CHAPTER 24

CYBERCRIME

KIM-KWANG RAYMOND CHOO AND PETER GRABOSKY

2014. Oxford University Press.
All rights reserved. May not be reproduced in any form without permission from the publisher, except fair uses permitted under U.S. or applicable copyright law.

I. Introduction

Computers and network-based systems lie at the heart of critical infrastructures around the world, particularly in the technologically advanced countries (National Infrastructure Advisory Council 2004). This is hardly surprising as the proliferation of information and communications technologies (ICT) and connectivity of the Internet in today's digital age open the door to increased productivity, faster communication capabilities, and immeasurable convenience. This creates not only benefits for the community, but also risks of criminal exploitation.

Digital technology has empowered ordinary individuals as never before. A person acting alone can communicate with millions of people, instantly and at negligible cost. Sole individuals are now able to penetrate and disrupt major governmental systems and prominent retailing sites. Organizations too have been greatly empowered by digital technology, for better and for worse.

This essay looks at the exploitation of digital technology in furtherance of organized crime. It first addresses the concept of criminal organization and suggests the desirability of a more expansive construction to accommodate the evolution and diversification of organizational forms in the modern era. It then looks at three types of organized crime groups: (1) traditional organized crime groups, which make use of ICT to enhance their terrestrial criminal activities; (2) organized cybercrime groups, which operate exclusively online; and (3) organized groups of ideologically and politically motivated individuals, who make use of ICT to facilitate their criminal conduct. The essay notes emerging trends in organized cybercrime and concludes with a few suggestions for the prevention and control of organized crime in the digital age.

Although it would be pleasing to be able to cite comprehensive statistics on patterns and trends in organized cybercrime, this remains an elusive goal. Much cybercrime is

EBSCO Publishing: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY 877306; Letizia Paoli; The Oxford Handbook of Organized Crime Account:ehost.

unreported. Some is even undetected. Of those offenses that do come to the attention of authorities, the organizational circumstances of the perpetrator (or perpetrators) is often unknown. Those official statistics that do exist often relate to the substantive offense rather than the technologies by which it was committed. One may say with confidence that the increasing pervasiveness of digital technologies means that they will continue to be exploited for criminal purposes by organizations both terrestrial and virtual.

II. Organizations

A. Morphology

Legitimate organizations look very different today from the way they appeared a century ago (if indeed they existed that long in the past and have survived). What were once vertically integrated organizations have shed functions, preferring to "contract out" specific tasks to specialist service providers rather than deliver everything using in-house resources. In recent years, the term *virtual organization* has been coined to refer to networked entities, in general, or to those organizations that outsource a significant amount of activity (Tapscott and Williams 2006).

When scholars and law enforcement officials think of organized crime, they instinctively think about stereotypical organizations committing certain types of crime. The classic monolithic, pyramidal organization, such as the Yakuza, triads, or the Italian mafia, engaged in extortion or in the delivery of illicit services come immediately to mind. While a few criminal organizations still fit the classic monolithic, hierarchical, formal model, analysts began well over a decade ago to observe emerging variations (Halstead 1998). Much organized criminal activity began to be recognized as the collective work of loose coalitions of groups, collaborating with each other from time to time to achieve certain objectives. A case discussed below illustrates the franchise-like operations of an organized crime family in the United States, where peripheral associates manage teams of ordinary criminals and pass a percentage of their "take" to formal ("made") family members. Indeed, today the term *network* has become more familiar than *family* to describe organized crime (Williams 2001). Such networks are involved in activities as "traditional" as extortion and drug trafficking and as contemporary as software piracy, credit card fraud, and online child exploitation (Choo, Smith, and McCusker 2007; Choo 2009).

There remain aspects of organizational life in cyberspace that resemble the terrestrial world. In some cases, small groups of youth engage in online activity much as they would on the street; "hanging out" and showing off to each other. While much adolescent behavior in either setting is an innocent manifestation of youthful exuberance, some is not so innocent. Youth congregate in cyberspace, as they do on the street, for

EBSCOhost: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY. All use subject to https://www.ebsco.com/terms-of-use.

illicit fun and for illegal profit. Their organizational structure resembles more that of kids "messing around" in physical space than that of an organized crime group.

Other aspects are different. Organizations in cyberspace may involve repeated and intense interactions among people who have never met each other in person. Moreover, they may be situated almost anywhere on the surface of the earth. Drug newsgroups attract people interested in the manufacture of synthetic illicit drugs (Schneider 2003). To the extent that these relationships become institutionalized, new organizational forms are created. Contact made in IRC chatrooms between people who have never met each other (and may never meet each other) in physical space can evolve into hacker groups, piracy or "warez" groups, or child pornography rings (Holt 2007).

B. Longevity

The lifecycle of organizations has also become more varied. Some organizations are stable and enduring, such as the Vatican or Oxford University. Others transform themselves, adapting to dramatically changing circumstances. The Singapore Police Force of today is substantially different from the Singapore Police Force of 1819. Some organizations have come into existence only recently to exploit a new opportunity. Google, Inc. was first incorporated as recently as 1998. Other organizations are short-lived, coming into existence for a particular purpose and then disbanding. Consider the Beijing Organizing Committee for the Olympic Games (BOCOG) that was established to oversee the 2008 Olympic Games in Beijing. It exists no longer. Some organizations are extremely short-lived. One of the more recent manifestations of the evanescent organization is swarming, i.e., "the unexpected gathering of large numbers of people in particular public locales" (White 2006). The communications processes that underlie such gatherings need not involve high technology; rather, word of mouth can suffice. But one can easily appreciate how swarming can be facilitated by the Internet or by digital telephony. In Australia, recent years have seen the use of text messages to make plans for group sexual assaults and race riots (Morton 2004; Perry 2005). Iranian dissidents used social networking technologies to organize protests against President Mahmoud Ahmadinejad in 2009 (LaFraniere and Ansfield 2010).

More recently, social media played a significant role in organizing the uprisings in Egypt and Tunisia that led to the overthrow of their authoritarian regimes. Social networking sites such as Facebook enabled strategic communications regarding the timing and location of protest activity. Media such as YouTube were used to transmit a picture of brutal police repression, locally and throughout the world, in avoiding state censorship (Preston 2011). Social media were also used in coordinating the riots that took place across the United Kingdom in August 2011. The BlackBerry messaging service was used to encourage looting and to arrange the time and location of gatherings. This prompted the British government to explore the development and imposition of controls over the technology (Pfanner 2011).

EBSCOhost: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY. All use subject to https://www.ebsco.com/terms-of-use.

III. Organized Crime Groups

The definition of "organized criminal group" from Article 2 of the UN Convention on Transnational Organized Crime is adopted in this essay:

> a group having at least three members, taking some action in concert (i.e. together or in some co-ordinated manner) for the purpose of committing a 'serious crime' and for the purpose of obtaining a financial or other benefit. The group must have some internal organization or structure, and exist for some period of time before or after the actual commission of the offence(s) involved.

Whether the changes in organizational life noted above will result in more ephemeral collectivities to be deemed criminal organizations remains to be seen. It has even been suggested that a single individual who succeeds in building a network of compromised computers (a robot network or "botnet")[1] is creating a new form of criminal organization (Chang 2012).

A. Traditional Organized Criminal Groups

Organized crime is not a new phenomenon. It preceded, and then accompanied, the rise of the modern state. Pursuit of financial gain has always been the driving force behind traditional organized crime, although the desire for power, respect, comradeship, and adventure also figure prominently in the motivational mix.

However, the nature of organizational life is changing for criminal organizations no less than for legitimate ones. Monolithic, hierarchical, formal organizations still exist, but organizational form is becoming increasingly diverse. So too are the activities in which criminal organizations engage. To a significant extent, these trends are the products of rapid developments in information and communications technology (ICT), as traditional organized criminal groups have recognized the value of leveraging ICT to facilitate or enhance the commission of crimes. Examples include: using ICT to facilitate drug trafficking; to traffic in corporate secrets and identity information; to commit extortion, frauds, and scams online; to launder money using online payment systems; and to distribute illegal materials over the Internet. Of course, criminal organizations, like their legitimate counterparts, also use digital technology for routine incidental purposes, such as record keeping and communication.

Examples of traditional organized criminal groups involved in cybercrime include the highly structured and global criminal syndicates such as the Asian triads and Japanese Yakuza, whose criminal activities have been known to include computer software piracy and credit card forgery and fraud (Organisation for Economic Co-operation and Development 2007). Commentators have also suggested that traditional organized crime groups (e.g., outlaw motorcycle gangs) use online resources, such as social networking sites, to perform background checks on

EBSCOhost: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY. All use subject to https://www.ebsco.com/terms-of-use.

potential and new members (Douglis 2010) and to promote themselves to impressionable young people.

Traditional organized criminal groups from eastern Europe have also been known to carry out extortion from online gambling and pornography websites by threatening to carry out denial-of-service attacks using botnets (Choo 2007). In recent years, organized criminal groups have been reported to recruit "a new generation of high-flying cybercriminals using tactics which echo those employed by the KGB to recruit operatives at the height of the cold war" (McAfee 2006, p. 2). This should come as no surprise to long-time political observers. In countries such as Russia, the lack of economic and employment opportunities have forced many highly educated individuals with advanced computer and programming skills to work in the cyber underground.

In its 2008 threat assessment, the Serious Organised Crime Agency in the United Kingdom warned that traditional organized criminal groups are also "increasingly using false and stolen identities to commit non-fiscal frauds" (Serious Organised Crime Agency 2008, p. 9). For example in May 2009, 11 defendants, alleged to be members of a "crew" working in Florida for an associate of the New York–based Bonnano crime family, were charged with various offenses, including the illegal manufacture of fraudulent checks and fraud in connection with access devices. The group included one individual with a background in computing who accessed databases with a view toward identifying potential extortion victims. He also used his computing skills in the production of counterfeit checks.[2] In Japan, conventional criminal groups also provide venture capital for technicians specializing in hacking and fraud (Tokyo Reporter 2009). Another case involved a large and diverse conspiracy among members of the Gambino crime family alleged to have engaged in fabrication of false bar code labels and credit cards. One member of the conspiracy, who worked for a chain of home improvement stores, had access to the requisite technology (US Department of Justice 2010). A third example involved other associates of the Bonnano family who were active in the telecommunications industry and who were implicated in a scheme of fraudulent billing of telephone accounts.[3]

In October 2011, 111 individuals from five different criminal groups were indicted by local authorities in New York City for a range of offenses related to identity theft, credit card forgery, and fraud. A number of the accused were also allegedly involved in a range of terrestrial offenses, including burglary and robbery. It was alleged that the groups obtained credit card details from skimming (for example, by complicit restaurant employees) or from Internet suppliers through illegal websites. Counterfeit credit cards were then manufactured, and teams of shoppers deployed to purchase high-end merchandise, some of which was sold online by fences (Queens County District Attorney 2011).

Traditional organized crime groups (and organized cybercrime groups described in the next section) have also been known to hire money mules in the money laundering process. Money mules are individuals hired by organized criminals to perform international wire fraud or to purchase prepaid cards, and then to mail or ship prepaid cards out of the country without regulators being aware (Choo 2008, footnote 14). As Choo,

EBSCOhost: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY. All use subject to https://www.ebsco.com/terms-of-use.

Kim-Kwang Raymond, Russell G Smith, and Rob McCusker (2009, p. xxi) point out, "[o]rganised operations that make use of conventional technology-enabled crime methodologies, such as financial scams or piracy, will also increase as the use of networked computers for criminal purposes develops."

In rare cases, criminal organizations may engage the services of former law enforcement officers with a degree of technological expertise. One former FBI agent accessed the bureau's database and alerted two suspects that they were targets of an investigation (US Department of Justice 2005).

B. Organized Cybercriminal Groups

Another category of organized criminal group consists of like-minded individuals who usually know each other only online, but who are involved in an organizational structure working collectively toward a common goal because the Internet makes it far easier to meet and plan activities. Although the objective is usually pursuit of financial gain, it can include other criminal goals such as producing and disseminating child pornography and related materials. For example, in 2007 more than 700 suspects associated with the UK-based Internet chatroom, "Kids, the Light of Our Lives," were arrested worldwide (Child Exploitation and Online Protection 2007).

Another example relates to software piracy. "Drink or Die" was a group of information technology specialists who obtained copies of software and other digital products, stripped them of their copyright protection, and posted them to hundreds of Internet sites around the world. Prior to their collaboration in furtherance of piracy, none had significant criminal backgrounds. Members were located in a number of countries, including the United States, the United Kingdom, and Australia; most of their interactions occurred in cyberspace rather than on the ground. In December 2001, the simultaneous execution of 58 search warrants brought an end to the conspiracy. One of the members, an Australian, had never set foot in the United States, although he was eventually extradited, convicted, and imprisoned there (Urbas 2006).

C. Ideologically and Politically Motivated Cybercrime Groups

Prior to September 11, 2001, terrorism and organized crime were usually considered separate entities because they did not share the same motivating factor. The primary objective of organized crime is money. By contrast, terrorist organizations have political goals. In recent years, however, a convergence between terrorism and organized crime has been noted. The variety of ways in which digital technology may be used in furtherance of terrorism include communications, intelligence, propaganda and psychological warfare, recruitment, and training (Thomas 2003). Conventional criminal organizations have a great deal of expertise to offer terrorist groups. Crimes commonly associated with organized criminal groups (e.g., scam and fraud schemes, identity and

EBSCOhost: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY. All use subject to https://www.ebsco.com/terms-of-use.

immigration crimes, and the counterfeit of goods) are also precursor crimes used by terrorist groups to raise funds (Sanderson 2004).

Some terrorists engage in cybercrime to acquire resources with which to finance their operations, especially since formal funds transfers have come under increasing scrutiny from anti–money laundering authorities. Imam Samudra, convicted architect of the 2002 Bali bombings, reportedly called upon his followers to commit credit card fraud (Sipress 2004). The Tamil Tigers are alleged to have engaged in credit card fraud to support their operations (Hutchinson and O' Malley 2007).

Others seek to harass or threaten an adversary. Originally, this took the form of "mail bombing" in which thousands of emails were directed at a target in an effort to degrade the system. In May 1999, the White House website was overloaded with "visits" following the bombing of the Chinese embassy in Belgrade (National Infrastructure Protection Center 2001). Today, botnets are used for such a purpose, as was the case in the 2007 denial of service attacks against Estonian servers (Landler and Markoff 2007).

A 2006 report (IDSS 2006) highlighted the proliferation of jihad-oriented sites in Southeast Asia, which facilitate radicalization among the Muslim community in the region. Eight thousand websites espousing radical ideologies, such as hosting hate and terrorism contents, are reportedly identified in a more recent report by the Wiesenthal Center's Digital Terror and Hate 2.0 (Simon Wiesenthal Center 2008). Such sites target the digital generation—the young and the Internet-aware—particularly within the Muslim community. The latter, with a shallow understanding of Islam, may be vulnerable to the seductive propaganda posted on such sites and forums.

In 2007, Singapore's Internal Security Department investigated Internet-driven radicalization cases involving Singaporeans attracted to terrorist and radical ideas on the Internet (Kor 2007). More recently, in April 2010, a full-time national serviceman in the army was arrested in Singapore under that nation's Internal Security Act. According to the media release from the Ministry of Home Affairs, it was alleged that the accused began searching for jihadist propaganda online while he was a student in one of Singapore's local educational institutions. Over time, the accused became deeply radicalized by the materials he found online and convinced that it was his religious duty to undertake terrorist activities. The accused allegedly went online in search of information on bomb-making, and he produced and posted a video glorifying suicide bombing before being arrested (Ministry of Home Affairs, Singapore 2010). This case and others around the world illustrate some of the ways in which terrorists can exploit the Internet and new media channels (e.g., social networking sites) for criminal purposes.

D. State-Organized Cybercrime

When a government or large commercial network comes under cyber attack, it is not immediately apparent whether the source of the attack is a skillful teenager, an organized crime group, or a nation-state. In fact, it may involve two or more of these. Governments do not always use civil servants to perform their "dirty work." They may turn a blind eye

EBSCOhost: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY. All use subject to https://www.ebsco.com/terms-of-use.

to illegality that is seen as serving state interests. They may offer tacit, or even active, encouragement to cyber criminals.

A number of prominent attacks, the origins of which remain obscure, have occurred in recent years. The cyber attacks against government servers in Estonia in April 2007 apparently sought to intimidate the Estonian government and its people for having relocated a Soviet-era memorial to fallen Russian soldiers. It has been suggested that criminal organizations played a significant role in the attacks; the degree to which the Russian government was complicit remains unclear (Landler and Markoff 2007).

In March 2009, it was revealed that a number of computer systems serving the Dalai Lama's Tibetan exile centers around the world had been penetrated by a sophisticated surveillance system. The scale of the surveillance activity, which was traced to three sites in China as well as to a webhosting service in Southern California, seemed to indicate government activity. It was suggested the work may have involved patriotic hackers who were associated with, but independent of, the state.[4] The Chinese government dismissed the suggestion that it was involved in the surveillance (Markoff 2009; Munk Centre 2009). Cybercriminals can make use of various technologies, including launching a cyber attack from proxy servers in third countries to conceal their identity. Definitive attribution of the source(s) of any cyber attack is no easy task and can be very time consuming. It largely depends on the technical expertise of perpetrators and several other factors, including the jurisdiction from which they operate. State-sponsored cyber attacks are no longer fiction, but the question remains: "How does one determine whether an attack is criminal or an act of cyber war?"

In January 2010, Google announced that it had become the target of a sophisticated and coordinated attack, apparently originating in China, that resulted in the accessing of Gmail accounts, including those of Chinese human rights activists. The Chinese government denied responsibility. More broadly, the US government, assisted by the telecommunications industry, engaged in widespread illegal interception of telecommunications traffic during the George W. Bush administration (Bamford 2008).

In 2010, it became apparent that a worm malware referred to as "Stuxnet" had disrupted centrifuges essential to uranium enrichment processes in Iran. Analysis of Stuxnet suggested that the malware was designed to reprogram the ICS "by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment" and the malware consisted of "[several] zero-day exploits, a Windows rootkit, the first ever PLC rootkit, antivirus evasion techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates, and a command and control interface" (Falliere, Murchu, and Chien 2010, pp. 1–2). The degree of sophistication of the code, the knowledge of Siemens control systems necessary for its development, the need for testing and refinement of the worm, and the challenge of its ultimate insertion in relevant Iranian computer systems suggest that it was the work of state actors, subsequently reported to be the United States and Israel (Markoff 2010, 2011; Sanger 2012).

In 2011, South Korean authorities accused China-based North Korean hackers of infiltrating online gaming sites. After establishing robot accounts and using automated

EBSCOhost: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY. All use subject to https://www.ebsco.com/terms-of-use.

software, the players allegedly accumulated gaming points and exchanged them for cash. A percentage of the proceeds was reportedly retained by the players and the remainder transferred to North Korea (Choe 2011).

Cybercrime, in general, and organized cybercrime, in particular, are following two basic trends: sophistication and commercialization.

E. Sophistication

Technology does not stand still, and those who seek to make best use of it, for purposes legitimate or otherwise, must keep abreast of the latest developments. The trajectory is a long one from using commercial off-the-shelf (COTS) technology to scan and duplicate $50 notes to the industrial-sized operations for the manufacture of pirated DVDs.

Viruses and worms once took days to spread around the globe. They now take minutes to do so. Malicious code can be designed to look for openings and, once it invades a target computer, to cover its own tracks (Thompson 2004; Markoff and Vance 2010); it can also be designed to allow remote control of a computer, enabling the intruder to activate audio and video recording features and to capture the information contained therein (Markoff 2009). The scope and complexity of the attack against the Dali Lama's systems appears to be without precedent, as does the domestic electronic surveillance practiced by the US government. The "Stuxnet" worm that infected Iranian nuclear facilities in 2010 was precisely calibrated and apparently the work of a skilled team of programmers (Broad and Sanger 2010). On a more modest level, participants in an international stock fraud conspiracy (discussed below) used special software to conceal the origin of their Spam emails and to circumvent their recipients' Spam filters. (US Department of Justice 2009*a*).

F. Commercialization

At the dawn of the digital age, much computer crime took place for fun rather than for profit. The distribution of illicit images of children occurred in the context of a barter economy. Other computer criminals were motivated by the intellectual challenge, by adventure, or by rebellious spirit rather than by mercenary considerations. Practitioners of digital piracy gave products away rather than selling them. Virus writers regarded their activity as an art form rather than as a way to make a living. Today, the services of accomplished hackers are available for hire; a criminal group can rent robot networks for use in spamming, denial of service attacks, or extortion, and digital piracy has become big business. Additional categories of financially motivated cybercrimes include:

> **Computer or network intrusions such as hacking and unauthorized access to obtain sensitive information**. For example, in 1994, A Russian named Vladimir Levin obtained access to the servers of Citibank in the United States. He was able

EBSCOhost: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY. All use subject to https://www.ebsco.com/terms-of-use.

to impersonate legitimate Citibank account holders and began to transfer funds from their accounts to new accounts opened by his accomplices around the world. The fraud was detected, and the accomplices were arrested when they attempted to withdraw the money (Smith, Grabosky, and Urbas 2004, p. 51).

In August 2008, 11 individuals (including three US citizens, one from Estonia, three from Ukraine, two from the People's Republic of China, one from Belarus, and one with unknown place of origin) were charged with numerous crimes, including conspiracy, computer intrusion, fraud, and identity theft. It was alleged that the group members were involved in the hacking of nine major US retailers and the theft and sale of more than 40 million credit and debit card numbers. These numbers were used to withdraw tens of thousands of dollars from ATMs (US Department of Justice 2008).

Phishing: Internet scams frequently use unsolicited messages purporting to originate from a legitimate source to deceive individuals or organizations into disclosing their financial and/or personal identity information. This information can then be used to commit or facilitate crimes such as fraud, identity theft, and stealing of sensitive information (e.g., banking credentials or trade secrets). Several researchers and security practitioners have also noted the involvement of organized crime groups in phishing scams. A large conspiracy involving 38 individuals in Romania and the United States obtained credit card details through phishing. They then used these details in the counterfeiting of credit cards (US Federal Bureau of Investigation 2008*a*, 2008*b*).

Spam is unsolicited commercial email intended to persuade recipients to buy products, legitimate or otherwise. Spam may also be used to spread false rumors about stocks traded on stock exchanges around the world. In November 2009, four men were sentenced in the United States for their participation in an international stock fraud scheme. They purchased thinly traded shares and then used mass emails to spread false rumors about the shares likely increase in price. When the price of the shares increased, the conspirators sold their holdings for a profit (US Department of Justice 2009*a*).

Malware creation and dissemination: Malware, also known as malicious software, is designed to install itself on a computer without the computer owner's informed consent, particularly if it does so in a way that may compromise the security of the computer. Malware includes Trojans, viruses, and worms. The 2008 UK Threat Assessment report noted that "most new malware is designed to steal financial data (such as credit card details, bank account details, passwords, PIN numbers) as a precursor to various frauds and other deceptions" (SOCA 2008, p. 9). In 2009, Albert Gonzalez, a resident of Miami, Florida, pleaded guilty to controlling a number of servers and granting access to other hackers with the knowledge that they would use their access to store malware and then attack corporate victims. Their ultimate objective appears to have been theft of credit card details. Gonzalez used multiple antivirus programs to test the quality of his malware (US Department of Justice 2009*b*).

EBSCOhost: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY. All use subject to https://www.ebsco.com/terms-of-use.

Internet frauds and scams are limited only by the imagination of prospective criminals. Offenses of this type include Nigerian advance fee frauds (also known as 419 scams), online auction frauds, and identity and credit card frauds. Fraudulent investment solicitations are greatly facilitated by digital technology. In 2004, four men pleaded guilty to fraud concerning an Internet-based Ponzi scheme involving 15,000 investors and USD$60 million in investments (US Department of Justice 2004).

G. Countries Involved in Contemporary Cybercrime

Organized cybercrime is a global phenomenon. Those countries that strictly regulate online access (such as Burma) host fewer offenders and have fewer victims. Countries with many persons skilled in information technology, but which offer fewer opportunities for legitimate enrichment (such as Russia), have many offenders. Affluent nations with high individual and corporate connectivity, and with a vibrant e-commerce sector (such as the United States, the United Kingdom, and the countries of continental western Europe), will have more victims. The world's two most populous nations, China and India, are experiencing increasing affluence and digital connectivity; their prominence in cybercrime is likely to increase commensurately.

IV. Responding to Organized Cybercriminal Activities

As the Internet and other forms of information and communications technologies continue to advance, the opportunities for cybercriminal activities will increase. At the same time, the resources and skills of most law enforcement agencies will remain limited. This gap will require an adroit combination of warnings, reassurance, and strategic targeting of the most serious cyber threats. Sovereign states have their own priorities. Authorities in the United States are particularly attentive to online child pornography, theft of (US-owned) intellectual property, and attempts to compromise US government and commercial systems. By contrast, law enforcement in the People's Republic of China is more concerned about comments critical of government policy, including statements advocating Tibetan and Taiwanese independence.

We have noted that cybercrime can be committed by individuals or groups alike as easily from across the globe as from across town. And some organizations themselves transcend national borders. As is the case with terrestrial transnational organized crime, the effective control of transnational cybercrime requires a degree of cooperation between countries. The foundation for this cooperation requires a degree of legislative uniformity, common priorities, and adequate investigative capacity.

EBSCOhost: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY. All use subject to https://www.ebsco.com/terms-of-use.

A. Self-Defense

Regardless of whether or not the perpetrator is organized, the first line of defense against cybercrime is self-defense. Just as is the case in the terrestrial world, people with assets to protect should safeguard them. At the most basic level, parents should exercise a degree of supervision over their children's use of digital technology to reduce the likelihood of their becoming victims or offenders. Ordinary users should invest in an appropriate level of security software, safeguard their PIN numbers, and avoid unsolicited overtures from suspect sources. Large organizations that may be vulnerable to attack should have a security system in place commensurate with the assets that they need to protect. Fortunately, enormous incentives are in place for commercial actors to contribute to cyberspace security. Untold riches await those who can design systems that are easy to use but difficult to exploit for criminal purposes.

B. Capacity Building

Jurisdictions need the legislative and enforcement capacity to respond to cybercrime as it continues to evolve. Because cyber attacks can originate from almost anywhere and can be routed through numerous jurisdictions en route to their target, it is in the interest of all nations that those on the disadvantaged side of the digital divide have the resources to allow cooperation with their better endowed counterparts. Unfortunately, this is easier said than done. The poorest nations cannot afford to pay their police much less establish high-tech crime squads.

Essential to successful interdiction of cross-national organized cybercrime are three factors, namely (1) legislative harmony, (2) a framework of law enforcement cooperation, and (3) the capacity to investigate and, if necessary, to prosecute. The first steps in this direction were taken by the G-8 and by the Council of Europe, whose cybercrime convention has served as a legislative and policy model for a number of non-European nations, including Australia and Japan. The UN Convention against Transnational Crime provides a further framework.

Not all of the world's nations are equally enthusiastic about the Council of Europe Cybercrime Convention, however. Those who were not involved in the laborious work of drafting the convention may feel a lack of "ownership." Others, recalling the history of European imperialism, may harbor suspicions of policies emanating from Europe. Alternative protocols have thus been proposed with a view toward obtaining the imprimatur of the United Nations (Schjolberg and Ghernaouti-Helie 2009).

C. Public/Private Cooperation

In years past, police in many countries would portray themselves as omniscient, omnicompetent, and omnipresent. This posture of invincibility was central to their strategy

EBSCOhost: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY. All use subject to https://www.ebsco.com/terms-of-use.

of public reassurance. More recently, police have conceded that the volume of cybercrime exceeds their capacity to control it on their own. Thus, they have sought to form partnerships with a variety of nonstate actors.

This is entirely appropriate as a great deal of knowledge about cybercrime and its control resides outside of the public sector. The information security industry, for example, commands vast expertise. Software and entertainment industries are often very knowledgeable about the risks they face and about where these risks originate. Large corporations such as Microsoft provide training programs for law enforcement agencies around the world, and they offer monetary rewards for information leading to the identification of virus writers.

D. International Cooperation

Organized cybercrime has proven to be a daunting challenge for law enforcement but not an insurmountable one. One could cite a number of successful investigations, not only within a given jurisdiction, but also investigations of cross-national criminal activity involving law enforcement agencies from many countries. A number of cross-national investigations of organized cybercrime groups have been successful. Among many others, these include the case involving the arrest of two Romanian citizens on an Interpol warrant. Both defendants were extradited to the United States and were charged each with one count of conspiracy to commit fraud in connection with access devices, one count of conspiracy to commit bank fraud, and one count of aggravated identity theft. It was alleged that both defendants and five other Romanian citizens participated in an Internet phishing scheme that victimized individuals, financial institutions, and companies (US Federal Bureau of Investigation 2009).

E. Cyber Security Research

Although networks and software breaches often attract most of the media's attention when it comes to cybersecurity, hardware is similarly vulnerable. A hardware breach can be more difficult to detect and, hence, defend against than a network or software intrusion. The challenge for the public and private sectors is to design technologies that are robust in the sense that their legitimate use is minimally constrained but their illegitimate use is prevented or discouraged (Grabosky 2007). A need exists, arguably, for more research to be funded to find ways to mitigate existing and new cybersecurity risks.

Governments are wise to invest significantly in education, science, and R&D. Doing so would enable information security researchers to play a more significant role in designing state-of-the-art cryptographic software and hardware that can be deployed in an online environment. Of course, criminals are also able to develop and use technologies in furtherance of their own objectives. The future of organized cybercrime seems likely to be characterized by a continuing technological "arms race."

EBSCOhost: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY. All use subject to https://www.ebsco.com/terms-of-use.

V. Conclusion

Few today would challenge the assertion that the era of globalization has been accompanied by an increase in transnational organized crime. Digital technology has empowered traditional criminal organizations, dramatically increasing the ease with which they can commit offenses such as fraud and extortion. It has also enabled the emergence of entirely new crime groups and entirely new crime types, such as online piracy and vandalism. It is likely that, as digital technology becomes more pervasive, its use as an instrument and as a target of organized crime will become increasingly common. Every new technology, and every new application, will be potentially vulnerable to criminal exploitation. It is also likely that new organizational forms will emerge to combat cybercrime. These forms could entail increasingly integrated international and public/private partnerships. Indeed, Susan Brenner has suggested that, one day, the response to cybercrime may be the responsibility of a private multinational body (Brenner, 2002). This may sound farfetched, but it is no more farfetched than was the idea of cybercrime itself a generation ago.

Notes

1. A botnet ("robot network") is a network of individual computers infected with bot malware. These compromised computers are also known as zombies or zombie computers. The zombies, under the control of the botnet controller, can then be used as remote attack tools to facilitate the sending of spam, hosting of phishing websites, distribution of malware, and mounting denial of service attacks. Building botnets requires minimal levels of expertise (Ianelli and Hackworth 2005). A brief two-step overview on how to build a botnet is outlined in Choo (2007).
2. http://www.justice.gov/usao/fls/PressReleases/Attachments/090521-02.Indictment.pdf.
3. http://www.justice.gov/usao/nye/vw/PendingCases/CR-03-304_Indictment_S6-_US_v_SALVATORE_LOCASCIO.pdf.
4. Among the many classified US government documents published by Wikileaks in November 2010 were allegations that the Chinese government orchestrated a systematic campaign of computer intrusions, including "government operatives, private security experts," and specially recruited "internet outlaws" (Shane and Lehren 2010).

References

Bamford, James. 2008. *The Shadow Factory: The Ultra-secret NSA from 9/11 to the Eavesdropping on America.* New York: Doubleday.

Brenner, S. W. 2002. "Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships." *North Carolina Journal of Law & Technology* 4(1):1–50.

EBSCOhost: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY. All use subject to https://www.ebsco.com/terms-of-use.

Broad, William J., and David E. Sanger. 2010. "Worm Was Perfect for Sabotaging Centrifuges." *New York Times* (November 18). http://www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.html?pagewanted=2&emc=eta1

Chang, Yao Chung. 2012. *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait*. Cheltenham: Edward Elgar

Child Exploitation and Online Protection. 2007. "Global Online Child Abuse Network Smashed - CEOP lead international operation into UK based paedophile ring." CEOP (June 18) http://www.ceop.police.uk/Media-Centre/Press-releases/2007/Global-Online-Child-Abuse-Network-Smashed/

Choe, Sanh Hun. 2011. "Seoul Warns of Latest North Korean Threat: An Army of Online Gaming Hackers." *New York Times* (August 4). http://www.nytimes.com/2011/08/05/world/asia/05korea.html?_r=1&scp=1&sq=north%20korea%20hackers&st=cse

Choo, Kim-Kwang Raymond. 2007. "Zombies and Botnets." *Trends and Issues in Crime and Criminal Justice* 333:1–6. http://www.aic.gov.au/publications/current%20series/tandi/321-340/tandi333.aspx

Choo, Kim-Kwang Raymond. 2008. "Organised Crime Groups in Cyberspace: A Typology." *Trends in Organized Crime* 11(3): 270–95.

Choo, Kim-Kwang Raymond. 2009. *Online Child Grooming: A Literature Review on the Misuse of Social Networking Sites for Grooming Children for Sexual Offences*. Research and Public Policy 103. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/rpp/100-120/rpp103.aspx

Choo, Kim-Kwang Raymond, Russell G Smith, and Rob McCusker. 2009. *Future Directions in Technology-Enabled Crime: 2007–09*. Research and Public Policy 78. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/rpp/61-80/rpp78.aspx

Douglis, Fred. 2010. "Closing the Open (Face) Book." *IEEE Internet Computing* (September–October): 4–6.

Falliere N., L. O. Murchu, and E. Chien. 2010. *W32.Stuxnet Dossier: Version 1.3* (November 2010). Cupertino, CA: Symantec.

Grabosky, Peter. 2007. "The Internet, Technology, and Organized Crime." *Asian Journal of Criminology* 2(2): 145–161.

Halstead, Boronia. 1998. "The Use of Models in the Analysis of Organized Crime and Development of Policy." *Transnational Organized Crime* 4(1): 1–24.

Holt, Thomas J. 2007. "Subcultural Evolution? Examining the Influence of On- and Off-Line Experiences on Deviant Subcultures." *Deviant Behavior* 28:171–198.

Hutchinson, S., and P. O'Malley. 2007. "A Crime-Terror Nexus? Thinking on Some of the Links between Terrorism and Criminality." *Studies in Conflict & Terrorism*, 30(12): 1095–1107.

Ianelli N., and A. Hackworth. 2005. *Botnets as a Vehicle for Online Crime*. Pittsburgh, PA: CERT Coordination Center.

Institute of Defence and Strategic Studies (IDSS). 2006. *Proceedings of the International Conference on Terrorism in Southeast Asia: The Threat and Response*. http://www.rsis.edu.sg/publications/conference_reports/NEW%20TerrorismSEAConference05.pdf

Kor, Kor Bian. 2007. "S'pore's diy Terror: Who Is This Man." *The New Paper* (Singapore) (June 10).

LaFraniere, Sharon, and Jonathan Ansfield. 2010. "China Alarmed by Threat to Security from Cyberattacks." *New York Times* (February 11). http://www.nytimes.com/2010/02/12/world/asia/12cyberchina.html?emc=eta1

EBSCOhost: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY. All use subject to https://www.ebsco.com/terms-of-use.

Landler, Mark, and John Markoff. 2007. Digital Fears Emerge after Data Siege in Estonia." *New York Times* (May 29). http://www.nytimes.com/2007/05/29/technology/29estonia.html

Markoff, John. 2009. "Tracking Cyberspies through the Web Wilderness." *New York Times* (May 29). http://www.nytimes.com/2009/05/12/science/12cyber.html?scp=106&sq=dalai+lama&st=nyt

Markoff, John. 2010. "A Silent Attack, but Not a Subtle One." *New York Times* (September 26). http://www.nytimes.com/2010/09/27/technology/27virus.html?scp=5&sq=stuxnet&st=cse

Markoff, John. 2011. "Malware Aimed at Iran Hit Five Sites, Report Says." *New York Times* (February 11). http://www.nytimes.com/2011/02/13/science/13stuxnet.html?scp=3&sq=stuxnet&st=cse

Markoff, John, and Ashlee Vance. 2010. "Fearing Hackers Who Leave No Trace." *New York Times* (January 19). http://www.nytimes.com/2010/01/20/technology/20code.html?scp=4&sq=markoff&st=nyt

McAfee. 2006. *Virtual Criminology Report: Organised Crime and the Internet*. Santa Clara, CA: McAfee.

McCusker, Rob. 2006. "Transnational Organised Cyber Crime: Distinguishing Threat from Reality." *Crime, Law and Social Change* 46(4–5): 257–273.

Ministry of Home Affairs, Singapore (MHA). 2010. "Detention, Imposition of Restriction Orders and Release under the Internal Security Act, July 06, 2010." *Media release* (July 6). http://www.singaporeunited.sg/cep/index.php/web/Our-News/Detention-Imposition-Of-Restriction-Orders-And-Release-Under-The-Internal-Security-Act

Morton, Tom. 2004. "Mutating Mobiles." Background Briefing, ABC Radio National (April 25). http://www.abc.net.au/radionational/programs/backgroundbriefing/mutating-mobiles/3408828#transcript

Munk Centre for International Studies. 2009. "Tracking GhostNet: Investigating a *Cyber Espionage* Network." Toronto: Munk Centre. http://www.nartv.org/mirror/ghostnet.pdf

National Infrastructure Advisory Council (NIAC). 2004. *Prioritizing Cyber Vulnerabilities*. http://www.dhs.gov/xlibrary/assets/niac/NIAC_CyberVulnerabilitiesPaper_Feb05.pdf

National Infrastructure Protection Center 2001. *Cyber Protests: The Threat to the U.S. Information Infrastructure.* National Infrastructure Protection Center, Washington. http://www.au.af.mil/au/awc/awcgate/nipc/cyberprotests.htm

Organisation for Economic Co-operation and Development (OECD). 2007. *The Economic Impact of Counterfeiting and Piracy*. Paris: Organisation for Economic Co-operation and Development. http://www.oecd.org/dataoecd/11/38/38704571.pdf

Perry, Michael. 2005. "Sydney Violence Fueled by Race, Ignorance and Youth." *New York Times* (December15). http://www.redorbit.com/modules/news/tools.php?tool=print&id=330837

Pfanner, Eric. 2011. "Cameron Exploring Crackdown on Social Media after Riots." *New York Times* (August 11). http://www.nytimes.com/2011/08/12/world/europe/12iht-social12.html?scp=1&sq=social+media+london+riots&st=nyt

Preston, Jennifer. 2011. "Movement Began with Outrage and a Facebook Page That Gave It an Outlet." *New York Times* (February 5). http://www.nytimes.com/2011/02/06/world/middleeast/06face.html?pagewanted=1&sq=socialmediaegypt&st=cse&scp=2

Queens County District Attorney. 2011. "111 Individuals Charged in Massive International Identity Theft and Counterfeit Credit Card Operation Based in Queens." *Media release* (October 7). http://www.queensda.org/newpressreleases/2011/october/op%20swiper_credit%20card_id%20fraud_10_07_2011_ind.pdf

EBSCOhost: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY. All use subject to https://www.ebsco.com/terms-of-use.

Sanderson, Thomas. 2004. "Transnational Terror and Organized Crime: Blurring the Lines." *SAIS Review* 24(1): 49–61.

Sanger, David. 2012. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown.

Schjolberg, Stein, and Solange Ghernaouti-Helie. 2009. *A Global Protocol on Cybersecurity and Cybercrime*. Oslo: Cybercrimedata.

Schneider, Jacqueline L. 2003. "Hiding in Plain Sight: An Exploration of the Activities of a Drugs Newsgroup." *Howard Journal of Criminal Justice* 42(4): 372–389.

Serious Organised Crime Agency (SOCA). 2008. *The United Kingdom Threat Assessment of Serious Organised Crime.* London: Serious Organised Crime Agency.

Shane, Scott, and Andrew W. Lehren. 2010. "Cables Obtained by WikiLeaks Shine Light into Secret Diplomatic Channels." *New York Times* (November 28). http://www.nytimes.com/2010/11/29/world/29cables.html?hp

Simon Wiesenthal Center. 2008. *iReport: Online Terror + Hate: The First Decade*. http://www.wiesenthal.com/atf/cf/%7BDFD2AAC1-2ADE-428A-9263-35234229D8D8%7D/IREPORT.PDF

Sipress, A. 2004. "An Indonesian's Prison Memoir Takes Holy War into Cyberspace: In Sign of New Threat, Militant Offers Tips on Credit Card Fraud." *Washington Post* (December 14). http://msl1.mit.edu/furdlog/docs/washpost/2004-12-14_washpost_jihadis_online.pdf

Smith, Russell G., Peter Grabosky, and Greg Urbas. 2004. *Cyber Criminals on Trial.* Cambridge: Cambridge University Press.

Tapscott, Don, and Anthony D. Williams. 2006. *Wikinomics: How Mass Collaboration Changes Everything*. London: Atlantic.

Thomas, T. L. 2003. "Al Qaeda and the Internet: The Danger of 'Cyberplanning.'" *Parameters* 33(1): 112–123. http://www.iwar.org.uk/cyberterror/resources/cyberplanning/al-qaeda.htm

Thompson, Clive. 2004. "The Virus Underground." *New York Times Magazine* (February 8). http://www.nytimes.com/2004/02/08/magazine/the-virus-underground.html

Tokyo Reporter. 2009. "On the 'Tokyo Vice' Beat with Jake Adelstein." (October 27). http://www.tokyoreporter.com/2009/10/27/on-the-tokyo-vice-beat-with-jake-adelstein/

Urbas, Gregor. 2006. "Cross-National Investigation and Prosecution of Intellectual Property Crimes: The Example of 'Operation Buccaneer.'" *Crime Law and Social Change* 46(4–5): 207–221.

US Department of Justice. 2004. "Fourth Defendant in Massive Internet Scam Pleads Guilty to Fraud and Money Laundering Charges Case Involves $60 Million in Investments by 15,000 Investors." *Media release* (November 18). http://www.justice.gov/criminal/cybercrime/press-releases/2004/nordickPlea_triwest.htm

US Department of Justice. 2005. "Former FBI Agent Pleads Guilty to Obstruction of Justice." *Media release* (June 23). http://www.justice.gov/usao/nye/pr/2005/2005jun23.html

US Department of Justice. 2008a. "Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major US Retailers." *Media release* (August 5). http://www.justice.gov/opa/pr/2008/August/08-ag-689.html

US Department of Justice. 2008b. "38 Individuals in US and Romania Charged in Two Related Cases of Computer Fraud Involving International Organized Crime: International Law Enforcement Cooperation Leads to Disruption of Organized Crime Ring Operating in US and Romania." *Media release* (May 19). http://www.justice.gov/opa/pr/2008/May/08_odag_434.html

EBSCOhost: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY. All use subject to https://www.ebsco.com/terms-of-use.

US Department of Justice. 2009a. "Detroit Spammer and Three Co-conspirators Sentenced for Multi-million Dollar E-mail Stock Fraud Scheme." *Media release* (November 23). http://www.justice.gov/opa/pr/2009/November/09-crm-1275.html

US Department of Justice. 2009b. "Major International Hacker Pleads Guilty for Massive Attack on US Retail and Banking Networks." *Media release* (December 29). http://www.justice.gov/opa/pr/2009/December/09-crm-1389.html

US Department of Justice. 2010. "High Ranking Crime Family Soldier Pleads Guilty to Racketeering Charge." *Media release* (January 5). http://www.justice.gov/usao/nj/Press/files/pdffiles/2010/mer00105%20rel.pdf

US Federal Bureau of Investigation. 2008. "Gone Phishing: Global Ring Gets Rather Slick." (May). http://www.fbi.gov/page2/may08/phishing_052008.html

US Federal Bureau of Investigation. 2009. "Two Romanian Citizens Extradited to the United States to Face Charges Related to Alleged Phishing Scheme." *Media release*. (September 29). http://www.fbi.gov/newhaven/press-releases/2009/nh092909.htm

White, Rob. 2006. "Swarming and the Social Dynamics of Group Violence." *Trends and Issues in Crime and Criminal Justice* 326:1–6.

Williams, Phil. 2001. "Transnational Criminal Networks." In *Networks and Netwars,* edited by John Arquilla and David Ronfeldt. Santa Monica, CA: RAND Corporation, 61–97.

EBSCOhost: eBook Collection (EBSCOhost) printed on 9/20/2025 12:37:09 AM UTC via CHARLES STURT UNIVERSITY. All use subject to https://www.ebsco.com/terms-of-use.