of data breaches since the ITRC began amassing these data in 2005.[91]
- Symantec observed the prevalence of malicious Internet activity—including malicious code, spam, phishing hosts, and bot zombies—across the globe.[92] The United States ranked as the top country where malicious botnets or robot networks originated in 2013, followed by China, Italy, and Taiwan. While this report includes data on a range of malicious Internet activities, it does not provide information as to the prevalence of all forms of cybercrime in specific countries.

[88] PricewaterhouseCoopers, *Global Economic Crime Survey—US Supplement*, 2014, p. 14.

[89] Center for Strategic and International Studies and McAfee, *Net Losses: Estimating the Global Cost of Cybercrime*, June 2014, p. 5.

[90] Ibid.

[91] Identity Theft Resource Center, *Data Breaches*, http://www.idtheftcenter.org/id-theft/data-breaches.html. The IRTC indicates that the criteria for qualifying as a data breach is "an incident in which an individual name plus a Social Security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure. This exposure can occur either electronically or in paper format."

[92] It gathered this information from over 41.5 million attack sensors that monitor "threat activity in over 157 countries and territories through a combination of Symantec products and services.... " Symantec, *Symantec Internet Security Threat Report 2014*, Volume 19, April 2014.

Self-Reporting Cybercrime Victimization

One noteworthy factor impacting availability of data on cybercrime prevalence and its impact is that much of the available data on cybercrime are self-reported. Some have speculated that this self-reporting leads to an underestimation of the true breadth and impact of victimization. This underestimation may be due in part to victims' lack of knowledge that a specific crime has occurred (and its subsequent impact). This underestimation of the scope of cybercrime may also be due to victims' unwillingness to report a crime. For instance, "[m]any financial organisations still prefer to draw a veil over the issue of cybercrime losses because of the technological 'lack' it suggests in their operations."[93] Companies may fear that reporting data breaches could damage their professional reputations and lead to customers/consumers pulling their support and patronage. Individuals may also be unlikely to report such crime if they view their subsequent losses as relatively small and not worth their time and money to report to officials.

Others, however, have suggested that self-report surveys may lead to an overestimation of the prevalence or magnitude of the cybercrime threat. This could be in part because errors in estimated losses—in terms of the amount of data or number of dollars lost to cybercrime—are always positive; there are no negative loss estimation errors because individuals do not report negative losses from cybercrime. Outliers in estimated cybercrime losses may impact survey results and drive up the findings on estimated losses. As such, any average errors in estimated losses may be skewed to have an upward bias.[94]

Another factor that may contribute to unreliable self-reported victimization data is that individuals may be reporting victimization to one or more types of entities—or not at all. For instance, while some victims may file a report with consumer protection entities such as the Internet Crime Complaint Center or the Federal Trade Commission's Consumer Sentinel database, others may file complaints with credit bureaus, while still others may file complaints with law enforcement. Not all victims, however, may file complaints with consumer protection entities, credit reporting agencies, and law enforcement. This uneven reporting can thus distort overall estimates of victimization.

Rather than measuring the cybercrime problem solely in terms of estimated victim losses, researchers have raised the idea of measuring the extent of the cybercrime problem as a ratio of cybercrime consumer losses to cybercrime perpetrator profits. One researcher has noted that

> [t]he harm experienced by users [consumers] rather than the (much smaller) gain achieved by hackers is the true measure of the cybercrime problem. Surveys that perpetuate the myth that cybercrime makes for easy money are harmful because they encourage hopeful, if misinformed, new entrants, who generate more harm for users than profit for themselves.[95]

Moving Forward

Policy makers may debate whether to direct an evaluation of the threats posed by cybercriminals. A comprehensive study could include an appraisal of costs to U.S. persons and businesses alike.

[93] John E Dunn, TechWorld, "Cybercrime Now Major Drag on Financial Services, PwC Finds," *NetworkWorld*, March 27, 2012.

[94] Dinei Florêncio and Cormac Herley, "The Cybercrime Wave That Wasn't," *The New York Times*, April 14, 2012.

[95] Ibid.

Some may argue that any such study should necessarily include well-delineated parameters for what constitutes cybercrime—whether defined by policy makers, a law enforcement community, or cyber scholars.

With a clear assessment of the breadth of the cybercrime threat, policy makers may be positioned to assess whether federal law enforcement has the tools and resources—both funding and manpower—to combat these threats. Congress has often examined cybercrime and related federal resources in the broader context of ensuring cybersecurity. And, policy makers have expressed interest in ensuring the strength and efficacy of the federal cyber workforce. As such, understanding the true nature and scope of the cyber threat may help Congress conduct oversight in these areas and ensure that the relevant resources are appropriately positioned.

Appendix. Existing Strategies and Cybercrime

This appendix presents a selection of current U.S. strategies and international conventions in which the United States participates. While these strategies do not all directly address cybercrime, many address a broad array of cyber threats or criminal threats under which cybercrime may be considered. Of note, the strategies presented below are organized by date of release or U.S. adoption.

Department of Defense Strategy for Operating in Cyberspace

In July 2011 the Office of the Secretary of Defense issued a document called the *Department of Defense Strategy for Operating in Cyberspace*, also known as the Five Strategic Initiatives.[96] This strategy does not specifically target cybercrime threats—though it notes that "[t]he tools and techniques developed by cyber criminals are increasing in sophistication at an incredible rate"[97]—and instead addresses cyber security on the whole. Its first initiative reiterates the Department of Defense's (DOD's) position that cyberspace is an operational domain to organize, train, and equip in order to take full advantage of its potential. The second initiative is to employ new defense operating concepts to protect DOD networks and systems, while the third is to partner with other departments, agencies, and the private sector to enable a whole-of-government cyber security strategy. The fourth initiative focuses on relationship building with U.S. allies and international partners, and the fifth intends to leverage the U.S. cyber workforce and technological innovation.

Although usually directed at military targets, not all intrusions on DOD networks are the result of a combatant. The Defense Cyber Crime Center (DC3) is a forensics, research, and training organization to assist with criminal investigations of network security breaches on DOD networks and cyber intrusions presenting a national security threat.[98] The DC3 is also responsible for the Defense Industrial Base Collective Information Sharing Environment (DCISE), a clearinghouse for threat data between DOD and its industry partners.

Strategy to Combat Transnational Organized Crime

In July 2011, the Obama Administration released the *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security*.[99] The strategy provides the federal government's first broad conceptualization of "transnational organized crime," highlighting it as a national security concern.[100] It highlights 10 primary threat categories posed by transnational organized crime: penetration of state institutions, corruption, and threats to governance; threats to the economy, U.S. competitiveness, and strategic markets; nexus between

[96] U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, http://www.defense.gov/news/d20110714cyber.pdf.

[97] Ibid., p. 3.

[98] For more information on the DC3, see http://www.dc3.mil.

[99] The White House, *Strategy To Combat Transnational Organized Crime: Addressing Converging Threats to National Security*, July 2011, http://www.whitehouse.gov/sites/default/files/microsites/2011-strategy-combat-transnational-organized-crime.pdf. (Hereinafter *Strategy To Combat Transnational Organized Crime*.)

[100] For a discussion of organized crime and this strategy, see CRS Report R41547, *Organized Crime: An Evolving Challenge for U.S. Law Enforcement*, by Jerome P. Bjelopera and Kristin Finklea.

criminals, terrorists, and insurgents; expansion of drug trafficking; human smuggling; trafficking in persons; weapons trafficking; intellectual property theft; the critical role of facilitators;[101] and cybercrime. The strategy outlines six key priority actions to counter the range of threats posed by transnational organized crime:

- taking shared responsibility and identifying what actions the United States can take to protect against the threat and impact of transnational organized crime;
- enhancing intelligence and information sharing;
- protecting the financial system and strategic markets;
- strengthening interdiction, investigations, and prosecutions;
- disrupting drug trafficking and its facilitation of other transnational threats; and
- building international capacity, cooperation, and partnerships.[102]

While this strategy does not focus solely on cybercrime activities of criminal networks, it does include a prominent discussion surrounding organized crime's involvement in cybercrime. The strategy notes that "[v]irtually every transnational criminal organization and its enterprises are connected and enabled by information systems technologies, making cybercrime a substantially more important concern."[103] It also points out a significant impediment to law enforcement successfully investigating cybercriminal activities: "Crimes can occur more quickly, but investigations proceed more slowly due to the critical shortage of investigators with the knowledge and expertise to analyze ever increasing amounts of potential digital evidence."[104]

Further, a number of the threats identified in the strategy—while not specifically identified under the cybercrime umbrella—may overlap with cybercrime or may be directly facilitated by the Internet and other advanced technologies. For instance, the theft of intellectual property is often carried out through illegal computer intrusions and the digital extraction of information and thus could also be considered cybercrime. Indeed, many crimes or malicious activities can fall under various threat categories outlined by the strategy; for instance, many crimes related to financial fraud and identity theft may fall under the categories of cybercrime, intellectual property theft, or threats to the economy, U.S. competitiveness, and strategic markets. As such, this strategy does not provide a detailed outline for how the U.S. should counter each category of threat, and the Administration indicated that this strategy is meant to complement a range of other strategies, including the International Strategy for Cyberspace.[105]

International Strategy for Cyberspace

In May 2011, the Obama Administration issued the *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. This strategy outlines U.S. engagement

[101] "Facilitators" are "semi-legitimate players such as accountants, attorneys, notaries, bankers, and real estate brokers, who cross both the licit and illicit worlds and provide services to legitimate customers, criminals, and terrorists alike." See *Strategy To Combat Transnational Organized Crime*, p. 8.

[102] Ibid., p.4.

[103] Ibid., p. 3.

[104] Ibid., p. 8.

[105] Ibid., p. 4.

with international partners to confront the full array of cyber issues—including cybercrime.[106] According to this strategy, the U.S. government's core principles are fundamental freedoms, privacy, and the free flow of information while protecting the security of national networks. Rather than imposing a global governance structure, the strategy recommends building international norms of behavior and enhancing interoperability.

The strategy outlines five principles that nations should support, one of which is protection from crime. Under this principle, nations are expected to "identify and prosecute cybercriminals, to ensure laws and practices deny criminals safe havens, and cooperate with international criminal investigations in a timely manner."[107] The strategy also provides a core set of seven policy priorities as well as proposed actions to accomplish each of these priorities. Directly relating to the prevention, investigation, and prosecution of cybercrime, one overarching policy priority involves extending law enforcement collaboration and rule of law. To accomplish this, the strategy proposes that the United States will

- fully participate in the development of international cybercrime policy,
- encourage nations' participation in the Council of Europe Convention on Cybercrime,
- direct cybercrime legislation toward combating illegal activities rather than restricting Internet access, and
- prevent Internet exploitation by terrorists and criminals seeking to plan, finance, or carry out malicious activities.[108]

The International Strategy for Cyberspace addresses cybercrime in the broader context of cyber security. Moreover, it primarily discuses how the United States will increase its domestic and multilateral cybercrime fighting capacities.

National Strategy for Trusted Identities in Cyberspace

The Obama Administration released the *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy* in April 2011. In this strategy, the Administration proposed an "Identity Ecosystem" where individuals and organizations adhere to standards to authenticate their online identities and the identities of their digital devices. It was suggested that this ecosystem would provide, among other things, enhanced security such that it would be more difficult for criminals to compromise online transactions.[109] Further, the strategy posits that an environment with secure authentication can support forensics to "maximize recovery efforts, enable enhancements to protect against evolving threats, and permit attribution, when appropriate, to ensure that criminals can be held accountable for their activities."[110] In

[106] The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf.

[107] Ibid., p. 10. The other four principles to which nations should adhere include upholding fundamental freedoms, respecting property, valuing privacy, and retaining the right to self-defense.

[108] Ibid., pp. 19-20.

[109] The White House, *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy*, April 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[110] Ibid., p. 12-13.

encouraging major vendors and companies to take up enhanced standards for verifying user identities and storing personal data online, this strategy provides one step in protecting information online.[111]

Council of Europe Convention on Cybercrime

The Council of Europe's Convention on Cybercrime was developed in 2001 to address several categories of crimes committed via the Internet and other information networks.[112] It is the first—and only[113]—international treaty on this issue, and its primary goal is to "pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation." To date, 47 countries are signatories to the convention and 31 of these—including the United States—have ratified it.[114]

Signatories to the convention must define criminal offenses and sanctions under their domestic laws for four categories of computer-related crimes: (1) security breaches such as hacking, illegal data interception, and system interferences that compromise network integrity and availability; (2) fraud and forgery; (3) child pornography; and (4) copyright infringements. The convention also requires signatories to establish domestic procedures for detecting, investigating, and prosecuting computer crimes, as well as collecting electronic evidence of any criminal offense. It also requires that signatories engage in international cooperation "to the widest extent possible."

There has been a debate about whether there should be a global standard—be it the Convention or a different entity—for dealing with cybercrime.[115] Some have suggested that a global convention could help countries harmonize their legislation on cybercrime. One argument in this case is that similar legislation across countries could enhance international cooperation since a number of countries base mutual legal assistance on the notion of "dual criminality," wherein an action that is illegal in one country is also considered a crime in the other.[116] Others, however, have expressed reservations about supporting a global standard for combating cybercrime. Concerns have centered not only around the feasibility of global coordination, but around whether such legal harmonization could put certain nations in a position of enforcing laws that may depart from the nation's basic tenets;[117] for instance, could laws curbing certain levels of inflammatory "speech" online infringe upon the right to free speech guaranteed in the United States, and if so, how would the United States balance enforcing harmonized global laws with ensuring constitutional rights?

---

[111] Nicole Perlroth, "Even Big Companies Cannot Protect Their Data," *The New York Times*, January 17, 2012.

[112] For more information on the Convention, see archived CRS Report RS21208, *Cybercrime: The Council of Europe Convention*, by Kristin Archick. A copy of the Convention is available at http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.

[113] Duncan B. Hollis, "An e-SOS for Cyberspace," *Harvard International Law Journal*, vol. 52 (2011), pp. 392-393.

[114] The U.S. Senate ratified the Convention on August 3, 2006. For the current list of signatories and ratifications, see http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG.

[115] Brian Harley, "A Global Convention on Cybercrime?," *The Columbia Science and Technology Law Review*, March 23, 2010, http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/.

[116] See, for example, Twelfth United Nations Congress on Crime Prevention and Criminal Justice, *Recent Developments in the Use of Science and Technology by Offenders and by Competent Authorities in Fighting Crime, Including the Case of Cybercrime*, United Nations, Working paper prepared by the Secretariat, January 22, 2010.

[117] Brian Harley, "A Global Convention on Cybercrime?," *The Columbia Science and Technology Law Review*, March 23, 2010, http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/.

Global Internet Freedom

In 2006, the Department of State launched the Global Internet Freedom Task Force (GIFT). The GIFT's main foreign policy objective is enhancing global Internet freedom by monitoring human rights abuses and enhancing access to the Internet through technical and financial support for increasing availability in the developing world. A form of expanding access to the Internet is to create mirror sites that serve as alternatives to websites that are blocked in some countries, or to develop tools and instructions that enable users to work around a country's firewalls. The International Strategy for Cyberspace and Global Internet Freedom initiatives present a very different view of cyberspace from DOD doctrine, which emphasizes full spectrum dominance and cyberspace as an operational, war-fighting domain.

A question exists about the definition of sovereignty in cyberspace. Although no one country "owns" cyberspace, each may have the authority to regulate its portion of the Internet, similar to territorial waters or airspace. What constitutes computer-based crime may be determined by domestic standards, and one country's Internet freedom initiative may be another country's cybercrime.

National Strategy to Secure Cyberspace

Following the terrorist attacks of September 11, 2001, the newly formed Department of Homeland Security (DHS) issued a document that recognized cyberspace as a strategic asset with national security implications and offered suggestions for private network owners and operators to increase protection efforts. The 2003 *National Strategy to Secure Cyberspace* places DHS as the lead for coordinating federal network protection as well as working with the private sector, and also offers a framework for improving international cooperation. The strategy prioritizes five components to securing cyberspace:

- a national cyberspace security response system,
- a national cyberspace security threat and vulnerability reduction program,
- a national cyberspace security awareness and training program,
- securing governments' cyberspace, and
- national security and international cyberspace security cooperation.[118]

Like the *International Strategy for Cyberspace*, the *National Strategy to Secure Cyberspace* addresses cybercrime in the broader context of cyber security. Within this context, it prioritizes improving U.S. response to cyber incidents and reducing any potential damage, reducing threats from and vulnerabilities to cyber attacks—including cybercrime—and preventing cyber attacks.

[118] U.S. Department of Homeland Security, *The National Strategy to Secure Cyberspace*, February 2003, p. x, http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.

Author Contact Information

Kristin Finklea
Specialist in Domestic Security
kfinklea@crs.loc.gov, 7-6259

Catherine A. Theohary
Specialist in National Security Policy and Information Operations
ctheohary@crs.loc.gov, 7-0844