4. Organized Crime in Cyberspace

by Tatiana Tropina

Introduction

The growing importance of information and communication technologies in all facets of business and everyday life has dramatically changed our way of living. With its anonymity, ease of use, communication speed, and the possibility to share information across borders and reach a large audience, the Internet has become a key enabler both for legitimate users and for those who wish to exploit all the benefits of global information networks to commit crimes.

The problem of cybercrime is clearly evident and is now one of the biggest international concerns. However, while the number of crimes committed in cyberspace is constantly growing and criminal activities are becoming more sophisticated, the combination of a lack of reliable sources of information, the international character of cybercrime, and continually evolving tools used by cybercriminals makes it difficult to obtain an accurate picture of the "dark side" of the information networks. In this regard, one of the ongoing debates is whether cybercriminality can be attributed to organized criminal groups. Though there are some clear indications that organized crime groups are getting increasingly involved in cybercrime (Commission of the European Committees 2007, 1), it is still not clear to what extent online crime is organized (BAE Systems Detica 2012, 1). Do organized crime groups use the Internet to facilitate crimes in the same way that they use any technologies, such as mobile phones or, earlier, the telegraph? Or does cyberspace create a new form of organized crime with new types of structures and interactions between members as well as new business models and criminal supply chains? Does the international community face a new and evolving form of criminality in global information networks?

This article examines the issue of the possible transformation of cybercrime into a global, fast-expanding, profit-driven illegal industry with a new form of organized criminal groups thriving behind it. Firstly, the paper provides some insights into the debate around cyberspace being either a medium for traditional

* Tatiana Tropina works at the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany.

organized crime or a perfect environment for the creation of a new form of organized crime. Then it analyzes the structure of the online criminal groups and defines the business models used by those operating in the underground economy in cyberspace. Finally, the article identifies the possible future trends of organized crime in cyberspace and the problems of tackling this phenomenon.

1. Organized crime and cyberspace: A new medium or a new form?

It is already evident that the current era of cybercrime is no longer dominated by young "computer geeks" committing attacks and stealing data just for fun as demonstrations of their technical skills or for peer recognition (BAE Systems Detica 2012, 5; POST 2006, 2). The development of the digital economy and the increasing dependence of many financial services on the information networks has changed dramatically both the criminal landscape and the motivation of offenders. High rewards combined with low risks have made digital networks an attractive environment for various types of profit-driven criminals, who, according to some research, might shape the new form of organized criminal networks (Ben-Itzhak 2008; BAE Systems Detica 2012; Rush et al. 2009; KPMG 2011, 5; Council of Europe 2004).

There is an ongoing discussion about how organized crime groups can – and already – use global information networks. The main assumption that initiated this discussion was that, in the non-digital era, organized crime sought "safe havens" offered by countries with weak governments and unstable political regimes (Williams 2002, 2). With the possibility to commit cybercrimes across national borders and without needing to be physically present at the crime scene, organized crime groups can benefit from national jurisdictions that do not have proper legal frameworks nor the technical capabilities to fight cybercrime (Williams 2002, 2; Rush 2009, 3; Goodman 2010).

Though it is obvious that traditional organized crime and terrorist groups can gain significant advantages from the use of information and communications technologies (ICTs) (Shelley 2003, 307; Williams 2002, 2) and "safe haven" jurisdictions, the discussion revolves around the question of whether cybercrime can be ascribed to organized crime. This debate is characterized by McCusker (McCusker 2006, 257) as a tension between logic and pragmatism, where logic postulates that traditional organized crime will engage in criminal activities in cyberspace as they would in any low-risk and high-reward illegal business in the physical world; pragmatism, in turn, questions the necessity for traditional organized crime to step into this area and its capacity to secure a return on investment and to produce the desired financial benefits.

A decade ago Williams (2002, 1) suggested that although there was growing evidence that organized crime groups use the Internet, organized crime and cybercrime would never be synonymous because organized crime will continue to operate offline, and most of the cybercrimes will be committed by individuals

rather than criminal organizations. Brenner (2002, 25) highlighted the same fact of not having an indication that online crime was reaching the gang level of organization. During the past 10 years, the criminal landscape has changed dramatically, but there is still no clear concept of the synergy between organized crime and cyberspace. Analytical reports now produced by security companies reveal the professionalization and sophistication of cyber attacks and financial crimes committed in global networks, suggesting that cybercrime represents a new type of organized crime with different, constantly evolving structures, and new ways of using hi-tech tools to attain criminal goals. The scholarship research in this field is somewhat confusing because of the existing concept of transnational organized crime. It is very hard to fit cybercrime, even when committed in the traditionally organized way, into this concept.

To avoid confusion in the debate on organized crime in cyberspace, it is perhaps necessary to make a distinction between the migration of traditional organized crime to the virtual world (as well as the synergy between traditional organized crime and online crime) and the organized groups focused on committing cybercrimes.

Cyberspace has already become a tool for facilitating all types of offline organized criminality, including child abuse, illicit drug trafficking, trafficking in human beings for sexual exploitation, illegal migration, different types of fraud, counterfeiting, and the firearms trade. It provides anonymity in communication; greater possibilities for advertisement and product placement as well as money laundering via online gambling; and allows for trade in virtual currencies and virtual precious metals (Europol 2011, 5; Goodman 2010, 313). However, some studies suggest that we are entering the new era of organized crime, where the exploitation of cyberspace by traditional organized crime groups coexists with a new phenomenon, namely, organized structures operating solely in global information networks (BAE Systems Detica 2012, 2; Ben-Itzhak 2008).

It should be noted that the two afore-mentioned tendencies – organized criminality moving into cyberspace and the emergence of a new form of organized crime – are not mutually exclusive. Rather, they complement each other, giving rise to the synergy between traditional organized crime and criminal structures operating online. However, while the first phenomenon – namely, the use of cyberspace by traditional crime to facilitate its activities – has already been widely discussed in the academic literature, there is a lack of research concerning this new form of organized crime online. This article concentrates more on the latter, providing analysis of the structures of the new online groups and the models of their operation.

2. Underground economy in cyberspace: Model of operations

Recent studies of organized crime in the hi-tech era point out that, with the convergence of offline and online worlds, the information society has arrived at a point where new digital crime is being organized, though it has not yet been consolidated (BAE Systems Detica 2012, 2; Symantec 2008). The new groups operating in cyberspace enjoy more rewarding and less risky operations and represent newer types of criminal networks that operate only in the area of e-crime.

Illegal activities online, such as credit card fraud, trading compromised users' accounts, selling banking credentials and other sensitive information, have given rise to the increasingly sophisticated and self-sufficient digital underground economy (Europol 2011, 4). Specific Internet forums and communications channels are used as underground marketplaces for the trading of illegal goods and services (Fallmann et al. 2010, 1). Any data traded on these shadow platforms has its own monetary value.[1] This value represents an illicit commodity, intangible and easily transferrable across borders. It drives the development of illegal markets: Specific criminal activities have been developed and are being constantly improved to steal sensitive information (e.g., phishing, pharming, malware, tools to attack commercial databases). Online criminality includes a broad spectrum of economic activity, whereby various offenders specialize in developing specific goods (exploits, botnets) and services such as malicious code-writing, crimeware distribution, lease of networks for carrying out automated attacks or money laundering (Cárdenas et al. 2009, 1; Europol 2010, 4).

Criminals in global information networks borrow and copy business models from legitimate corporations. Cybercrime business models were similar to those of high-technology companies in the early 1990s, when digital criminality was still in its infancy. Since the early 2000s, cybercriminals have developed patterns imitating the operations of companies such as eBay, Yahoo, Google, and Amazon (Kshetri 2010, 190). One factor indicating the current maturation of the cybercrime industry is the degree of professionalization of the IT attacks, for example fraudulent activities such as classic phishing, which is becoming the greatest identity-theft threat posed to professional businesses and consumers (BSI 2011, 4). Another factor is the increasing specialization of perpetrators (BKA 2010), which means that cybercrime involves a division of labor. Other factors include the so-

1 | For example, according to Symantec (2008, 12), the advertized prices for bank account credentials ranged from $10 to $1,000, with prices depending on the amount of funds available, the location, and the type of account (corporate accounts might cost more than double the price of personal bank accounts; EU accounts are advertised at a considerably higher cost than their US counterparts).

phistication, commercialization, and integration of cybercrime[2] (Grabosky 2007, 156).

Technological developments, research, innovation, and the transformation of value chains into value networks has driven the globalization of the legal sector and has affected the organizations, making them more decentralized and collaborative, with regard to external partners. In the same way, innovation has fueled the creation of new patterns in criminal ecosystems, with regard to product placement, subcontracting, and networking (Rush et al. 2009, 37). Cybercriminals employ schemes similar to the legitimate B2B (business-to-business) models for their operations, such as the highly sophisticated C2C (criminal-to-criminal) models, which make very effective crime tools available through digital networks (Ben-Itzhak 2008, 38). Computer systems' vulnerabilities and software are exploited to create crimeware: "malware specially developed with the intention of making a profit and which can cause harm to the user's financial well-being or valuable information" (ESET 2010a, 4). These crimeware tools such as viruses, Trojans, and keyloggers offer criminal groups the flexibility of controlling, stealing, and trading data.

It is argued, though, that there is a difference between cybercrime business models and legitimate business in terms of core competencies and important sources: While the latter is aimed at creating the most value for customers, cybercrime involves defrauding prospective victims and minimizing the risk of having illegal operations uncovered (Kshetri 2010, 189). However, if one considers cybercrime as a model establishing a relation between the supplier of illegal tools and services and the customer who uses these tools to commit the crime against the victim, this difference does not have much significance: Cybercrime business models are focused on providing the most value for the "consumers," who are not the victims of crimes but of the criminals using the tools.

Automation plays a significant role in the development of C2C models. Automation tools use technology to avoid the operational requirement for physical groupings and force of numbers (Europol 2011, 6). In this regard, botnets – networks of compromised computers running programs under external control – were one of the main factors in transforming some types of cybercrimes, such as phishing, into a worldwide underground ecosystem, run, supposedly, by organized groups (Barroso 2007, 7). With a botnet, cybercriminals can make use of many computers at the same time to automate attacks on private and corporate systems, distribute spam, host phishing websites, disseminate crimeware, launch denial of service attacks, and scan for system vulnerabilities: Without one, they must target victims and machines manually and individually (Europol 2011, 6).

2 | Offenses subsequently lead to other offenses, for example, attacks result in information theft, and then stolen information can be sold and used by those who bought it to commit fraud.

The estimated financial gains of crime groups using botnets range from tens of thousands to tens of millions of dollars. The trading of botnets has also become a high-revenue C2C activity. Criminal organizations offer botnets for relatively low costs, profiting from the turnover based on the number of "customers." For example, a server with stored malware, exploit kits, or botnet components costs anywhere from $80 to $200 a month; the botnet administration pack, known as the Eleonore Exploit Pack, has a value of $1,000; hiring a botnet of between 10 and 20 computers, if administered using the pack mentioned above, costs an average of $40 a day; Zeus kit v1.3 costs $3,000 to $4,000 (ESET 2010b, 7). These costs are relatively low compared to the criminals' financial gains. But the damage to individual consumers and businesses, as well as to the financial health, reputations, and trust in online transactions as a whole is extremely high.

Crimeware is also used to deploy Crime-as-a-Service business models that represent the system of trading and delivering crimeware tools. Data-supplying models are also used to share the tools to commit cybercrimes. For instance, by creating "customer" systems where instruments are available on demand, "users" just log into the server and choose from the range of tools suitable for fraud, phishing, and data-stealing and then download them. When user data is stolen, criminals can use crimeware servers to commit organized attacks. Crimeware servers allow for controlling compromised computers and managing the stolen data (Ben-Itzhak 2008, 38).

Monetization of the intangible commodity – data – nowadays seems to be the main "bottleneck" for cybercrime groups. One major problem with any type of cash-out operation involving money mules is that there are not enough of them in service. Mules typically work only for a very short time before they are either abandoned by their handler or are captured by law enforcement. The ratio of stolen account credentials to available mule capacity could be as high as 10,000 to 1 (Cisco 2011, 9). Money mules are typically recruited via employment search websites and social networking sites. Their goal is to "cash in" stolen personal and financial information, very often in different jurisdictions than those in which the crimes have been committed. The mules are the visible "face" of the organized cybercrime since they are particular individuals turning the data into money (Europol 2011). Often the money is put into their personal accounts before they transfer it (Kshetri 2010, 177). As the cybercrime economy continues to expand, it will be increasingly challenging for scammers to maintain an adequate supply of these temporary "employees" to profit fully from their illegal activities. Many sophisticated techniques have already been developed to hire the mules, including masking the supposed illegal activities as legitimate services, such as help in a job search (Cisco 2011, 9), and these techniques very likely are going to continue evolving.

3. Organized crime in cyberspace: Changing structure

Since cybercrime has moved away from individual, fragmented activities to the models that are mimicking modern corporate business (Rush et al. 2009, 42), it is inevitable that it has changed the structure on the operational side. The most common view on the structure of organized criminal groups is that they are formed by high-skilled, multi-faceted virtual criminals (UK Home Office 2010, 12). This is in contrast to traditional organized crime groups, which are ethnically homogeneous, formally and hierarchically structured, multi-functional, bureaucratic criminal organizations (Council of Europe 2004, 2). These networks mark "the cleanest break to date from the traditional concept of Organized Crime groups as hierarchical" (Europol 2011, 5).

In fact, the Internet represents the platform where new and old forms of organized groups can coexist without disturbing each other because of the very specific characteristics of Internet crime. It is known that traditional organized crime groups violently maintain a monopoly over their assets and territory to control certain scarce or illegal commodities on the black market (Rush et al. 2009, 35). With stolen, intangible data, which represents a commodity for the shadow digital economy (Europol 2011, 5), cybercriminals do not require control over a geographical territory; need fewer personal contacts and less enforcement of discipline between criminals; and, in the end, there is less necessity for a formal organization. Moreover, the classic hierarchical structures of organized crime groups may even be unsuitable for organized cybercrime (Council of Europe 2004, 7). This new type of organized crime in information networks is non-competitive and allows collaboration across criminal networks (UK Home Office 2010, 13). Another major difference between traditional organized crime groups and cybercrime groups is, again, the automation technique. In other words, the power of the group is in the strength and sophistication of its software, not in the number of individuals (Brenner 2002, 27; Choo and Smith 2007, 41).

Criminal groups operating in cyberspace are believed to be more flexible as compared to traditional organized crime groups, allowing for the incorporation of members for limited periods of time due to their flexibility (United Nations 2010, 10). These networks are structured on a "stand alone" basis, as members of the groups are often not supposed to meet (Choo 2008, 7) – or, very rarely, meet in person – thereby relying solely on electronic communications and sometimes not even having virtual contact with other colleagues. Supposedly, the majority of them function using a number of web-based forums devoted to online fraud (Symantec 2008, 5; Rush 2009) or Internet Relay Chats (Fallmann et al. 2010, 1), channels where members know each other only by their nicknames.

The higher the degree of sophistication of these networks, the more cautious its operators are about potential members to ensure that only trusted people get access to the illegal goods and services traded on the underground markets (UK Home Office 2010, 12). This complex structure – together with access to the core

operations granted only to trusted associates – prevents organized cybercrime groups from being detected and infiltrated by law enforcement agencies. In this regard, though, both web forums and IRC channels are operated by administrators and serve the same goal, forums seem to be more advanced ways of organizing criminal activity online, because web forums have a peer-review process that every potential vendor needs to go through before status is granted. In contrast, virtually anyone can use IRCs for advertisement, which makes them more accessible to law enforcement agents or unreliable criminals. As a solution, IRCs offer services to check the validity of the data offered for sale (Rush et al. 2009, 50).

Online forums serve as a vital introduction and recruitment medium for the digital shadow economy, since they facilitate cooperation within and between the groups and exhibit a certain degree of organization at the administrative level, enabling offenders to get together to work on specific projects. At the same time, online marketplaces represent the platform for advertising, learning, and information-sharing (Europol 2011, 5).

Speculation and debate as to the professionalism and organization of criminal groups online are fueled by the nature of such forums, because they can be considered more as tools for collaboration between individuals loosely connected to each other than as platforms for highly organized groups (Symantec 2008, 5). Nevertheless, it is obvious that there is a certain level of organization occurring on these platforms, at least on the administrative level.

It should be noted that recent research argue that there is an incorrect assumption that organized crime in global networks relates only to distributed non-hierarchical "networks" with no links to traditional organized crime families, which are assumed to be lacking technical capacity and relying on physical and geographical proximity as well as violence; rather, there is a movement toward long-term organized crime activities online (BAE Systems Detica 2012, 6). Symantec states that there is significant evidence that organized crime is involved in many cases involving the online underground economy (Symantec 2008, 5).

The main problem of assessing the structure of cybercrime groups and their level of organization is that there is much more information about what they are doing – or can possible do – than about *who* is behind those groups (Rush 2009, 49). Moreover, a single individual or group of perpetrators can play separate or simultaneous roles (developers of malware, buyers, sellers, enablers, administrators) in the cybercrime economy, which makes the structure of the illegal market "complex and intertwined" (Trend Micro 2006, 6).

In addition to the discussion within the framework of the analysis of supposed cybercrime structures, there are also controversies in assessing the possible social and demographic characteristics of the members of these groups. On the one hand, according to Europol, the demographic profile of members of online crime groups is very different to what is traditionally associated with transnational organized crime: More than 60 percent of hackers are under the age of 25 (Europol 2011, 6). On the other hand, some studies, such as the BAE Systems Detica re-

port, challenge the assumption of digital criminal organizations being related to their network types, trans-jurisdictional natures, and the type of member, who is normally perceived to be a young, technically literate individual (BAE Systems Detica 2012, 6). In contrast, the results of the research show that there are more organized digital crime group members over 35 years of age (43%) than under 25 years of age (29%). This might be explained by increased levels of computer literacy and the availability of different tools to commit crimes, which can be easily distributed or purchased online without special, high-level skills (BAE Systems Detica 2012, 5).

As to the size of the networks, the estimates vary from 10 to several thousand members, when the affiliated networks are incorporated into the structure. Regardless of the number of members and affiliates, virtual criminal networks are usually run by a small number of experienced online criminals who do not commit crimes themselves, but act rather as entrepreneurs (UK Home Office 2010, 12). The criminal structures collaborate in teams where the roles are defined and the labor is divided (Rush et al. 2009, 42). For instance, the first group writes malicious code, such as the "Trojan"; the next group is responsible for the distribution and use of malicious software on the Internet; while another group collects data from the illegal platforms and prepares everything for the identity theft. This data may then be used by other groups of offenders (BSI 2011, 4). The leading members of the networks divide the different segments of responsibility (spamming, controlling compromised machines, trading data) among themselves. Some "elite" criminal groups act as closed organizations and do not participate in online forums because they have enough resources to create and maintain the value chains for the whole cycle of cyber-offenses, and therefore have no need to outsource or to be active in other groups.

4. Addressing the problem

Fighting cybercrime has always been a complex task due to the number of ICT network users, the transnational nature of the Internet, and its decentralized architecture (Gercke 2011). Organized criminal groups in cyberspace, both traditional ones and those operating solely online, remain – and probably will continue to remain – several steps ahead of legislators and law enforcement agencies. C2C networks are very likely to continue benefiting from anonymous communications, automation of attacks, and the difficulties that law enforcement agencies experience in determining locations: Servers with crimeware could be in one country, while members of the network could be in another one targeting victims across the world.

In addition to strengthening the current legal frameworks, updating old legislation, and harmonizing laws on an international level, what is needed is also cross-sector cooperation on the national level as well as international cooperation in detecting, investigating, and preventing e-crimes committed by organized

criminal groups (Europol 2011). The development of a comprehensive understanding and a forward-looking approach are required, since organized cybercrime seems to be a moving target.

International collaboration between states is the key, since the problem has a trans-border nature. Some states just do not have the necessary tools to respond to the activities of the organized cybercriminals, or they may lack the technical skills or face legal drawbacks (Goodman 2010). The development of a common understanding that no country can be safe alone in the global ICT network is very important. The problem of the legal harmonization can be solved only on the global level (Sieber 2008).

With the absence of a global strategy to counter organized cybercrime, the problem is very likely to deepen in the foreseeable future. With the development of ICT networks and the opportunities they offer, organized criminal groups will benefit from the entire range of tools and models available to legitimate economy sectors. The information's availability makes it easier for organized groups to foster and automate their fraud-committing activities. It will also probably tie more opportunistic criminals to existing criminal networks.

Cybercrime might be going through a transformation into an organized illegal industry, where syndicates are highly sophisticated and very hard to identify. Soon, some cybercrime industries may be run solely by organized criminal groups that are constantly seeking the newest technical solutions and the creation of new markets. As a result, it is likely that the cybercrime ecosystem will soon be dominated by criminal organizations, as cybercrime networks that have already become international will multiply the opportunities and reach to a global scale by exploiting the weaknesses of legal frameworks while searching for safe havens in countries with fewer resources to detect and fight them. This will make fighting cybercrime an even more difficult task for law enforcement agencies.

Conclusion

Though it is still not clear how organized networks in cyberspace are structured and how they operate, it is evident that this new form of organized groups is emerging in cyberspace, although it is not yet consolidated but dangerous nonetheless. As markets and trading itself have always attracted organized criminal groups seeking benefits from illegal activities, the growth of digital operations and services in legitimate markets are key enablers for organized cybercriminals, both for committing traditional crimes and for developing new types of illegal activities. Using business models that have proved their effectiveness in the legal business sector, organized cybercrime groups deploy highly sophisticated tools for online criminal activities. The risks to individuals, businesses, and governments grow with the further digitalization of the economy. E-criminal activities are conducted as long-term sustainable operations. Due to the borderless nature of the Internet, the problem of organized cybercrime has truly global consequences

when a country can only ensure safety within its borders. The way to address the problem is to develop long-term responses that would include coordination and harmonization of efforts on both the national and international levels.

Glossary

Botnet – a network of Internet-connected computers whose security defenses have been breached and control ceded to an unknown party. Their owners are unaware that computers have been set up to forward transmissions, which also include malicious programs or spam, to other devices over the Internet. Each compromised devices is also known as a "bot" (short for "robot"), or "zombie." The controller of the botnet is able to direct the activities of these compromised computers and perform automated attacks that include large numbers of bots.
Crimeware – malware specially developed with the intention of making a profit and which can cause harm to the user's financial well-being or valuable information.
Denial of service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) – an attempt to make a machine or network resource (website or service) unavailable to its intended users. By targeting a computer and its network connection, or the computers and network of the sites people are trying to use, an attacker may be able to prevent users from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer. The most common type of DoS attack occurs when an attacker "floods" a network with information and requests to view the website or to access the services. The server can only process a certain number of requests at once. Thus, an attacker overloads the server with illegally generated requests and the server cannot process requests from legitimate users.
Exploit (from the verb "to exploit", in the meaning of using something to one's own advantage) – a piece software, or data, or sequence of commands that takes advantage of computer security vulnerabilities in order to cause unintended or unanticipated behavior to occur on computer software or hardware. This frequently includes such things as gaining control of a computer system, or allowing illegal access to data, or launching denial of service attacks.
Internet Relay Chat (IRC) – a protocol for real-time Internet messaging (chat) and conferencing, mainly designed for group communications in discussion forums, called channels. However, one-to-one communication is also possible via private message and chat.
Keylogger – software that tracks the keys struck on a computer keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.
Malicious code – any code in any part of a software system or script that is used to cause undesired effects, security breaches, or damage to a system.

Malware – an abbreviated term for malicious software. It is software used, or created, to disrupt computer operations, gather sensitive information, or gain access to private computer systems. This term is used to refer to a variety of forms of hostile, intrusive, or annoying software.
Money mule – regarding cybercrime, this term is used to describe a person who electronically transfers stolen money.
Pharming – is an attack that redirects a website's traffic to another, bogus site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a software vulnerability. Malicious code is installed on a personal computer or server, misdirecting users to fraudulent websites without their knowledge or consent.
Phishing – a criminal activity using variations of social engineering techniques, typically carried out using email or an instant message, or phone contact. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by posturing as a trustworthy person or business in an electronic communication. Communications purporting to be from popular social websites, auction sites, online payment processors, or IT administrators are commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware.
System vulnerability – a weakness that allows a criminal to reduce a computer system's information assurance.
Trojan – a type of malicious software that masquerades as a legitimate file or helpful program with the ultimate purpose of granting cybercriminals unauthorized access to a computer. Trojans do not attempt to inject themselves into other files, like computer viruses do. Trojans may copy themselves, steal information, or harm their host computer systems.
Virtual currencies – currencies that are used to purchase virtual goods within a variety of online communities (social networks, online games, virtual worlds). Some virtual currencies can be exchanged to real currencies, like, for example, Linden Dollar, the currency of the virtual world "Second Life."
Virtual precious metals – relatively new way of transferring value online, enables users to secure cash deposits against precious metals held offshore.

References

BAE Systems Detica. 2012. Organised crime in the digital age: The real picture. Executive Summary. Available at: http://www.baesystemsdetica.com/uploads/resources/ORGANISED_CRIME_IN_THE_DIGITAL_AGE_EXECUTIVE_SUMMARY_FINAL_MARCH_2012.pdf.

Barroso, D. 2007. Botnets – The silent threat. ENISA Position Paper No. 3. Available at: http://www.dihe.de/docs/docs/enisa_pp_botnets.pdf.

Ben-Itzhak, Y. 2008. Organized cybercrime. *ISSA Journal* (October). Available at: https://dev.issa.org/Library/Journals/2008/October/Ben-Itzhak-Organized%20Cybercrime.pdf.

BKA (Bundeskriminalamt). 2010. Cybercrime. Bundeslagebild 2010. Available at: http://www.bka.de/nn_193360/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true.

Brenner, S. 2002. Organized cybercrime? How cyberspace may affect the structure of criminal relationships. *North Carolina Journal of Law & Technology* 4(1) (Fall).

BSI (Bundesamt für Sicherheit in der Informationstechnik). 2011. Available at: https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011.pdf?__blob=publicationFile.

Cárdenas, A., et al. 2009. An economic map of cybercrime. The 37th Research Conference on Communication, Information and Internet Policy (TPRC). Arlington, VA: George Mason University Law School. September.

Choo, K. 2008. Organised crime groups in cyberspace: A typology. *Trends Organ Crim* 11: 270–295.

Choo, K., and R. Smith. 2007. Criminal exploitation of online systems by organised crime groups. *Asian Criminology* 3: 37–59.

Cisco. 2011. Cisco 2010 annual security report. Highlighting global security threats and trends. Available at: http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf.

Commission of the European Committees. 2007. Towards a general policy on the fight against cyber crime. COM(2007) 267 final. Brussels. May 22.

Council of Europe. 2004. Summary of the organised crime situation. Report 2004: Focus on threat of cybercrime. Council of Europe Octopus Programme. Strasbourg, September 6. Available at: http://www.coe.int/.

ESET. 2010a. Cybercrime coming of age white paper. January. Available at: http://go.eset.com/us/resources/white-papers/EsetWP-CybercrimeComesOfAge.pdf.

———. 2010b. Trends for 2011: Botnets and dynamic malware. By ESET Latin America's Lab. November 22. Available at: http://go.eset.com/us/resources/white-papers/Trends-for-2011.pdf.

Europol. 2011. Threat assessment (abridged). Internet facilitated organised crime. iOCTA. File No.: 2530–264. The Hague. January 7. Available at: https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf.

Fallmann, H., G. Wondracek, and C. Platzer. 2010. Covertly probing underground economy marketplaces. Vienna University of Technology Secure Systems Lab. Available at: http://www.iseclab.org/papers/dimva2010_underground.pdf.

Gercke, M. 2011. Understanding cybercrime: A guide for developing countries. ITU, Geneva.

Goodman, M. 2010. International dimensions of cybercrime. In: Cybercrimes: A multidisciplinary analysis, ed. S. Ghosh and E. Turrini. Berlin and Heidelberg: Springer-Verlag.

Grabosky, P. 2007. The Internet, technology, and organized crime. *Asian Criminology* 2: 145–161.

KPMG. 2011. Cyber crime – A growing challenge for governments. Issues monitor. Vol. 8, 3. July.

Kshetri, N. 2010. The global cybercrime industry. Berlin and Heidelberg: Springer-Verlag.

McCusker, R. 2006. Transnational organised crime: Distinguishing threat from reality. *Crime Law and Social Change* 46, 257–273.

POST (Parliamentary Office of Science and Technology). 2006. Postnote – Computer crime. Number 271. October. Available at: http://www.parliament.uk/parliamentary_offices/post/pubs2006.cfm.

Rush, H. et al. 2009. Crime online. Cybercrime and iilegal innovation. NESTA research report. July. Available at: http://www.eprints.brighton.ac.uk/5800/01/Crime_Online.pdf.

Shelley, L. 2003. Organized crime, terrorism and cybercrime. In Security Sector Reform: Institutions, Society and Good Governance, ed. Bryden and Fluri. Baden-Baden: Nomos Verlagsgesellschaft, 303–312.

Sieber, U. 2008. Mastering complexity in the global cyberspace: The harmonization of computer-related criminal law. In: Les chemins de l'Harmonisation Pénale/Harmonising Criminal Law, ed. M. Delmas-Marty, M. Pieth, and U. Sieber. Collection de L'UMR de Droit Comparé de Paris. Bd. 15. Paris: Société de législation comparée, 127–202.

Symantec. 2008. Symantec report on the underground economy: July 7–8. November. Available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf.

Trend Micro. 2006. Phishing. A trend micro white paper. November. Available at: http://www.antiphishing.org/sponsors_technical_papers/trendMicro_Phishing.pdf.

———. 2010. The business of cybercrime. A complex business model. Focus Report Series. January. Available at: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_business-of-cybercrime.pdf.

UK Home Office. 2010. Cybercrime strategy. Stationery office limited on behalf of the controller of Her Majesty's Stationery Office.

United Nations. 2010. Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime. Working Paper prepared by the Secretariat. Twelfth United Nations Congress on Crime Prevention and Criminal Justice. V.10-50382 (E) 100210 110210. Salvador, Brazil. April 12–19.

Williams, P. 2002. Organized crime and cyber-crime: Implications for business. Available at: http://www.cert.org/archive/pdf/cybercrime-business.pdf.