Cybercrime and Economic Crime

7

ALEXANDER SEGER

Contents

Introduction: Ecosystem of Cybercrime

Crime does not take place in isolation. It is affected by its political, economic, socio-cultural, technological, ecological, and legal or regulatory environment. Crime is shaped by its environment, interacts with it, and influences it. Thus, in many ways, crime and its environment constitute an ecosystem.

Environmental scans* help explain, for example, that drug-related crime is a function of globalization, political conditions, historical and socio-cultural factors, and human development.† Money laundering is not simply a consequence of drug trafficking; the globalization of the financial system prepared the ground for the laundering of the proceeds of all types of crimes.‡ The fall of the wall of Berlin in 1989 and the subsequent period of transition of Central and Eastern European countries toward democracy and market economies created opportunities for organized crime and corruption that led to regulatory responses§ that subsequently forced the "old" democracies of Western Europe to adopt stricter measures in their own countries. Additionally, the September 11, 2001 attacks led to actions to prevent terrorism and considerable reinforcement of actions against money laundering¶, including the confiscation of crime proceeds, due diligence, expanded supervision, and other preventive measures in the financial sector. These measures were further reinforced in the wake of the recent global financial crisis.

This seems particularly true for cybercrime. The evolution, relevance, and impact of cybercrime can only be understood in the context of the evolution of information and communication technology (ICT) and the consequent emergence of the information network society.** This evolution has certainly

* The Council of Europe introduced environmental scans in its annual organized crime situation reports from 2001 to 2005. Search also for PEST (analysis of the environment divided into Political, Economic, Socio-cultural, and Technological domains) or PESTEL analysis (of PEST plus Ecological and Legal domains).

† See Seger, A. (1998): Entwicklung und Drogen in Asien: Drogenprobleme, Drogenkontrolle und nachhaltige menschliche Entwicklung in Laos, Afghanistan und Pakistan. PhD Thesis, Bonn.

‡ From an international regulatory perspective, money laundering was first dealt with in 1988 in the United Convention on Illicit Traffic in Narcotic Drugs and Psychotropic Substances. More recent agreements favor an all-crimes approach. See Council of Europe Convention on the Laundering, Search, Seizure and Confiscation of Proceeds from Crime and the Financing of Terrorism (CETS 198) of 2005.

§ See soft- and hard-law instruments developed by Council of Europe covering money laundering, corruption, organized crime, trafficking in human s, and international cooperation in criminal matters from 1990 onward that apply to all 47 European countries; also see monitoring mechanisms such as GRECO and MONEYVAL (www.coe.int/economiccrime).

¶ Prior to September 11, 2001, the U.S. government planned to reduce its participation in international anti-money laundering efforts, but reversed these plans soon afterward.

** Castells, M. (2000).

been the most influential factor and transformed societies worldwide during the past decade. In the information society, "the creation, distribution, and manipulation of information has become the most significant economic and cultural activity."* For illustration, it is estimated that Internet use grew by some 445% between 2000 and 2010; some 2 billion people now use it.† While penetrations rates are unequal among regions (77.4% in North America, only 10.9% in Africa) and a digital divide continues all regions have experienced significant growth.‡

There is general agreement that the rise of the information society offers unique opportunities to people worldwide in terms of economic development and also in fostering human rights and democracy.§ ICT changed the ways companies and people do business and offer, buy, and sell products and services. The participatory information sharing of Web 2.0 altered the ways people interact with each other globally with fewer frontiers and on a "flat playing field."¶

Obviously, businesses at all levels are now required to maintain online presences to succeed. The financial sector took advantage of ICT at an early stage to prepare the ground for borderless, around-the-clock global trading and offering of services.** Public administrations also function online by offering electronic government services and organizing elections through e-voting. Estonia is very advanced in these respects.†† In summary, both people and businesses around the world rely on ICT. As a result public services and infrastructures have also become highly dependent on ICT and this reliance makes societies vulnerable.

A major threat arising from the evolution of ICT is cybercrime. Is it not surprising that criminals use ITC to commit crimes and also actively search for vulnerabilities in the systems and exploit them?‡‡ The evolution of the global information society led to a proliferation of cybercrime to the point that it can be argued that cybercrime and the information society form an ecosystem in which crime continues to exploit new technologies and related

* This is a widely used and simple definition of "information society." See http://whatis.techtarget.com/definition/0,,sid9_gci213588,00.html

† http://www.Internetworldstats.com/stats.htm

‡ This is also true for Africa with a growth in Internet use of 2.357% in the past 10 years and further growth expected from the expansion of fiber optics technology there.

§ See documentation related to the World Summit on the Information Society (http://www.itu.int/wsis/index.html) and discussions of the Internet Governance Forum (http://www.intgovforum.org/cms/).

¶ Friedman, Th. (2006).

** With positive but also disastrous consequences.

†† e-Estonia (http://www.valitsus.ee/?id=5450).

‡‡ Illustrated by high underground market value of "zero-day exploits", that is, vulnerabilities in software that are not known and against which no countermeasures have been taken, so that an attack is likely to be very successful.

developments or morphs to countermeasures in an opportunistic manner.* Cybercrime may even be considered an integral part of the information society as reflected in the following definition:

> Post-industrial society in which information technology (IT) is transforming every aspect of cultural, political, and social life and which is based on the production and distribution of information. It is characterized by the (1) pervasive influence of IT on home, work, and recreational aspects of the individual's daily routine, (2) stratification into new classes: those who are information-rich and those who are information-poor, (3) loosening of the nation state's hold on the lives of individuals and the rise of highly sophisticated criminals who can steal identities and vast sums of money through information related (cyber) crime.†

This chapter aims to explain the concept of cybercrime, provide an overview of trends and data, demonstrate how cybercrime is an economic offense, and discuss effective practices for countering cybercrime threats.

Concept of Cybercrime

Cybercrime can be defined in many ways. One could argue that, in essence, cybercrime is not an entirely new type of conduct, but simply an extension of already existing criminal behavior; the only difference is that cybercrime utilizes new technologies.‡ Another approach is to define it as any crime in which a computer is the agent, facilitator or target of the crime.§ This is a broad concept since most crime now involves a computer in some way. The definition could also be limited to cover all crimes targeting computer data or systems. However, this definition would exclude crimes that existed earlier and gained greater impacts through the use of computers, for example, child pornography, fraud, and intellectual property right violations.

It is therefore expedient to apply a definition that covers new types of crime along with old types of crime involving computer use¶ without being too broad and therefore meaningless. The definition should be sufficiently robust to cover all relevant types of conduct even if technology evolves and

* See Information Warfare Monitor/Shadowserver Foundation (2010) for a description of the ecosystem of crime and espionage embedded in the fabric of global cyberspace (http://www.nartv.org/mirror/shadows-in-the-cloud.pdf).
† http://www.businessdictionary.com/definition/information-society.html
‡ http://www.britannica.com/EBchecked/topic/130595/cybercrime/235698/Defining-cybercrime
§ Definition used by Symantec. See http://securityresponse.symantec.com/en/uk/norton/cybercrime/definition.jsp
¶ Europol. (2007).

cybercrime techniques appear to change constantly. Moreover, the definition should be widely accepted, and finally it should be possible to operationalize and use it, for example, for criminal law purposes.

A definition meeting these criteria became available via the Council of Europe's Budapest Convention on Cybercrime.* The treaty denotes cybercrime as offenses against the confidentiality, integrity and availability of computer data and systems,† that is, offenses against computer data and systems, including:

- Illegal access to a computer system, such as "hacking" (Article 2)
- The illegal interception of the transmission of computer data (Article 3)
- Data interference, that is, the damaging, deletion, deterioration, alteration or suppression of computer data (Article 4)
- System interference, that is, hindering of the functioning of computer systems (Article 5), including denial of service attacks
- The misuse of devices (Article 6)—the production, sale, procurement, or otherwise making available of devices or data (e.g., hacking tools) for purposes of committing the above offenses,
- Offenses committed by means of computer systems (limited‡ to "old" forms of crime that produce new impacts through the use of computers:
- Computer-related forgery, that is, conduct resulting in inauthentic data that is acted upon for legal purposes as if it were authentic (Article 7)
- Computer-related fraud, that is, the causing of loss of property to another person by any input, alteration, deletion, or suppression of computer data or the interference with the functioning of a computer system with the intent of procuring an economic benefit (Article 8)
- Child pornography, that is, the production, offering or making available, distribution or transmission, procuring through or possession in a computer system or storage medium of pornographic material that visually depicts a minor (under age 18) engaged in sexually explicit conduct (Article 9)§
- Offenses related to infringements of copyrights and related rights on a commercial scale (Article 10).

* www.coe.int/cybercrime

† The so-called cia offenses.

‡ The Budapest Convention procedural laws and international cooperation measures apply to any crime involving electronic evidence or committed via a computer system. This provides the treaty with wide scope (see Article 14).

§ This article also covers persons appearing to be minors or realistic images even if no real minor is a victim. Not all countries agree to this and therefore reservations of this article are possible.

This approach may at first appear too simple in the face of complex crimes. For example, in 2009 and 2010, a widespread phenomenon was the Zeus Trojan horse used to steal banking information. This malware spread primarily through drive-by downloads when Internet users clicked on infected online advertisements. This installed the malware on the user's computer that acted as a robot ("bot") or zombie controllable from a command and control (CC) server operated by criminals.

When the user accessed his bank account online to make a financial transaction, the login credentials and other relevant data were transferred to the CC server. The transaction was intercepted automatically and modified to transfer the money to the account of a "money mule" who made it available for this purpose. From there it was transferred to other accounts and finally cashed out or laundered. The transaction appeared legitimate to the banking computer because the instruction appeared to have come from the accredited user and the user also received a receipt from the bank that appeared to be correct.* Schemes of this type involved hundreds of victims and millions of euros and dollars.

The COE definition cited above is capable of capturing cases that combine illegal access, illegal interception, data and systems interference, forgery, and fraud.

Although the Budapest Convention was sponsored by the Council of Europe (with 47 current European member states), Canada, Japan, South Africa, and the U.S. participated. The U.S. became a full party to the treaty in 2006. A number of other non-European countries are in the process of accession.† Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, and the Philippines have been invited to accede. Many more countries used the treaty as a guideline for domestic legislation (Botswana, Mauritius, Senegal, India, Indonesia, and Sri Lanka). In short, the concept or definition of cybercrime proposed by the Budapest Convention is widely shared and applied in practice.

* See the case documented by M 86 Security (White Paper): Cybercriminals Target Online Banking Customers (August 2010). http://www.m86security.com/documents/pdfs/security_labs/cybercriminals_target_online_banking.pdf Similar cases have been investigated in other countries including Germany and Belgium.

† Council of Europe (2010): Contribution of the Secretary General of the Council of Europe to the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Salvador, Brazil, 12–19 April 2010 (SG/INF (2010) 4). http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/SG%20Inf%20_2010_4%20-%20UN%20Crime%20congress_ENGLISH.pdf

Tools and Infrastructure of Cybercrime

Cybercriminals rely on a set of tools and an infrastructure that include several elements described below.

Malware

Malicious software or "malware" denotes all types of software "inserted into an information system to cause harm to that system or other systems or subvert them for uses other than those intended by their owners."[*,†]

Viruses—A virus is hidden code that is activated when its host program is run and it spreads from there to other programs. A virus can simply slow the performance of a computer or damage, alter, and destroy data.

Worms—A worm is similar to a virus but replicates itself without the need for a host program.

Trojan horses—A Trojan horse or other type of spyware may appear to be a legitimate program but has functionalities that disable security systems or contain a key logger that records what the user types including passwords and online banking credentials that may subsequently be transmitted to criminals when the computer is online.

Malware has been around for more than 20 years; the "Morris worm" raised public attention in 1988 when it infected 10% of the then 60,000 personal computers connected to the Internet in less than 2 hours.[‡] Malware remains the main tool for committing cybercrime and is reported to have evolved into a major industry with a complex economic infrastructure and well-organized and well-funded criminal gangs.[§] Viruses, worms, and Trojans that cripple security applications, download additional malware, infect files, and steal logins, account credentials, and other data are considered the most malicious code samples.[¶]

[*] OECD (2007).
[†] OECD (2007).
[‡] Schmidt, H. (2006), p. 72.
[§] *Sophos Security Threat Report*. (August 2010). p. 28. http://www.sophos.com/security/topic/security-report-2010.html
[¶] For statistics, see Symantec Intelligence Quarterly, April–June 2010. http://www.symantec.com/business/theme.jsp?themeid=threatreport; Microsoft Security Intelligence Report, Vol. 8, July–Dec. 2009. http://www.microsoft.com/security/about/sir.aspx

Increasing numbers of computers are becoming infected. [*] Most computers become compromised through the Internet, for example, by visiting websites that may appear to be legitimate but are infected; visitors may also be redirected to infected pages.[†]

E-mail, particularly spam, is another vehicle for spreading malware, often in connection with fraud schemes.[‡] It is estimated that 75 to 90% of all e-mail traffic consists of spam.[§] It is surprising that most spam can be traced back to a small group of operations.[¶] The main tool for spam and for other types of cybercrime is botnets.

Social networking sites and the number of users expanded considerably in recent years.[**] Social sites are now also used to spread malware and find targets for other forms of cybercrime; as a result they constitute security risks. According to Sophos,[††] social networks have become viable and lucrative markets for malware distribution with Web 2.0 botnets stealing data, displaying fake antivirus alerts, and generating income for criminals.

Botnets

A computer can be infected by malware that turns it into a zombie, robot, or bot; this allows it to be controlled by a third person without the knowledge of a legitimate user.[‡‡] The person who controls the computer can instruct it to send spam messages, spread malware, or act as a proxy to conceal the origin of an attack.

A bot-infected computer is usually connected to a command and control (CC) server from which additional malware is installed, instructions are received, or data is sent. When many of these bot computers are linked and controlled by the same CC server, they form a "botnet" managed by

[*] In Germany, it was estimated in 2010 that 43% of Internet users experienced malware infections of their computers. http://www.bitkom.org/65019_65010.aspx According to Symantec, 51% of computers globally experienced malware. http://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf

[†] Sophos Security Threat Report. http://www.sophos.com/security/topic/security-report-2010.html

[‡] Microsoft Security Intelligence Report, Vol. 8, July–Dec. 2009. http://www.microsoft.com/security/about/sir.aspx

[§] According to Commtouch Internet Threats Trend Report, first quarter, 2010, spam and phishing messages average 183 billion per day. www.commtouch.com/download/1679

[¶] Spamhouse lists about 100 such operations in its Register of Known Spam Operations (ROKSO) database. http://www.spamhaus.org/rokso/

[**] Facebook alone claims some 500 million active users. http://www.facebook.com/press/info.php?statistics

[††] Sophos Security Threat Report. http://www.sophos.com/security/topic/security-report-2010.html

[‡‡] See Microsoft Security Intelligence Report, Vol 9, Jan.–June 2010 with detailed analysis of botnets (http://www.microsoft.com/security/sir/)

a "bot herder." They may involve hundreds of thousands or even millions of computers,* and some are capable of sending tens of billions of spam or phishing messages per day.

Botnets are thus powerful tools in the hands of organized criminals for spreading spam and malware and intercepting and stealing confidential information. In addition, they can be used for denial-of-service (DOS) attacks. When thousands of computers send requests to the same domain name server† at the same time, the system is overloaded and service is denied. DOS attacks can thus be used to paralyze the information infrastructure of an organization, sector, or even a country‡ while clear attribution is difficult because many thousand systems appear to be the sources of attacks.

Underground Economies

An underground economy usually involves exchanges of goods and services that are hidden from official view".§ Such an underground economy has now become available on the Internet and has become a critical pillar of the infrastructure of cybercrime. It provides malware and other tools for committing crimes, rents botnets to carry out attacks, develops malware and anti-forensics techniques to avoid detection, and supplies bullet-proof hosting of domains used for criminal purposes¶ and spam delivery. An underground economy offers a market for stolen goods, in particular credit card or bank account details and other personal information useful for identity-related fraud** and drop zones for stolen goods and crime proceeds. In short,

* Mariposa botnet dismantled in December 2009 consisted of 12 million infected computers.

† A DNS server translates a request with a memorable human name (e.g., www.coe.int) into a numeric Internet protocol (IP) address (193.164.229.51) that identifies and locates the corresponding computer system on the Internet.

‡ One of the best known examples is the attack against Estonia in May 2007.

§ http://www.encyclopedia.chicagohistory.org/pages/1280.html

¶ Many bullet-proof domains are reportedly hosted in Eastern Europe and the Far East. For Europe, see report by Spamhouse on the criminal 'Rock Phish' domains registered at Nic.at (http://www.spamhaus.org/organization/statement.lasso?ref=7) http://en.wikipedia.org/wiki/Bulletproof_hosting Registrars and registries often fail to exercise due diligence when domains are registered. The 2010 Octopus conference of the Council of Europe recommended due diligence measures by ICANN, registrars and registries and accurate WHOIS information, and endorsement of the Law Enforcement Recommended Amendments to ICANN's Registrar Accreditation Agreement (RAA) and Due Diligence Recommendations in line with data protection standards (http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/2079_IF10_messages_1s%20provisional%20_24%20Apr%2010.pdf).

** *Symantec Intelligence Quarterly*. Apr.–June 2010. http://www.symantec.com/business/theme.jsp?themeid=threatreport.

the underground economy offers an economic environment for offenders to organize for cybercrime.*

Money Mules

After a crime is committed, the victims have been defrauded, and money has been stolen, criminals must transfer the proceeds online without disclosing or leaving traces of their own identity. This appears to be the most difficult part of economic crime on the Internet. The most common transfer practice is using "money mules" or "financial agents" who open bank accounts or make their own accounts available for transfers of proceeds of crimes. After mules have the funds in their accounts, they receive further instructions to transfer them to other accounts or send them abroad via wire transfer and retain their commissions.† Mules may be recruited via e-mail, respond to spam, or access what appear to be legitimate websites offering work at home or financial manager jobs. They may sign formal contracts and deposit copies of ID documents. Not all of them are aware that they are essential parts of a criminal enterprise.

Organized Cybercrime

The Council of Europe, in its 2004 organized crime situation report, formulated some general hypotheses regarding links between cybercrime and organized crime.‡ These were validated in the following years, and are still valid today:§

- ICTs offer anonymity, facilitate logistics, and reduce the risks for organized criminals to be prosecuted. They facilitate remotely controlled operations, covert activities, transnational operations, networking, and encrypted communication.
- The penetration and infiltration of banks and corporations along with online bank robberies via the Internet are far less risky than burglaries in the real world. Modern computer and communication networks have developed specific characteristics that are useful for criminal perpetrators and difficult for prosecutors to overcome. International computer networks offer anonymity to perpetrators

* G Data Whitepaper on Underground Economy, 2009: http://www.gdata-software.com/uploads/media/Whitepaper_Underground_Economy_8_2009_GB.pdf
† http://www.banksafeonline.org.uk/moneymule_explained.html
‡ Council of Europe (2004).
§ Extracts from Council of Europe (2005, p. 42–43). The authors were responsible for the preparation of that report.

that can be lifted only if all countries crossed by a communication decide to cooperate.
- ICTs are tools for global outreach and search for potential victims.
- ICTs are likely to change the structure of organized crime, that is, the way members organize to carry out crimes.

Depersonalization of contacts, ease of access, and rapidity of electronic transactions make ICTs attractive tools for money laundering. Organized crime exploits the vulnerabilities of societies, public institutions, businesses, and individuals using the Internet. Exploitation affects not only corporations engaged in e-commerce and business-to-business operations, but also involves electronic theft and phishing. Even children are vulnerable.

As economic crime already is a primary activity of organized crime groups, information and communication technologies will further facilitate the commission of new types of fraud. Traditional crimes will have the help of new technologies and morph into electronic bank robberies, cyber extortion and other forms.

Cybercrime does not require control over a geographical territory. It requires few personal contacts and fewer relationships based on trust and enforcement of discipline. In summary, it presents less need for formal organization. The classical hierarchical structures of organized crime groups may even be unsuitable for Internet crime. ICTs favor organizations that are already based on flat structured networking.

ICTs may also change the characteristics of offenders. In the real world legal businessmen engage in organized forms of economic crime. *Modus modendi*, the opportunities offered by ICTs, may tempt legal commercial entities to organize for cybercrime, that is, become organized cyber criminals. The complexity of many cybercrime operations, the infrastructure used, the level of specialization, and the division of labor are all indications of structured organized criminal groups that act in concert to commit offenses to obtain financial or other material benefits.*

Internet Fraud

People have many reasons to commit cybercrimes. So-called "script kiddies" may be eager to prove how clever they are and in doing so may create major damage.† Pedophiles may use the Internet to pursue their sexual interests by grooming victims or exchanging child abuse materials. Terrorists may use ICTs for

* As defined in Article 2 of the United Nations Convention on Transnational Organised Crime.

† A notorious example is the "I-love-you bug" launched by a student in the Philippines in 2000.

propaganda, recruitment, training and other preparatory acts, target identification, communication, financing and other logistical purposes, or implementing denial-of-service or other types of attacks against critical infrastructures.[*]

Other politically motivated attacks[†] may include "hacktivism," espionage, or conflicts via computer systems such as the intrusions and denial-of-service attacks on Estonia in 2007,[‡] Georgia in 2008,[§] the U.S. and South Korea in July 2009,[¶] the Google intrusion in December 2009,[**] the intrusion into governmental, business and academic computer systems in India in 2009, the Stuxnet worm reportedly designed to sabotage Iranian nuclear power plants,[††] and the attacks and counterattacks following the release of U.S. State Department internal documents by Wiki Leaks in late 2010.[‡‡] Nevertheless, it seems that most cybercrime is aimed at generating economic benefits for offenders. Cybercrime therefore is very much about fraud.

Computer-Related Fraud

Fraud broadly involves intentional deception by which one person causes loss to another for economic gain. It can be defined as "an intentional misrepresentation of material existing fact made by one person to another with knowledge of its falsity and for the purpose of inducing the other person to act, and upon which the other person relies with resulting injury or damage."[§§]

Whether fraud takes place on the Internet or is related to computer systems in any other way should be irrelevant. In some countries, however, the law requires that a person or a human mind is deceived for a specific conduct

[*] http://book.coe.int/EN/ficheouvrage.php?PAGEID=36&lang=EN&produit_aliasid=2221 http://www.mpicc.de/ww/en/pub/forschung/forschungsarbeit/strafrecht/cyberterrorismus.htm http://www.indiajournal.com/pages/event.php?id=6472 http://www.securitydefenceagenda.org/Portals/7/Reports/2008/SoD_110208_cyber.pdf

[†] Also named "Advanced Persistent Theats" or APT. http://www.mandiant.com/services/advanced_persistent_threat/. For a brief definition see http://www.damballa.com/knowledge/advanced-persistent-threats.php

[‡] http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

[§] http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf

[¶] http://www.guardian.co.uk/world/2009/jul/08/south-korea-cyber-attack http://en.wikipedia.org/wiki/July_2009_cyber_attacks

[**] http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html

[††] http://www.schneier.com/blog/archives/2010/10/stuxnet.html http://www.computerweekly.com/Articles/2010/11/30/244264/Iran-confirms-Stuxnet-hit-uranium-enrichment-centrifuges.htm

[‡‡] http://www.cbsnews.com/stories/2010/11/29/world/main7099028.shtml http://www.nbcconnecticut.com/news/politics/Lieberman-Among-Many-Caught-in-Suspected-Wiki-Leaks-Cyber-Attack-111590714.html http://news.yahoo.com/s/afp/20101208/tc_afp/usdiplomacywikileaksInternetcomputersecurity

[§§] http://definitions.uslegal.com/f/fraud/

to qualify as fraud. A computer system deceived through the manipulation of data and tricked into transferring money to a specific account may not necessarily constitute fraud. In Germany, for example, a specific article had to be introduced into the criminal code to cover computer-related fraud.* This article is based on a specific provision of the Budapest Convention on Cybercrime of the Council of Europe†:

> **Article 8: Computer-related fraud** — Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: (a) any input, alteration, deletion or suppression of computer data; (b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Forgery is a related concept. The Budapest Convention requires parties to the treaty to criminalize the following conduct in their domestic legislation:

> **Article 7: Computer-related forgery** — Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

These definitions and legal provisions help capture a wide range of fraud by not only addressing physical world conduct but also covering the specifics of computer-related forgery and fraud even if technology keeps evolving. Nevertheless, they are too broad to allow for an analysis of fraud and related crime on the Internet.

An organization that has been collecting data on cybercrime and is receiving more than 100,000 complaints per year is the Internet Crime Complaint Center (IC3)‡ in the U.S. The IC3 has been struggling with the challenge of

* Brunst, P. & Sieber, U. (2010), p. 730.

† For the Budapest Convention explanatory report and the status of signatures, ratifications, and accessions, see www.coe.int/cybercrime

‡ Internet Crime Complaint Center. (2010). Internet Crime Report. http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

categorizing types of fraud that make reporting by victims simple and at the same time accommodating the complexity and constant evolution of fraud schemes to achieve meaningful analysis. Until 2008, the IC3 classified frauds into nine categories:

1. Business fraud (including bankruptcy fraud, IPR infringements and counterfeit goods)
2. Communications fraud (including theft of IT and communication services)
3. Confidence fraud (including action fraud, non-delivery of goods, advance fee fraud)
4. Financial institutions fraud (including credit and debit card fraud, and identity theft)
5. Gaming fraud (betting and online gambling fraud)
6. Government fraud (including tax evasion, welfare fraud, counterfeiting currency)
7. Insurance fraud
8. Investment fraud (including market manipulation and pyramid schemes)
9. Utility fraud

However, this methodology that involved a large number of subcategories was replaced in the 2009 report to avoid overlap, ensure clearer distinctions, reduce the number of subcategories, and extend the scope beyond fraud. The new classification covers 79 complaint types encompassing fraud and also drug trafficking, intimidation, pornography, terrorism, and a range of other offenses involving the Internet.

The IC3 in 2009 received 336,655 complaint submissions, of which 146,663 were referred to law enforcement. Most of the referrals concerned non-delivery of goods and services (19.9%), identity theft (14.1%), debit and credit card fraud (10.4%), and auction fraud 10.3%).* In Europe as well, most cybercrime reported and recorded by law enforcement is about fraud. In Germany, for example, more than one-third of computer crimes recorded in federal police statistics concern "carding" (the use of unlawfully obtained credit or debit cards). In addition, the German Federal Criminal Police in 2009 recorded more than 50,000 cases of cybercrime of which more than 70% were related to fraud and forgery.†

While it is acknowledged that fraud is the most prevalent type of cybercrime, it remains unclear how to differentiate the many categories of fraud.

* Internet Crime Complaint Center (2010): Internet Crime Report. http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

† http://www.bka.de/lageberichte/iuk/bundeslagebild_iuk_2009.pdf

For example, identity theft is sometimes described as a specific type of fraud separate from carding or account take-over, and sometimes it is limited to the theft of a person's identity, that is, a step before the stolen identity is used to commit fraud. While discussions about the best way to classify fraud involving the Internet will have to continue, for the purposes of this chapter, we assume that identity theft is a constituent of many types of fraud.

Identity Theft

Identity theft may be interpreted in various ways. Some argue that it pertains only to the theft of personally identifiable information (PII). Others consider identify theft to mean that PII is stolen with the intention to commit fraud. Those concerned about legal responses maintain that the possession and transfer of PII of another person with fraudulent intention must be criminalized, particularly if the underground economy is to be targeted.

For example, the U.S. Identity Theft and Assumption Deterrence Act [United States Code, Title 18, Section 1028(a)(7)] imposes punishment on a person who "knowingly transfers or uses, without lawful authority, of a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."

Others include the theft of PII, possession, transfer or fraudulent intention, and the actual commission of fraud and define ID theft as "fraud or another unlawful activity where the identity of an existing person is used as a target or principal tool without that person's consent."* Considering these various approaches, ID theft involves three distinct phases†:

1. The obtaining of identity information, for example, through physical theft, through search engines, insider attacks, attacks from the outside (illegal access to computer systems, Trojans, key loggers, spyware, and other malware), or phishing and other social engineering techniques
2. The possession and disposal of ID information, which includes the sale of such information that now plays an important role in the e-underground economy where credit card information, bank account details, passwords or full identities are among the most offered goods

* Definition proposed by Koops, B.J. & Leenes, R. (2006). http://www.fidis.net/fileadmin/fidis/publications/2006/DuD09_2006_553.pdf

† Seger, A. (2007), p. 154. http://www.ispac-italy.org/pubs/ISPAC%20-%20Identity%20Theft.pdf; http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf

3. The use of ID information to commit fraud or other crimes, for example by assuming another person's identity to exploit bank accounts and credit cards, create new accounts, obtain loans and credit, order goods and services, or disseminate malware.

Phishing (fishing for passwords) is one of the most common social engineering techniques used for ID theft. Users are encouraged to disclose passwords, access credentials for online accounts, and other personal information on seemingly legitimate websites. Organizations such as the Anti-Phishing Working Group* record more than 100,000 such attacks every year.

Alternative techniques include smishing (mobile phone text messaging to seek the disclosure of information), spear phishing (targeted phishing of specific persons or groups), pharming (redirection of users to bogus websites), and spoofing (sending an e-mail seeking personal information in the name of an apparently known and legitimate person. However, while phishing and similar techniques are widespread, other forms of theft through illegal access, illegal interception, data interference, attacks against computer data and systems, physical attacks, thefts by insiders, or simply losses of data through negligence are equally important.

After bank account or payment card details, PIN codes or other access credentials, place and date of birth, mailing address, and other personally identifiable data are obtained, the information can be used to commit fraud.

Types of Fraud

Identity theft and fraud in relation to online payments, particularly, payment card fraud, online banking misuse, and account take-over, constitute most computer-related fraud in most countries. Too many types of fraud exist to be detailed here, but we will discuss some of the most common ones.

Payment Card Fraud

The most reported type of payment card fraud involves card-not-present (CNP) payments made via Internet, telephone, or mail order by using genuine but stolen card details. For example, in the United Kingdom, CNP fraud was responsible for more than half of the losses from payment card fraud in 2009.†

Other types of payment card fraud include the use of counterfeit cards that include data from stolen genuine cards. For example, a genuine card is

* http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf
† £266.4 million of total losses of £440.3 million in 2009. See Financial Fraud Action UK (2010).

"skimmed" and then "cloned." Furthermore, lost or stolen cards can be used for purchases that do not require PIN codes. Finally, a new credit or debit card account may be opened in the name of another person on the basis of stolen ID information.

Online Banking Attacks and Account Takeover

After bank account details and online banking credentials have been stolen through phishing and other techniques, an account can be taken over to make payments or transfer money, often to the accounts money mules. Taken-over accounts can also be used to apply for new accounts, loans, new credit cards, or used as mule accounts to receive and transfer money from other criminal operations. Another technique is compromising computers through Trojans that intercept communication between the user and his bank in the course of online payments so that money is transferred to an account different from the intended one.

Mass Marketing Fraud

Mass marketing fraud consists of "fraud schemes that use mass communications media including telephones, the Internet, mass mailings, television, radio, and even personal contact, to contact, solicit, and obtain money, funds, or other items of value from multiple victims in one or more jurisdictions."* Variations include advance-fee fraud,† 419 fraud,‡ lotteries,§ and phony prize winning schemes. Mass marketing fraud is often committed by criminal enterprises that operate globally and create losses estimated at several billion dollars per year.

Confidence Fraud Including Auction Fraud

Because many people purchase goods and services on the Internet and through online auctions, confidence and auction fraud are among the most reported offences on the Internet.¶,** Confidence fraud is the misrepresentation of a product advertised for sale or the non-delivery of goods for which customers paid.

* According to International Mass-Marketing Fraud Working Group (June 2010). http://www.fincen.gov/news_room/rp/reports/pdf/IMMFTAFinal.pdf
† http://www.consumerfraudreporting.org/nigerian.php
‡ Article 419 of the Criminal Code of Nigeria criminalizes such conduct. http://www.efccnigeria.org
§ http://www.consumerfraudreporting.org/lotteries.php
¶ http://www.consumerfraudreporting.org/auctionfraud.php
** U.S. Internet Crime Complaint Center lists non-delivery as the complaint most often cited to law enforcement in 2009 (19%). http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

Investment Fraud Including Stock Market Manipulation

The Internet creates opportunities for investment fraud and stock market manipulation, for example, by online "pump and dump" schemes in which a large volume of low value stock is purchased and subsequently a spam or telemarketing campaign encourages its purchase. When those behind the scheme sell their shares and stop promoting the stock, its price drops rapidly and other investors are left with stock worth significantly less than they paid for it.

Counterfeit Pharmaceuticals

Counterfeit medicines and medical devices represent a criminal market worth billions of dollars. The World Health Organization defines a counterfeit medicine as "one which is deliberately and fraudulently mislabeled with respect to identity and/or source. Counterfeiting can apply to both branded and generic products and counterfeit products may include products with the correct ingredients or with the wrong ingredients, without active ingredients, with insufficient active ingredients or with fake packaging."[*]

Criminal enterprises exploit the opportunities offered by the Internet, namely to trade in counterfeit medicines to generate high profits at low risk and low cost in a global market place. The two main means are:

- Internet pharmacies that often sell substandard, non-approved or counterfeit medicines.[†] The money is paid by customers through online payment systems to banks abroad.[‡]
- Mass marketing fraud or spam messages related to pharmaceuticals reportedly account for the largest share of many billion spam messages sent daily.[§] Spammers may send messages on behalf of a particular e-pharmacy or act as affiliate advertisers that receive commissions for clicks on a spam message or for actual sales.[¶]

[*] http://www.who.int/medicines/services/counterfeit/overview/en/

[†] http://v35.pixelcms.com/ams/assets/312296678531/455_EAASM_counterfeiting%20report_020608.pdf

[‡] See Moneyval typology study on money laundering and counterfeiting (2008). http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL(2008)22RRepTyp_counterfeiting.pdf

[§] For 81% of the 183 billion spam messages sent per day according to the Commtouch Internet Threats Trend Report Q1 2010. www.commtouch.com/download/1679

[¶] GlavNed reportedly pays a commission of 30 to 40% of drugs sold. http://www.networkworld.com/news/2009/071609-canadian-pharmacy-spam.html?hpg1=bn

Violations of Copyrights and Related Rights

Information technologies and the Internet facilitate the digital reproduction and dissemination of materials protected by copyrights and related rights. For example, with respect to software piracy on the Internet, losses have been estimated to amount to $53 billion for 2008 in direct lost revenues. This does not include the damage caused by unpatched pirate software that facilitates the spreading of malware.*

Measures against Cybercrime and Economic Crime

For many decades, measures to combat economic crime have been pursued. Since the late 1980s, the measures increasingly target crime proceeds.† During the 1990s, societies began to devise measures against the emerging threats of cybercrime at domestic and international levels. A milestone has been the adoption of the Council of Europe's Convention on Cybercrime opened for signature in Budapest in November 2001. Since then, a range of other measures by governments, international organizations, and the private sector have been implemented.

Nevertheless, measures targeting crime proceeds through financial investigations and the prevention and control of money laundering have been largely disconnected from measures against cybercrime. This is now changing. For example, the FATF has undertaken two studies, one on money laundering and terrorist financing vulnerabilities related to Internet payment systems in June 2008‡ and one on money laundering and terrorist financing through new payment methods in October 2010.§ In 2009, the Council of Europe decided to undertake a typology study on criminal money flows on

* http://portal.bsa.org/Internetreport2009/2009Internetpiracyreport.pdf

† Reflected in the 1988 United Convention on Illicit Traffic in Narcotic Drugs and Psychotropic Substances by the creation of the Financial Action Task Force in 1989, in the Council of Europe Convention on the Laundering, Search, Seizure and Confiscation of Proceeds from Crime of 1990, and in the Council of Europe Convention on the Laundering, Search, Seizure and Confiscation of Proceeds from Crime and the Financing of Terrorism (CETS 198) of 2005. http://www.unodc.org/unodc/en/treaties/illicit-trafficking.html; http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=141&CM=8&DF=&CL=ENG; http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236836_1_1_1_1_1,00.html; http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=198&CM=8&DF=&CL=ENG; http://www.coe.int/t/dghl/cooperation/economiccrime/SpecialFiles/FI_en.asp

‡ Financial Action Task Force. (2008). Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems. http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf

§ http://www.fatf-gafi.org/dataoecd/4/56/46705859.pdf

the Internet to examine risks, develop indicators and red flags, and identify possible countermeasures.*

The question of criminal money on the Internet was also on the agenda of the global Octopus Conference on cybercrime organized by the Council of Europe in March 2009.† Discussions and information available suggest that in addition to general preventive and public awareness, measures and good practices against cybercrime and economic crime and in particular targeting crime proceeds may comprise the following:

International Standards and Cooperation

A precondition for criminal justice action against cybercrime is that the conduct to be investigated, prosecuted, and adjudicated is defined as a criminal offence. Law enforcement authorities must have the legal power to search computer systems, preserve electronic evidence, and undertake other investigative measures. Because of the transnational nature of cybercrime and the volatility of electronic evidence, authorities must have international cooperation. This also means that substantive and procedural legislation among countries must be compatible and reciprocal. The Budapest Convention provides a solution by requiring states to:

- Criminalize attacks against computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices‡) and offenses committed by means of a computer system (including computer-related forgery and fraud§, child pornography¶, and infringements of copyright and related rights**).
- Enact legal procedural measures to enable its competent authorities to investigate cybercrime and secure volatile electronic evidence in an efficient manner (including expedited preservation of data, search and seizure of computer systems, and interception of communications).

* The study was carried out by the Council of Europe's anti-money laundering evaluation mechanism (MONEYVAL, www.coe.int/moneyval) in cooperation with the Global Project on Cybercrime and the joint European Union project on money laundering in the Russian Federation (MOLI-RU2). The author of this chapter also served as a lead author of the typology study. This explains similarities between parts of this chapter and sections of the typology study. Only information from publicly available sources has been used here.

† http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20interface%202009/Interface2009_en.asp

‡ Articles 2–6 of the Budapest Convention on Cybercrime of the Council of Europe (CETS 185).

§ Articles 7 and 8 of the Budapest Convention.

¶ Article 9 of the Budapest Convention.

** Article 10 of the Budapest Convention.

- Cooperate efficiently with other parties to the convention through general (extradition, mutual legal assistance) and specific provisions (expedited preservation of data, access to stored computer data, interception of traffic and content data, creation of 24/7 points of contact) to assure international cooperation.

Although developed by the Council of Europe, this treaty serves as a global standard, as noted earlier. In addition to most European countries, it has also been signed or ratified by Canada, Japan, South Africa, and the U.S. Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, and the Philippines have been invited to become parties and several other countries on all continents use the Budapest Convention as a guideline for reforming their cybercrime legislation.*

Similarly, with regard to financial investigations and measures against money laundering, countries are well advised to strengthen their legislation and take other measures in line with international standards such as the recommendations of the FATF† and the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and on the Financing of Terrorism ("Warsaw Convention").‡

Cybercrime Reporting

Public and private sector stakeholders, particularly criminal justice authorities, must have the necessary information to detect cybercrime and determine whether apparently minor fraud schemes are part of a major criminal operation. Reporting systems that provide such information are increasingly utilized. Examples are the Internet Crime Complaint Centre (IC3)§ in the U.S., MELANI¶ in Switzerland, and the National Fraud Reporting Centre** in the United Kingdom. In the European Union, an Internet Crime Reporting Online System (I-CROS) is being established at Europol. Signal Spam is a public–private partnership in France that allows Internet users to report spam messages that are recorded in a single database that is then used for criminal and administrative investigations. It also serves as a research on enhancing network security and email delivery.††

* See Council of Europe (2010).
† http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236920_1_1_1_1_1,00.html
‡ http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=198&CM=8&DF=&CL=ENG
§ http://www.ic3.gov/default.aspx
¶ http://www.melani.admin.ch
** http://www.actionfraud.org.uk/home
†† https://www.signal-spam.fr/

Risk Management in Financial Sector

General guidelines for financial sector organizations to manage risk related to money laundering have been available for some time.* Some organizations also designed measures to manage specific Internet-related risks such as the creation of centralized databases to correlate transactions, two-factor authentication, and monitoring for mule account activities. The payment card industry has established security standards for merchants, processors, and financial institutions† and risk management guides for merchants.‡ Commercial websites and Internet payment systems now often pursue proactive risk-based approaches including models for detecting unusual activity.§

Due Diligence of Registries and Registrars of Domains

The operation of botnets, the hosting of illegal content, and other cybercrimes is possible only because domain name registries and registrars fail to exercise due diligence when domains are registered.¶ For example, a registrant is not identified or information entered into the WHOIS database** is not accurate.†† Some services offer bullet-proof hosting, that is, they protect criminal activities and do not cooperate with law enforcement.‡‡

In 2009, law enforcement agents prepared a set of recommendations, "Law Enforcement Recommended Amendments to ICANN's Registrar Accreditation Agreement (RAA) and Due Diligence Recommendations."§§ The recommendations, among other issues, require ICANN¶¶ to perform due diligence investigations on all registrars and registries and ensure that they collect accurate and complete data from those registering domain names. In June 2010, the recommendations gained the support of the ICANN

* http://www.wolfsberg-principles.com/risk-based-approach.html

† For example, Payment Card Industry Data Security Standard (PCI DSS) and related requirements. https://www.pcisecuritystandards.org/security_standards/index.php

‡ http://usa.visa.com/download/merchants/visa_risk_management_guide_ecommerce.pdf

§ See Financial Action Task Force (2008).

¶ To better understand of registration, see report of Wolfgang Kleinwächter for Council of Europe Project on Cybercrime http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_wolfgangkleinwaechter1.pdf

** http://www.whois.net/

†† http://www.icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf

‡‡ Many bullet-proof domains are reportedly hosted in Eastern Europe and the Far East. For Europe, see report by Spamhouse on criminal 'Rock Phish' domains registered at Nic.at (http://www.spamhaus.org/organization/statement.lasso?ref=7) http://en.wikipedia.org/wiki/Bulletproof_hosting.

§§ http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Presentations/Ws%202/LEA_ICANN_Recom_oct2009.pdf

¶¶ Internet Corporation for Assigned Names and Numbers (www.icann.org)

Governmental Advisory Committee (GAC). The committee encouraged the ICANN board to address these recommendations.*

Specialized Units and Interagency Cooperation

Many countries have established financial intelligence units.† These central authorities receive, analyze, and disseminate information on money laundering and the financing of terrorism, and assist with asset recovery and financial investigation.

In recent years, governments have also begun to create specialized prosecution and high-tech crime police services responsible for investigating and prosecuting cybercrime. Obviously, the better cooperation of authorities responsible for fraud, economic crime, financial investigations, and money laundering with other agencies responsible for cybercrime, the better the chances of success against Internet fraud.

Public and Private Cooperation

Most vital information for combating economic crime on the Internet is held by private sector organizations (banking, payment card providers, online banking services and platforms, and money transmitters) and different types of Internet service providers, domain name registries and registrars, and a wide range of industries, research institutions, and initiatives against cybercrime.‡ Cooperation and information exchange between public and private sectors can therefore achieve major impact. Good practices include information sharing and analysis centers (ISACs) for the financial sector in the U.S.,§ the Netherlands,¶ and other countries. To strengthen cooperation among law enforcement authorities and Internet service providers, the

* http://gac.icann.org/system/files/Brussels-communique.pdf

† http://conventions.coe.int/Treaty/EN/Treaties/Html/198.htm

‡ Examples of initiatives focusing on fraud are: The Anti-Phishing Working Group (http://www.antiphishing.org/), a global pan-industrial and law enforcement association focused on eliminating fraud and identifying theft from phishing, pharming, and e-mail spoofing. The London Action Plan (http://www.antiphishing.org/) promotes international spam enforcement cooperation and addresses spam-related problems such as online fraud and deception, phishing, and dissemination of viruses. The participants also open the Action Plan for participation by other government and public agencies and appropriate private sector representatives as a way to expand the network engaged in spam enforcement cooperation. The Messaging Anti-abuse Working Group (http://www.maawg.org/ or (MAAWG) was formed to encourage the messaging industry to work collaboratively and successfully address messaging abuses such as spam, viruses, denial-of-service attacks, and other exploitations.

§ http://www.fsisac.com/

¶ http://www.samentegencybercrime.nl/

Council of Europe in 2008 developed guidelines for law enforcement and ISP cooperation in the investigation of cybercrime.*

Training

Today, and more so in the future, most criminal activities will involve information technologies and thus yield electronic evidence. Therefore, law enforcement officers, prosecutors, and judges must have at least basic knowledge of cybercrime and electronic evidence. Some may require more advanced training and a few should become highly specialized in certain aspects of cybercrime. In Europe, efforts have been undertaken for more several years to harmonize law enforcement training on cybercrime and computer forensics and are coordinated by the European Cybercrime Training and Education Group (ECTEG).†

Based on the assumption that specific measures are required to enable judges and prosecutors to process cybercrime correctly and make use of electronic evidence through training, networking and specialization, the Council of Europe in 2009 adopted a "concept for cybercrime training for judges and prosecutors" to incorporate such training in domestic training programs.‡

Efficient International Cooperation

Cybercrime is transnational as are the criminal money flows from economic crime on the Internet. The international standards such as the Budapest Convention, FATF recommendations, and Warsaw Convention allow countries to cooperate efficiently to preserve volatile evidence. However, countries have not yet fully exploited the opportunities offered by these agreements. For example, based on the experience of the G8 High-Tech Crime Subgroup, Article 35 of the Budapest Convention requires parties to this treaty to establish 24/7 points of contact:

> **Article 35: 24/7 Network**—(1) Each Party shall designate a point of contact available on a 24-hout, 7-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating,

* http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp
† http://www.ecteg.eu/
‡ http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/default_en.asp

or, if permitted by its domestic law and practice, directly carrying out the following measures: (a) Provision of technical advice; (b) Preservation of data pursuant to Articles 29 and 30; and (c) Collection of evidence, the provision of legal information, and locating of suspects.

(2) (a) A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis; (b) if the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

(3) Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Other important channels of cooperation include Interpol's I-24/7 global communication system and its National Central Reference Points (NRCP) network of designated investigators working in national computer crime units in more than 120 countries. However, many of the 24/7 contact points and NRCP are yet to become fully operational.* A number of other questions remain to be resolved:

- How can the private sector cooperate with law enforcement agencies of other countries?
- What role can networks such as the Egmont Group† of financial intelligence units or the CARIN‡ network of asset recovery agencies play in exchanging financial information related to cybercrime?
- As cloud computing allows increased storage of data and applications on servers in foreign jurisdictions or at unknown locations rather than on individual computer systems, how can law enforcement access and evidence preservation be ensured?§

* Regarding 24/7 contact points, see http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf

† http://www.egmontgroup.org/

‡ http://www.europol.europa.eu/publications/Camden_Assets_Recovery_Inter-Agency_Network/CARIN_Europol.pdf

§ http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf

Conclusions

The threat of cybercrime and other information security risks cannot be overstated in light of the worldwide reliance of societies on information and communication technologies . ICT and the Internet offer criminals unprecedented opportunities to organize and operate a global marketplace at low cost and low risk while criminal justice authorities are bound by agency, geographic, and public–private boundaries that hinder cooperation and must operate with limited skills and resources. Criminals will continue to exploit new technologies, seek vulnerabilities, and adjust to countermeasures. Cybercrime and the information society will continue to function within an ecosystem.

Currently, most cybercrime reported by law enforcement is economic—committed to generate economic benefits. A crucial element of any strategy against cybercrime should focus on the search, seizure, and confiscation of proceeds: following the money. Success can be achieved only by enhanced cooperation of anti-cybercrime, anti-money laundering, and financial investigation agencies, the financial sector, and ICT industries at all levels and across the globe.

International standards such as the Budapest Convention on Cybercrime, the recommendations of the Financial Action Task Force and the Council of Europe Convention on the Laundering, Search, Seizure and Confiscation of Proceeds from Crime and the Financing of Terrorism provide a common basis for joint action.

References

Brunst, P. & Sieber, U. (2010). Cybercrime legislation. In Basedow, J. & Sieber, U. (Eds). German National Reports to the 18th International Congress of Comparative Law, Washington.

Bundeskriminalamt (German Federal Criminal Police Office). (2010). FIU Jahresbericht 2009. Wiesbaden. http://www.bka.de/profil/zentralstellen/geldwaesche/pdf/fiu_jahresbericht_2009.pdf

Bundeskriminalamt (2010). IUK-Kriminalität. Bundeslagebild 2009. Wiesbaden. http://www.bka.de/lageberichte/iuk/bundeslagebild_iuk_2009.pdf

Castells, M. (2000). *The Rise of the Network Society*, 2nd ed. Oxford, Malden.

Commtouch Internet Threats Trend Report (Q1 2010). www.commtouch.com/download/1679

Council of Europe. (2002). Organised Crime Situation Report 2001. Committee PC-S-CO, Strasbourg. http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Report2001E.pdf

Council of Europe. (2003). Organised Crime Situation Report 2002. Committee PC-S-CO, Strasbourg. http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/PC-S-CO%20_2003_%207%20E%20OC-Report%202002-Provisional.pdf

Council of Europe. (2004). Organised Crime Situation Report 2004: Focus on the Threat of Cybercrime. Octopus Programme, Strasbourg. http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Organised%20Crime%20Situation%20Report%202004.pdf

Council of Europe. (2005). Organised Crime Situation Report: Focus on the Threat of Economic Crime. Octopus Programme, Strasbourg. http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Report2005E.pdf

Council of Europe. (2005). Convention on the Laundering, Search, Seizure, and Confiscation of Proceeds from Crime and the Financing of Terrorism (CETS 198). http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=198&CM=8&DF=05/12/2010&CL=ENG

Council of Europe. (2008). Guidelines for the cooperation between law enforcement and Internet service providers against cybercrime. Global Project on Cybercrime, Strasbourg. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp

Council of Europe. (2009). Functioning of 24/7 Points of Contact for Cybercrime. Global Project on Cybercrime, Strasbourg. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf

Council of Europe. (2010). Contribution of the Secretary General of the Council of Europe to Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Salvador, Brazil. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/SG%20Inf%20_2010_4%20-%20UN%20Crime%20congress_ENGLISH.pdf

Council of Europe. (2010). The Internet domain name registration process from the registrant to ICANN. Global Project on Cybercrime, Strasbourg. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_wolfgangkleinwaechter1.pdf

Council of Europe. (2010). Cybercrime training for judges and prosecutors. Global Project on Cybercrime, Strasbourg. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Training/default_en.asp

Council of Europe. (2010). Law enforcement challenges in transborder acquisition of electronic evidence from "Cloud Computing Providers". Global Project on Cybercrime, Strasbourg. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_joeschwerha1a.pdf

Council of Europe. (2010). Cloud computing and cybercrime investigations: territoriality versus power of disposal? Global Project on Cybercrime, Strasbourg. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf

Deutsche Gesellschaft für Technische Zusammenarbeit. (1998). Drugs and Development in Asia. http://www2.gtz.de/dokumente/bib/99-0026.pdf

Europol. (2007). High-tech Crimes within the EU: Old crimes new tools, new crimes new tools. Threat Assessment, The Hague. http://www.europol.europa.eu/publications/Serious_Crime_Overviews/HTCThreatAssessment2007.pdf

Financial Action Task Force. (2008). Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems. Paris. http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf

Financial Action Task Force. (2010). Money Laundering Using New Payment Methods. Paris. http://www.fatf-gafi.org/dataoecd/4/56/46705859.pdf

Financial Fraud Action UK. (2010). Fraud the facts: definitive overview of payment industry fraud and measures to prevent it. http://www.ukpayments.org.uk/files/fraud_the_facts_2010.pdf

Friedman, T.L. (2006). *The World is Flat*. London.

G Data. (2009). Whitepaper: Underground Economy. http://www.gdata-software.com/uploads/media/Whitepaper_Underground_Economy_8_2009_GB.pdf

Information Warfare Monitor/Shadowserver Foundation. (2010). Shadows in the Cloud: Investigating Cyber Espionage 2.0. http://www.nartv.org/mirror/shadows-in-the-cloud.pdf

Internet Crime Complaint Center. (2010). Internet Crime Report 2009. http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

Koops, B.J. & Leenes, R. (2006). Identity theft, identity fraud and/or identity-related crime. *Datenschutz und Datensicherheit,* 30, 9. http://www.fidis.net/fileadmin/fidis/publications/2006/DuD09_2006_553.pdf

M 86 Security. (2010). Whitepaper: Cybercriminals Target Online Banking Customers. http://www.m86security.com/documents/pdfs/security_labs/cybercriminals_target_online_banking.pdf

Microsoft Corporation. (2010). *Security Intelligence Report*, 9, Jan.–June. http://www.microsoft.com/security/sir/

OECD. (2007). Malicious Software (Malware): A Security Threat to the Internet Economy. http://www.oecd.org/dataoecd/53/34/40724457.pdf

Schmidt, H. (2006). *Patrolling Cyberspace*. North Potomac.

Seger, A. (2007). Identity theft and the convention on cybercrime. In Chryssikos, D. et al. (Eds.), *The Evolving Challenge of Identity-Related Crime: Addressing Fraud and the Criminal Misuse and Falsification of Identity*. UN ISPAC. http://www.ispac-italy.org/pubs/ISPAC%20-%20Identity%20Theft.pdf

Sophos. (2010) *Security Threat Report*, August. http://www.sophos.com/security/topic/security-report-2010.html