The Evolving Structure of Online Criminality

How Cybercrime Is Getting Organised

Tatiana Tropina

eucrim
European Law Forum: Prevention • Investigation • Prosecution

AUTHOR

Tatiana Tropina

CITE THIS ARTICLE

Tropina, T. (2012). The Evolving Structure of Online Criminality : How Cybercrime Is Getting Organised. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2012-022

Published in eucrim 2012, Vol. 7(4) pp 158 – 165

https://eucrim.eu

ISSN:

Increasing dependency of the society on the information technologies raises concerns over vulnerabilities in cyberspace and the "dark side" of the information networks. The growth of digital operations in legitimate markets is one of the vital factors for the economic development. However, as markets and trading themselves have always attracted criminals seeking benefits from illegal activities, digital networks become a key enabler for the growth of cybercrime, both with regard to committing traditional crimes in the Internet and to developing new types of computer misuse.

Cybercrime has been evolving in line with how society uses digital networks, reacting to every development in the legal sector with the new approaches to committing offences. In the last decade, it has gone through the process of transformation from fragmented acts committed by individuals to increasingly sophisticated and highly professionalised activity. Moreover, cybercrime is believed to be on the stage of evolution into the fast expanding illegal industry where criminal activities are conducted by professional networks as long-term sustainable operations. Due to the newness of the phenomenon, there is still lack of research on how these networks in cyberspace are structured and how they operate. However, it is currently being discussed that we are witnessing the emergence of a new form of organised crime groups operating solely in cyberspace: groups which are not yet consolidated but dangerous nonetheless.

This article seeks to contribute the current research on this problem by examining the question of the possible transformation of cybercrime into a global, fast-expanding, profit-driven illegal industry with a new form of organised criminal groups thriving behind it. Firstly, the paper puts the issue of the increasingly organised on-line criminality into the context of general debate about organised crime in cyberspace. Secondly, it analyses the business models of underground economy of cybercrime. The third part of the paper focuses on the structure of the online criminal groups and their way of functioning. The paper concludes with indicating the legal problems of tackling organised cybercrime.

I. "Organised Crime" in Cyberspace or "Organised Cybercrime"? Two Sides of the Problem.

In the early days of cybercrime, the scene was mainly dominated by young hackers illegally accessing computer systems and breaking security measures just for fun or for demonstrating their technical skills.[1] With the development of digital economy both the criminal landscape and the motivation of offenders have changed dramatically. High rewards combined with low risks have made digital networks an attractive environment for various types of profit-driven criminals thriving on cybercrime.

The ongoing debate about the use of global information networks by organised crime groups revolves around two issues: cyberspace as a *new medium* for traditional organised crime groups and cyberspace as enabler for the *new form* of organised crime. On the one hand, it is believed that cyberspace can be used by traditional organised crime groups to carry out their operations.[2] On the other hand, it is argued that on-line criminals are nowadays shaping the new type of organised criminal networks.[3]

The problem of cyberspace as a *new medium* is related to the possibility of traditional organised crime groups to use digital network for their illegal activity. The basic ground for this discussion is the general assumption that traditional organised crime always seeks for "safe havens" offered by countries with weak governments and unstable political regimes.[4] Cyberspace with its anonymity, absence of borders and the opportunity to commit offences without being physically present at the crime scene constitutes a perfect environment, especially when criminals can operate from countries that do not have proper legal frameworks and technical capabilities to fight cybercrime.[5] While it is obvious that traditional organised crime groups can benefit significantly from the use of information and communications technologies,[6] it is still not clear to

https://doi.org/10.30709/eucrim-2012-022

what extend cybercrime can be attributed to the traditional organised crime groups. McCusker[7] argues that this debate represents as a tension between logic and pragmatism, where logic postulates that traditional organised crime will engage in criminal activities in digital environment as they would in any low-risk and high-reward illegal business in the physical world; pragmatism, in turn, questions the necessity for traditional organised crime to step into this area and its capability to secure a return on investment and to produce the desired economic benefits.

A decade ago Williams[8] argued that despite the growing evidence that traditional organised crime groups use the digital networks, organised crime and cybercrime would never be synonymous because the former would be operating offline and most of the cybercrimes will be committed by individuals rather than organised structures. Brenner[9] also pointed out that there was indication that online crime was reaching the gang level of organization. Though the landscape of cybercrime has changed a lot since then, there is still no clear concept of the synergy between organised crime and cyberspace. Moreover, it is very hard to fit cybercrime into traditional concept of organised crime with its hierarchical homogenous structures.

To avoid confusion in the debate on organised crime in digital world, it is necessary to distinguish two different phenomena, namely, migration of traditional organised crime in cyberspace and organised groups focused on committing cybercrimes. The former is evident: Internet has already become a tool for facilitating all types of offline organised criminality, including child abuse, illicit drugs trafficking, trafficking in human beings for sexual exploitation, illegal migration, different types of fraud, and counterfeiting. It provides anonymity in communication; greater possibilities for advertisement and product placement as well as new money laundering schemes.[10] However, some studies suggest that in the current era of organised crime exploitation of cyberspace by traditional organised crime groups coexists with organised structures operating solely in global information networks and committing only cybercrimes[11] and, thus, we are witnessing the evolution of a *new form* of the organised crime. Recent reports produced by security companies highlight the professionalization and sophistication of cyber attacks and financial crimes committed in cyberspace by these groups, suggesting this new type of organised crime is characterised with different, constantly evolving structures and new ways of using hi-tech tools to get illegal profit.

These two tendencies – the move of the organised criminality into cyberspace and the emergence of a new form of organised crime – do not exclude each other. They go hand in hand, giving rise to the synergy between traditional organised 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 broadly discussed in the academic literature, there is a lack of research examining the new forms and structures of organised crime online. This paper further focuses on the latter issue, providing analysis of the model and structure of these new crime groups committing crimes mostly or solely in cyberspace.

II. Ecosystem of Cybercrime: Business-Model of Operations

1. Business Models of Cybercrime

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.[12] Specific Internet forums and communications channels are used as underground marketplaces for the trading of illegal goods and services.[13] Any data traded on these shadow platforms has its own monetary value.[14] 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.[15]

Cybercriminals are increasingly structure their operations by borrowing and copying business models from legitimate corporations. Cybercrime business models were similar to those of high-technology companies in the early 1990s because digital criminality was still in its infancy. But since the early 2000s, cybercriminals have developed patterns imitating the operations of companies such as eBay, Yahoo, Google, and Amazon.[16] 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.[17] Another factor is the increasing specialization of perpetrators,[18] which means that cybercrime involves the division of labour. Other factors include the sophistication, commercialization, and integration[19] of cybercrime.[20]

It is argued, though, that there is a difference between cybercrime business models and legitimate business in terms of core competences 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.[21] 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.

2. "Criminal-to-Criminal" and "Crime-as-Service" Models

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 fuelled the creation of new patterns in criminal ecosystems, with regard to product placement, subcontracting, and networking.[22] 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 stolen data and very effective crime tools available through digital networks.[23] 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".[24] These crimeware tools such as viruses, Trojans, and keyloggers offer criminal groups the flexibility of controlling, stealing, and trading data.

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.[25] The core of the automation is a system of botnets: networks of compromised computers which can be controlled by the perpetrators remotely and used as "zombies". Users are usually not aware that they computers are infected with the malware and serve for the purpose of criminal networks. With a botnet, cybercriminals can make use of many compromised and controlled computers at the same time to launch large-scale attacks on private and corporate systems, send spam, disseminate malware, and scan for system vulnerabilities. Without botnets, they must target victims and machines manually and individually which would have made attacks too costly and time-consuming.[26] In this regard, the possibility to infect computers and turn them into "zombie"

networks was one of the main factors in transforming some types of cybercrimes, such as phishing, into a worldwide underground ecosystem which is run, supposedly, by organised groups.[27]

Crimeware is also used to deploy *Crime-as-a-Service (CaaS)* as a part of C2C business models: the system of trading and delivering crimeware tools. The trading of botnets has become a high-revenue activity in the underground economy, specifically concerning *Crime-as-a-Service* models. Criminal organisations offer botnets for relatively low costs, profiting from the turnover based on the number of "customers." Moreover, as one of the logical shifts in adopting business models from legal economy, criminals started employing the policy of price differentiation, moving from static pricing lists to the flexible pricing schemes with discounts and bonuses.[28] In addition, they nowadays offer different packages of the same products depending on the service. For example, in 2012 the basic package of Distributed Denial of Service (DDoS) bot Darkness by SVAS/Noncenz cost $450. The same botnet was offered also under "Bronze", "Silver", "Gold" and other options which included, depending on the price, free updates, password grabbers, unlimited rebuilds, and also discount for other products.[29] The costs of DDoS attacks vary from $5 for one hour to $900 for one month of persistent attack. 5-15% discounts are offered on the return policy base.[30] These costs are relatively low compared to the criminals' financial gains: the estimated revenue of crime groups using botnets range from tens of thousands to tens of millions of dollars.

In addition to the botnet trade, there is another emerging core service related to "Crime-as-a-Service" models of operations, namely, Pay-Per-Install (PPI) service which has become a key growing area of the underground economy.[31] This service has been developed to meet one of the vital demands of illegal market – infection of computer systems via digital networks. It outsources the dissemination of malware by determining the raw number of victims' computers that should be compromised within the budget of the "customer".[32] A single PPI service can partner with thousands of affiliates which are paid for the number of malware installs. A typical affiliate can supply more than 10,000 install per months which can generate millions of infected computers for illegal business including thousands of affiliates.[33] This business might be very profitable for affiliates: for example, Trend Micro reported about an affiliate who generated $300,000 from rogue AV installs in only one month.[34]

As yet another advanced step in the development of underground economy, tools-supplying business models are also used to share the techniques to commit cybercrimes. For instance, by creating "customer" systems where instruments are available on demand, the owners of the server with crimeware allow "users" just log into the server and choose from the range of tools suitable for fraud, phishing, and data-stealing and then download them. Less skilled criminals can buy tools to identify vulnerabilities, compromise system and steal data. More sophisticated offenders can purchase malware or develop custom tools and scripts on their own. When user data is stolen, criminals can use crimeware servers to commit organised attacks. These servers also allow for controlling compromised computers and managing the stolen data.[35] Furthermore, the next generation of business models started offering such services as licensed malware and technical support for illegal software and tools.[36]

3. Money Laundering and Money Mules

The final and essential part of the cybercrime business model is monetization of illegal commodity (stolen data and information). For this purpose cybercriminals use "money mules". Mules are usually recruited via spam or false job offers, promising high commission: between 3% and 5% of the total money laundered.[37] Their goal is to open a bank account, or sometimes use their personal account, and transfer the cash, very often in different jurisdictions than those in which the crimes have been committed.[38] The mules are the visible "face" of the organised cybercrime[39] because they are particular individuals turning the data into money,

https://doi.org/10.30709/eucrim-2012-022

and thus can be easily captured by law enforcement. Some studies consider them to be yet other victims of cybercrime because they might not be aware of the fact that they take part in criminal operations.[40]

It has been argued that "money mules" are the main bottleneck of underground economy of cybercrime.[41] Cybercriminals face the same problem as any organised crime groups with cash-out operation involving money mules: there are not enough of them in service. The ratio of stolen account credentials to available mule capacity concerning digital crimes could be as high as 10,000 to 1.[42] The lack of money mules is given to the fact that they usually can operate only for a very short time before they are either abandoned by their handler or revealed by the law enforcement. As an underground digital economy continues to expand, it will be increasingly challenging for criminals to maintain a necessary level of supply of these temporary "workforce" to profit fully from their illegal activities. Many sophisticated techniques have already been developed to deceit people into being hired as mules, such as masking the supposed illegal activities as legitimate services, for example, help in a job search.[43] It is very likely that the scam techniques for hiring money mules will continue evolving.

III. Crime Networks in Cyberspace: Reconsidering the Traditional Concept of Organised Crime Structure

Though it is already evident that cybercrime is evolving into big profit-driven illegal industry, it is still uncertain to which extent this market is dominated by the organised structures and to which extent they can be called organised crime. Indeed, it is very hard to fit the new form of organised on-line criminality into the traditional concept of organised crime because the structure of these new groups differs from what is traditionally attributed to the organised crime. Traditional organised crime groups are considered to be ethnically homogeneous, formally and hierarchically structured, multi-functional, bureaucratic criminal organisations.[44] In contrary, cybercrime has never gone through this stage of organisation during its evolution. It moved from individual and fragmented criminal activities to the models employed from the modern corporate business[45] but the structure behind this criminal business marks "the cleanest break to date from the traditional concept of organised crime groups as hierarchical".[46] The most common view on the structure of organised criminal groups is that they represent flexible networks formed by high-skilled, multi-faceted virtual criminals.[47]

As it was mentioned afore, Internet is used either as a medium or a sole platform for operation by both new and old types of organised crime. They can coexist without disturbing each other because of the very specific characteristics of Internet crime. One of the core characteristics of traditional organised crime groups is that they violently maintain a monopoly over their assets and territory to control certain scarce or illegal commodities on the black market.[48] The commodity at the illegal market is stolen, intangible data which circulate in borderless cyberspace. Obviously, cybercrime groups do not require control over a geographical territory – the concept of geographical control would not work due to the specific environment where the operations are taking place. Furthermore, cybercrime does not require a lot of personal contacts between members or enforcement of discipline between criminals. Again, any discipline would be hard to enforce in the cyberspace due to the lack of control mechanisms. Thus, the groups operating in cyberspace have less necessity for a formal organisation.

Moreover, the classic hierarchical structures of organised crime groups may even be unsuitable for organised cybercrime.[49] The new type of the organised crime in digital environment is less competitive[50] and its model of competition is rather similar to the modern corporate world with pricing strategies, service-based competition, innovation and "customer care" policy. The power of the criminal group is in the strength and sophistication of its software, not in the number of individuals.[51] From this point of view, automation

https://doi.org/10.30709/eucrim-2012-022

techniques in committing cybercrimes played a vital role not only in the development of the underground criminal industry, but also became one of the core factors determining the structure of the groups: with the automation the power focus shifted from people to technical tools.

On-line crime groups are believed to be more flexible compare to traditional organised crime groups, allowing for the incorporation of members for limited periods of time due to their flexibility.[52]These networks are structured on a "stand alone" basis, as members of the groups are often not supposed to meet.[53] They mostly rely solely on electronic communications and sometimes members do not have even virtual contact with their fellows. It is supposed that the majority of them carry out criminal activities using a number of web-based forums devoted to online crime[54] or Internet Relay Chats,[55] anonymous channels where member know each other only by their nicknames.

Both web forums and IRC channels are operated by administrators and serve the same goal of being a platform for illegal activities. However, forums seem to be more sophisticated ways of organising criminal activity online, because they have a peer-review process that every potential vendor needs to go through before status is granted to ensure that only trusted people get access to the illegal goods and services traded on the underground markets.[56] In contrast, virtually anyone can use IRCs for advertisement, which makes them more inclined to admit law enforcement agents or unreliable criminals. As a solution, IRCs offer services to check the validity of the data offered for sale.[57]

Speculation and debate as to the professionalism and organisation of criminal groups online are actually fuelled 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 organised groups.[58] Nevertheless, it is obvious that there is a certain level of organisation occurring on these platforms, at least on the administrative level. Moreover, recent studies argue that there is an incorrect assumption that organised crime in global networks is organised only on administrative level or relates only to distributed non-hierarchical "networks" with no links to traditional organised crime families. They point out that there is already a movement toward long-term organised crime activities in cyberspace.[59] For example, Symantec experts state that there is significant evidence that organised crime is involved in many cases involving the online underground economy.[60]

Concerning the size of the cybercrime groups (or networks), the estimates vary from 10 to several thousand members, when the affiliated networks are incorporated into the bigger and more complex structures. 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.[61] The criminal structures collaborate in teams where the roles are defined and the labour is divided.[62] 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: they can be either sold or supplied as a part of collaboration efforts.[63] The leading members of the networks divide the different segments of responsibility (spamming, controlling compromised machines, trading data) among themselves. There are some "elite" criminal groups that act as closed organisations and do not participate in online forums because they have enough resources to create and maintain the value chains for the whole cycle of cybercrime, and therefore have no need to outsource or to be engaged as outsiders into other groups.

Due to the fact that the cybercrime industry, though being already powerful, is still in the early stage of its development, there is a lack of data related to this phenomenon, especially concerning the actual level of its organisation. Thus, the main problem of assessing the structure of organised cybercrime groups is that there is much more information about what they are doing – or can possible do – and what harm they can cause

https://doi.org/10.30709/eucrim-2012-022

than about *who* is behind those groups.[64] Moreover, it is assumed that 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".[65] Recent studies on the organised criminality pointed out that new digital crime is being organised, though it has not yet been consolidated.[66] Thus, we are now witnessing the process of evolution of organised cybercrime; and the results are still unforeseeable.

IV. Conclusion: Addressing the Problem

Fighting cybercrime has always been a complex task. It extends beyond the national borders and spans different jurisdictions.[67] Committing crime in cyberspace is easy, fast and relatively safe for cybercriminals: intangible computer data can be fast and easily transferred around the globe via computer networks while offenders have no need to be present at the same location as the target.[68] At the same time, cybercrime investigations take a lot of time and efforts due to the international scale of the crime.[69] While information society is struggling with the problem of harmonisation of cybercrime legislation and cooperation on operation level to investigate crimes and prosecute cybercriminals, organised 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 harmonising 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 organised criminal groups.[70] The development of a comprehensive understanding and a forward-looking approach are required, since fighting organised cybercrime seems to be a moving target. The main goal is to tackle not only the top of the iceberg like money mules, but also those who are behind the visible face of the underground economy. In this regard, the study of the organised on-line crime phenomenon should help to determine the core nodes of the networks: for example, targeting the writers of malicious codes is more effective than targeting affiliates operating in the "pay per install" market, legal frameworks and operational measures aiming to take down botnets' control-and-command centres might be more effective that tackling those who are at the end of botnet distribution chain.

In the borderless cyberspace, international collaboration between the states is the key. While some states just do not have the necessary tools to respond to the activities of the organised cybercriminals, or they may lack the technical skills or face legal drawbacks,[71] the organised cybercrime can always find the safe digital havens. 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 harmonisation can be solved only on the global level.[72]

Since there is yet no clear understanding of the phenomenon of organised crime groups in cyberspace, it is very hard to tackle this developing problem. The process of elaboration of specific legal strategies to tackle on-line organised crime groups is still mere in its infancy. With the absence of a global strategy to counter organised cybercrime, the problem is very likely to deepen in the foreseeable future. With the development of ICT networks and the opportunities they offer, organised criminal groups will benefit from the entire range of tools and models available to legitimate economy sectors. The information's availability not only makes more accessible to organised groups, but also easier for them to foster and automate their fraud-committing activities. It would also probably link more opportunistic criminals to existing criminal networks.

https://doi.org/10.30709/eucrim-2012-022

Cybercrime might be going through a transformation into an organised illegal industry, where syndicates are highly sophisticated and are very hard to identify. Some cybercrime industries might end up to be run solely by organised 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 organisations, 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. In this regard, the problem shall be addressed by developing long-term responses that would include coordination and harmonisation of efforts on both the national and international levels.

---

1. SecureWorks, 2010. The Next Generation of Cybercrime: How it's evolved, where it's going. Executive Brief. Available at: secureworks.com↩
2. Williams, P. 2002. Organized crime and cyber-crime: Implications for business. Available at: http://www.cert.org/archive/pdf/cybercrime-business.pdf; UNODC, 2010. Globalisation of Crime. A Transnational Organised Crime Threat Assessment. Available at: http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf; McCusker, R. 2006. Transnational organised crime: Distinguishing threat from reality. *Crime Law and Social Change* 46, 257–273.↩
3. 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 .; Ben-Itzhak, Y. 2008. Organized cybercrime. *ISSA Journal* (October). Available at: https://dev.issa.org/Library/Journals/2008/October/Ben-Itzhak-Organized%20Cybercrime.pdf; Rush, H. et al. 2009. Crime online. Cybercrime and Illegal Innovation. NESTA Research Report. July. Available at: http://www.eprints.brighton.ac.uk/5800/01/Crime_Online.pdf; KPMG. 2011. Cyber crime – A growing challenge for governments. Issues monitor. Vol. 8, 3. July, P. 5; 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/.↩
4. Williams (2002) op.cit. P. 2↩
5. Goodman, M. 2010. International dimensions of cybercrime. In: S. Ghosh and E. Turrini (eds.): *Cybercrimes: A multidisciplinary analysis*. Berlin and Heidelberg: Springer-Verlag; Rush, (2009), op. Cit. P. 3.↩
6. Shelley, L. 2003. Organized crime, terrorism and cybercrime. In: Bryden and Fluri (eds.): *Security Sector Reform: Institutions, Society and Good Governance*. Baden-Baden: Nomos Verlagsgesellschaft, P. 307, Williams (2002), opt.cit, P. 2↩
7. McCusker (2006), opt.cit, P. 257↩
8. Williams (2002) op.cit. P. 1↩
9. Brenner, S. 2002. Organized cybercrime? How cyberspace may affect the structure of criminal relationships. *North Carolina Journal of Law & Technology* 4(1) (Fall). P. 25↩
10. Goodman (2010), op.cit. P. 313; 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. P. 5↩
11. BAE Systems Detica (2012) op.cit. P 2; Ben-Itzhak (2008), op.cit.↩
12. Europol (2011), op.cit. P. 4↩
13. 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. P. 1↩
14. For example, credit card details cost $2-90 per item, prices for bank account credentials with guaranteed balance range from $80 to $700 according to Panda Security(2010). Prices for different credentials vary depending on the amount of funds available, the location, and the type of the 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 according to Symantec (2008).↩
15. Cardenas, 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. P. 1; Europol (2011), op.cit, P. 4↩
16. Kshetri, N. 2010. The global cybercrime industry. Berlin and Heidelberg: Springer-Verlag. P. 190↩
17. 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. P. 4↩
18. BKA (Bundeskriminalamt). 2010. Cybercrime. Bundeslagebild 2010. Available at: http://www.bka.de/nn_193360/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true.↩
19. Offences subsequently lead to other offences, for example, attacks lead to stealing information, and then stolen information can be sold and used by those who bought it to commit fraud.↩
20. Grabosky, P. 2007. The internet, technology, and organized crime. *Asian Criminology* 2, P. 156↩
21. Kshetri (2010), op.cit., P. 189↩
22. Rush et al. (2009), op.cit, P. 37↩
23. Ben-Itzhak (2008), op.cit, P. 38↩
24. ESET. 2010. 2010: Cybercrime coming of age white paper. January. Available at: http://go.eset.com/us/resources/white-papers/EsetWP-CybercrimeComesOfAge.pdf. P. 4↩
25. Europol (2011), op.cit, P. 6↩
26. Ibid↩

https://doi.org/10.30709/eucrim-2012-022

27. Barroso, D. 2007. Botnets – The silent threat. ENISA Position Paper No. 3. Available at: http://www.dihe.de/docs/docs/enisa_pp_botnets.pdf. P. 7↩
28. Danchev, 2010. Study finds the average price for renting a botnet. Available at: http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528↩
29. McAfee, 2012. McAfee Threats Report: First Quarter 2012. Available at: http://www.mcafee.com/sg/resources/reports/rp-quarterly-threat-q1-2012.pdf↩
30. Danchev, 2012. DDoS for hire services offering to 'take down your competitor's web sites' going mainstream. Avaliable at: http://blog.web-root.com/2012/06/06/ddos-for-hire-services-offering-to-take-down-your-competitors-web-sites-going-mainstream/↩
31. SecureWorks, (2010), op.cit↩
32. Caballero, J., C. Grier, C. Kreibich and V. Paxson, 2011. "Measuring pay-per-install: the commoditization of malware distribution", Proceeds of the USENIX Security Symposium, August 2011. Available at: http://www.icir.org/vern/papers/ppi-usesec11.pdf↩
33. SecureWorks, (2010), op.cit↩
34. Trend Micro. 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.↩
35. SecureWorks, (2010), op.cit; Ben-Itzhak (2008),op.cit, P. 38↩
36. SecureWorks, (2010), op.cit↩
37. Panda Security. 2010. Panda Security Report. Cybercrime Black Market: Uncovered. Available at: http://press.pandasecurity.com/wp-content/uploads/2011/01/The-Cyber-Crime-Black-Market.pdf↩
38. Council of Europe, 2012. Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction. Available at: http://www.coe.int/t/dghl/monitoring/moneyval/typologies/MONEYVAL(2012)6_Reptyp_flows_en.pdf; Kshetri (2010), op.cit, P. 177↩
39. Europol, (2011), op.cit.↩
40. Panda Security, (2010), op.cit.↩
41. Council of Europe, (2012), op.cit.↩
42. 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. P. 9↩
43. Ibid↩
44. Council of Europe, (2004), op.cit. P. 2↩
45. Rush et al. (2009), op.cit, P. 42↩
46. Europol (2011), op.cit., P. 5↩
47. UK Home Office. 2010. Cybercrime strategy. Stationery office limited on behalf of the controller of Her Majesty's Stationery Office. P. 12↩
48. Rush et al. (2009), op.cit., P. 35↩
49. Council of Europe, (2004), op.cit. P. 7↩
50. UK Home Office (2010), op.cit., P. 13↩
51. Brenner (2002), op.cit, P. 27; Choo, K., and R. Smith. 2007. Criminal exploitation of online systems by organised crime groups. *Asian Criminology* 3: 37–59. P. 41↩
52. 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. P. 10↩
53. Choo, K. 2008. Organised crime groups in cyberspace: A typology. *Trends Organ Crim* 11, P. 7↩
54. 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. P. 5, Rush at al, (2009), op.cit.↩
55. Fallmann et al. (2010), op.cit, P. 1↩
56. UK Home Office (2010), op.cit, P. 12↩
57. Rush at al., (2009), op.cit., P. 50↩
58. Symantec (2008), op.cit, P. 5↩
59. BAE Systems Detica (2012), op.cit.↩
60. Symantec (2008), op.cit.↩
61. UK Home Office (2010), op.cit.↩
62. Rush et al. (2009), op.cit, P. 42↩
63. BSI (2011), op.cit, P. 4↩
64. Rush et al. (2009), op.cit↩
65. Trend Micro. 2006. Phishing. A trend micro white paper. November. Available at: http://www.antiphishing.org/sponsors_technical_papers/trendMicro_Phishing.pdf. P. 6↩
66. BAE Systems Detica (2012), op.cit, P. 2; Symantec (2008), op.cit↩
67. Hunton, (2009), *The growing phenomenon of crime and the internet: A cybercrime execution and analysis model.* In: Computer Law&Security Review, Vl. 25, Issue 6, P. 533↩
68. Gercke, M. 2012. Understanding cybercrime: A guide for developing countries. ITU, Geneva; Joffee, (2010), Cybercrime: the global epidemic at your network door. In: Network Security 01/2010; 2010.↩
69. Bradbury, (2012), *When borders collide: legislating against cybercrime*. In: Computer Fraud & Security, Vol. 2012, No. 2. (February 2012), pp. 11-15↩
70. Europol (2011), op. Cit.↩

71. Goodman (2010), op. Cit.↩
72. Sieber, U. 2008. *Mastering complexity in the global cyberspace: The harmonization of computer-related criminal law.* In: M. Delmas-Marty, M. Pieth, and U. Sieber (eds.): *Les chemins de l'Harmonisation Pénale/Harmonising Criminal Law*. Collection de L'UMR de Droit Comparé de Paris. Bd. 15. Paris: Société de législation comparée, 127–202.↩

ABOUT EUCRIM
eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union