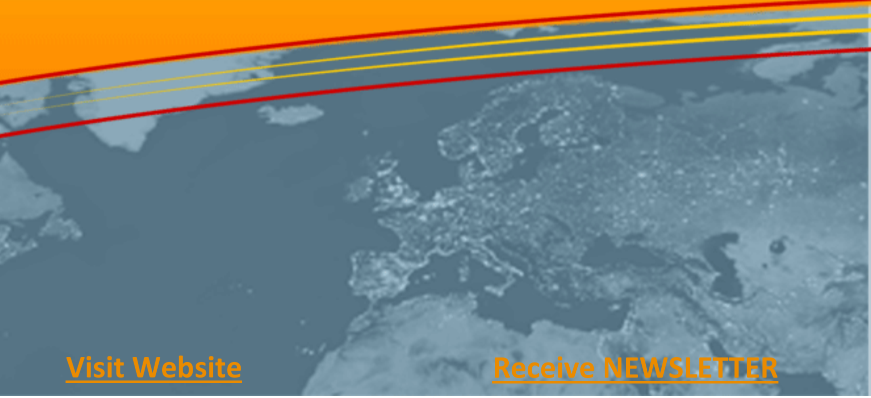
ieee.es
Spanish Institute for Strategic Studies

Analysis
Document



02/2014

07th January 2014

María José Caro Bejarano

ORGANISED CRIME AND INTERNET
2nd part

Visit Website

Receive NEWSLETTER

This document has been translated by a Translation and Interpreting Degree student, ALEJANDRA CUBERO ECHEVARRÍA, doing work experience under the auspices of the Collaboration Agreement between the Universidad Pontificia Comillas, Madrid, and the Spanish Institute for Strategic Studies.

ORGANISED CRIME AND INTERNET 2nd part

Abstract:

A former analysis document addressed industry and government concerns about cybercrime. It also underlined the need to distinguish whether a specific use of Internet by organized crime represents a threat to national or international security. This document continues and finishes the analysis of the issue, which is the basis to find the right answers.

Keywords:

Cybercrime, Information and Communication Technology, ICT, national and international security, cyber threats, cyber-attack, cyber security, critical infrastructures.

ORGANISED CRIME AND THE INTERNET. ITS IMPLICATIONS FOR NATIONAL SECURITY

A former document described the beginning of the analysis of whether organized cybercrime might have implications in national and international security or not. It underlined the need to distinguish which cybercrime actions form part of each category to find out the correct answers. This document we will study these issues to have a clear and organized view of them.[1]

A PROBLEMATIC CONCEPT

Internet provides anonymity, which makes it relatively easy to hide people's identity and, therefore, it is sometimes difficult to determine whether the perpetrator of a cybercrime is an individual, an organization or a third perpetrator (State or non-State) agent.

Expert hackers are often able to avoid attribution, therefore, people affected by an intrusion in their information system cannot be sure whether actions were made by just one perpetrator, by an organized crime group or by an alien government agent. In fact, it is possible that two or more of these actors act together under sponsorship agreements or hybrid forms. Organized crime groups can obtain specialized malicious codes from an individual provider (for example the role of the organized crime group called "Russian Business Network" is frequently speculated in the cyber-attacks against Estonia and Georgia and in the relationship between this group and the Kremlin during that time[2]).

At the same time, we cannot be sure of the physical location from where an attack is perpetrated. Cyberspace does not have limits and it is easier to commit a crime on the other side of the world as well as in the same jurisdiction. In fact, one of the distinctive characteristics of cybercrime is its "limitless" nature; the criminal, the victim and the evidence of the crime can be located in different places all around the world. Moreover, the mix of the public and the private sphere in advanced industrialized societies means that cybercrime space is very fluid. One day, a professional cybercriminal can work for a government, the next day for himself and the day after for an organized crime group.

[1] Grabosky, Peter, *Organised Crime and the Internet*, The RUSI Journal, 2013.

[2] Korns, Stephen W. y Kastenberg, Joshua E., *Georgia's Cyber Left Hook*, available on http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/08winter/korns.pdf

For this reason, the standard definition of organized crime, three or more people acting together to make money, does not precisely coincide with the complexity and features of its cyberspace version. For instance, it does not include some of the sophisticated forms of organization, such as the mobilization of botnets (the abbreviation for nets of robots), which some analysts consider as a form of organized crime activity. Botnets include a criminal, who generally acts alone, and uses a malicious code in order to take the control of a bigger number of devices (he/she can reach even more than a million of separate machines).

In this way, individual and institutional owners and users of the involved computers can take part in the criminal activity involuntarily. However, thanks to new technologies, this different form of organization allows individuals or small groups of people to access without permission and to control company's personal assets and potentially an enormous amount of information.

THE VARIOUS CRIMINAL USES OF THE INTERNET

At a very basic level, criminals use the Internet for their activities in the same way as normal people do, namely as a mean of communication and as a mean to store information and records. For instance, illicit drug producers trade with prescriptions through the Internet. This is the first of three steps in the criminal use of the Internet: as a criminal instrument. However, and maybe more importantly, it can be used as the criminal goal and even as an incidental support of the criminal activity. The three methods can be applied to an organizational and individual use and they are not necessary simultaneously excluded.

In a general way, the Internet is used as an instrument to attack other informatics systems. Most cybercrimes begin when a criminal obtains unauthorized access to the system. Systems are often attacked with the purpose of damaging or destroying them as well as the information they contain. This can be an act of vandalism or protest, or an activity made with other political objectives. One of the most common methods is the distributed denial of service (DDOS) which implies the flood of an informatics system by a massive amount of information so that the system slows down. Botnets are very useful for this purposes because they send various requests of coordinate service.

A famous example of a DDOS attack started by botnet took place in April 2007, when the Estonian public and commercial servers were seriously damaged for several days. Online banking services were interrupted intermittently and online access to certain governmental websites and to the media was limited. According to some sources, attacks originated in Russia[3] and it is alleged that it was the result of cooperationbetween Russian youth organizations and Russian organized crime groups. This collaboration was tolerated by the State even if it the degree of implication of the Russian Government was not clear.

As state actors or agents can use the Internet to pursue what they perceive as national security objectives, extremists and insurgents groups use Internet technology in different ways to promote their goals. These aims include the use of Internet as an stealing instrument in order to increase their databases, for example as a means of fraud.

However, the Internet is not used for illicit goals mainly and exclusively by political actors. Organized crime groups also use it every day at a global scale, through participation in activities that can include illicit acquisition, the copy and spread of intellectual property (piracy caused a loss of billions of dollars for software and entertainment industries[4]), but also the raid of bank and credit cards data, of trade secrets and the classified information owned by governments. These actions can also start with the unauthorized access to an informatics system: in fact, the stealing of financial personal data provided the basis for a flourishing market for these type of data, which allows fraud at a greater level.

ORGANIZED CYBERCRIME AS A THREAT TO SECURITY

Digital technology spread and, as a result, the vulnerability of cybercrime has proportionally increased. If we analyze the new forms of cybercrime in recent years, the potential risk for national security.is easily recognizable.

[3] Landler, Mark y Markoff, John, "Digital Fears Emerge After Data Siege in Estonia", *New York Times*, May 29, 2007. See http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all.

[4] Nowadays there are no reliable estimates about the cost of the organised cybercrime. A report of Dettica of 2011 estimated the cost of 27.000 million pounds in the United Kingdom which represents 2% of its GDP. A later study of 2012 calculated that the cost reached 5% of the GDP of the country. Anderson et al., *Measuring the cost of cybercrime*.
Available at: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

The former example about the attacks to Estonian Government services underlines the link between organized cybercrime and security and it raises the question of whether some types of cybercrime, carried out with the sponsorship of the State or State agents, can be considered as an act of war. Traditionally, an act of war implies threat or the use of force by a State against territorial integrity or the political independence of it. Cyber activities added another variable to the equation, therefore another definition of what is a hostile act between States is needed and how it has to be interpreted in legal terms. Again, another well-known example happened in 2010, when it came into light that the control systems that supported the uranium enrichment programs of the Iranian Government had been infected with a malicious code, which had consequently destroyed a great number of centrifuges.[5]

In addition, at least since 1998,military use of technology has been openly debated . Since then, the militarization of cyberspace has continued at a good pace. An unknown number of nations is developing offensive cyberwar capabilities to that can, among other things, interfere with the management, control and communication systems and confuse and destroy critical infrastructures. Already in October 2012, the United States Secretary of Defense, Leon Panetta, spoke about a “cyber-Pearl Harbor” in the hands of a hostile State or of an extremist group.[6]

States and non-State actors are cyber-spying -it is estimated that more than 100 countries all around the world were participating in some way in such activity.[7] This prevalence probably has not decreased since then, according to last month’s headlines.

The vulnerability of government secrets being stolen(despite the tendency of some guardian to exaggerate their value) was clearly explained through the publication of 400.000 diplomatic cables of the U.S. Department of State by Wikileaks organization. It is unlikely

[5] David Alandete, *El País*, June 1st, 2012: The New York Times revealed the existence of a cyber-attack programme, called Olympic Games operation by George Bush’s Administration. There are further explanations about this issue on the book called *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, by David Sanger.
See http://internacional.elpais.com/internacional/2012/06/01/actualidad/1338572841_317814.html

[6] *El País*, October, 12th 2012, “El Secretario de Defensa de EE.UU avisa del riesgo de un ataque cibernético” Available at: http://internacional.elpais.com/internacional/2012/10/12/actualidad/1350061446_784106.html

[7] Brodkin, Jon, *Government-Sponsored Cyberattacks on the Rise, McAfee Says*, Network World, November 29th, 2007. See http://www.networkworld.com/news/2007/112907-government-cyberattacks.html?page=1

that the copy and spread of such a big amount of information happened without the use of digital technology. Some people argue that the revelation of classified information is, ipso facto, a threat to national security, others affirm that the act of classifying information is subjective and that transparency must prevail.

This example also underlines how difficult it is to define organized cybercrime in certain circumstances: Wikileaks is an organization that cannot be classified according to any traditional definition as an organized criminal group, with respect to organized criminal activity on the Internet, with consequences in security, any good categorization is difficult to reach. There is also another level of complexity: non-State groups and individuals, when they act without State sponsorship, still have the capacity of interrupting and, therefore, of threatening national security. The interruption of electronic trade and bank services, for example, could jeopardize one of the main platforms of economic development.

THE DIVERSITY OF ORGANIZED CYBERCRIME

A brief descriptive review about organizational specific cybercriminal activity is outlined hereunder. The examples selected do not represent the entire world of organized cybercrime, but they illustrate the great diversity of organized crime activities that depend on the Internet, the consequences on security, and the reasons why people undertake such activities. In this way it is possible to highlight the difficulties that still persist in classifying in a clear way the different types of online organized criminal behaviors.

Azov Film production, based in Toronto, and its owner, Brian Way, were the main objectives of “Proyecto Espada” an operation that allowed the dismantlement a wide range of child pornography. Apparently the company worked on the distribution of naturist DVDs and streaming films, which were legal in Canada and in the U.S., but under this cover, Way sent videos with scenes of naked minors to 94 countries, obtaining an annual benefit of 1.600 million dollars. This police operation, which started in Canada with branches in other countries, Spain, Ireland, Sweden, Norway, South Africa, Australia, United States, Mexico and Hong Kong, concluded with 340 detentions in different countries, included Spain. The investigation, which started in 2010, seized up to 45 terabytes of thousands of sexual videos and images of minors.

The Anonymous group is a flexible collective of anarchists mainly based on the shared values of mischief and on resentment against authority.It is devoted to the so-called "hacktivism" or activism in the net. The dominant value of iconoclast started to focus on important symbols. The methods used were the disfiguration of websites and DDOS attacks, combined with verbal abuse in the network. Not in vain, the website of the Central Intelligence Agency of the U.S. (C.I.A.) represented an interesting target. The group, imbued with hacker spirit about the idea that information must be free, focused itself on the secret of the Scientology Church, the exclusive distributor of the American Society of Cinematographers, and became a supporter of Wikileaks.

When the U.S. Government convinced several electronic payment services providers to interrupt the processing of Wikileaks contributions, Anonymous managed DDOS attacks against to those who participated.

Zeus virus was refined by Eastern Europe software engineers, it was identified for the first time in July 2007 and it spread, in particular in spring 2009. This malicious code was used by Ukrainian hackers to obtain access to computers of workers of several small companies, municipalities and non-governmental organizations in the U.S. A virtual plague was developed for a simple and dangerous aim: to steal the bank account data and passwords of their victims. The affected devices were in danger when the victim opened an apparently harmless email. Having the access to the bank account details of the victims and their passwords, the Ukrainian attackers were able to log in in the target organisms of the bank accounts. Ukrainian attackers' accomplices posted announcements in websites written in Russian where they asked students that lived in the U.S. to help them in the transfer of funds outside the country. These students, called "mules" received false passports and they were asked to open accounts with false names in different financial institutions of the U.S. After transferring to the mules' accounts the the funds obtained illicitly, the attackers trained mules to move the funds to accounts in foreign countries, and in some cases, to smuggle funds physically out of the U.S.

This year in Facebook they appeared again with new strategy: use Facebook to infect computers. The virus makes it impossible to shut down the computer once it has been activated. According to some reports, the virus is attached to fake Facebook links and when the link is open, the user is redirected to a website that requests the download of a common software. After the download, the virus is activated. From that moment on, every time a user accesses to his/her bank accounts he/she is in danger. Zeus, also known as ZBOT, is as powerful that it can even substitute the homepage of afinancial institution in order to trick people into introducing their information.

In May of the current year, the "Policía Nacional", the Spanish police force, arrested the people responsible of a group that defraud more than 750.000 euros through cloned cards. People arrested presumably form the management leadership of the Spanish organization. They bought online high quality electronic products with fraudulent credit cards in order to sell them lately in e-commerce websites using shell companies. They were charged of the crimes of falsification of commercial documents, money-laundering, participation in criminal organization, informatics fraud and asset stripping. They obtained the card data through Trojan, phishing and/or pharming.[8]

The Olympic Games operation was a collaboration between the U.S. National Security Agency (NSA) and its Israeli counterpart, Unit 8200, with the aim of interrupting the Iran uranium enrichment program.[9] It allegedly implied the clandestine introduction of an extremely complex and sophisticated software (most commonly known as Stuxnet) into the communication and control systems in the nuclear plants of Natanz. The software included the capability of monitoring the communications and the working activity as well as the capability of corrupting the plant control systems. The success of the operation resides in the delay of the uranium enrichment program through the destruction by remote control of several centrifuges used in the process. The secret around the operation was compromised, in part, when the malicious code pass into the Internet due to a programming mistake. This constitutes the most famous cyber-cooperation operation for now.[10]

[8] Further information at http://www.policia.es/prensa/20130521_1.html

[9] This operation is outlined in the David Sanger book called Confront and Conceal.

[10] Sanger, David E. and Shanker, Thom. "Obama to Keep Security Agency and Cyberwarfare Under a Single Commander", *The New York Times*, December 13, 2013, See: http://www.nytimes.com/2013/12/14/us/politics/obama-to-keep-security-agency-and-cyberwarfare-under-a-single-commander.html?_r=0

GhostNet was the name given by a Canadian researchers group to a cyber-spying operation in 2010, which apparently operated from Internet commercial accounts in China. Hackers jeopardize the government computers in more than 100 countries and also controlled emails sent from the Dalai Lama server. Chinese government denied its direct participation and there was no conclusive evidence of the government complicity. Chines authorities showed to dissidents who returned to China from foreign countries the transcript of the Internet chats in which the dissidents were implied while they were out of the country. At least this can suggest that the State is an accessory.[11]

Maybe one of the most well-known groups that participated in organized cybercrimes (in this case, supposedly sponsored by the State) is the Unit 61.398 of the Chinese popular army, People Liberation's Army (PLA). In February 2013, the U.S. information security company, Mandiant, informed about a largescale industrial espionage program that started in 2006 in the Unit mentioned before.[12] Based in Shanghai, this organization supposedly obtained a massive volume of data of a wide range of English-speaking countries industries. Information allegedly extracted includes technical details, negotiation strategies, price lists and other data about owners. In 2009, an important U.S. beverage producer, one of the supposed objectives, was planning the major foreign takeover of a Chinese company until today. An apparently innocuous email to an executive member of the U.S. company contained an Internet link which, once opened, allowed attackers to access the company's network. According to the Mandiant report, Chinese intruders accessed regularly to sensible information on pending negotiations and finally the takeover was not concluded. It is not clear if PLA unit is exclusively formed by military personnel or if it includes civilian contractors.

The NSA, National Security Agency, part of the U.S. Defense Department has been developing a large-scale capture, storage, and analysis data program since 2001. This program, diffused by Edward Snowden, former analyst subcontracted by the NSA, is based especially on the cooperation between the telecommunication operators and the service

[11] *Tracking GhostNet: Investigating a Cyber Espionage Network,* March 29, 2009. See: http://www.securityfocus.com/blogs/1809.

[12] *Mandiant Intelligence Center Report, APT1: Exposing One of China's Cyber Espionage Units*. Available at: http://intelreport.mandiant.com/.

providers of private sector and on the participation of contracted private consultants, of which Snowden was part of. Companies that cooperated are well-known in the Internet field. According to what was reported, the program captured and stored a great range of data, included email messages, chats, Voice over Internet Protocols (VoIP), photos, data, transferred files, videoconferences and other social network content. The NSA and its private sector partners also achieved to avoid encrypt technologies in the network. One of the things discovered was that communications were intercepted between the Mexican and Brazilian President, the French Ministry of Foreign Affairs, among others, and Petrobas, the Brazilian semi-public oil company.[13]

The previous examples of cybercrime suggest that not all the organizations acting illicitly in the cyberspace can be considered as a threat for national and international security. Some of them are surely disturbing, extremely offensive and often harmful. In the meanwhile, there are some online activities which probably can weaken State's integrity and the economy and therefore they could be considered as a threat to security. U.S. software and entertaining industries affirm that piracy causes millions of dollars of lost profits for the domestic economy and a sense of fear over entrepreneurial and creative spirit all around the world. Nevertheless, U.S. economy is enough diversified so its strength in the future will depend on other factors.

In fact, it might be said that piracy allows citizens of least developed countries to access products that otherwise they would not be able to afford. In the same way, others say that organizations like Wikileaks, in fact, provide a service diffusing information that should not be hidden to the public. On the other hand, the principal and persistent industrial and political espionage, on a larger scale, can also be a threat for the security of a State.

Industrial espionage can weaken international competition of a company or of an industrial sector, in the most obvious case, when the information concerned referrers to weapon systems. In the same way, stealing bank data or credit cards, if it happens in a larger scale,

[13] Greenwald, Glenn, XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet", Guardian, July 31st 2013. See at http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data; Saiz, Eva, "EE.UU. accede a información de usuarios de los gigantes de internet", *El País*, June 7th 2013.
See at http://internacional.elpais.com/internacional/2013/06/07/actualidad/1370564066_752776.html.

will complicate for sure trade activities and the corresponding damage in the State’s economy. However, at the moment, the bank absorbs the losses (or they pass them to consumers) and the online fraud seems tolerable. Security in technologies must be refined and the most part of technology experts, at least in the developed countries, are able to protect themselves. Also online banking and electronic commerce are still flourishing. However, in the least developed countries where users have just entered the digital era, the lack of consciousness on cybersecurity can increase vulnerability of individuals and organizations of the public and private sector. In so far as the threat of cybercrime impede the development of electronic commerce, it can contribute to weaken of the economic security of a nation.

In regards to organization, it is observed that the major threats to national security are posed by the State itself, without the help or with the collaboration of expert amateurs or sophisticated cybercriminals. The cyber activity that lead to the destruction of the Iran centrifuges was defined, without any doubt, by their authorities as a threat to their security. Nations affected by similar attacks could consider them as cyberwar acts.

In the meantime, Anonymous activities, like spying a call conference between law enforcement authorities and the attempt to close the Central Intelligence Agency (CIA) website, were surely disturbing for the U.S. authorities. Although it is embarrassing, this relatively small scale activity does not constitute a threat to national security. However, if it is realized persistently or in a larger scale, such activity can send a message of indifference by the State, in the best case scenario, and in the worst one, of incompetence. Therefore it will invite several other attackers to do the same. So it is a real important potential threat. The threshold of a threat to an objective seems to be a possible function that can be reach by criminal activity, on the one hand, and the recovery and resistance capacity of the State and its infrastructures on the other hand.

In the Wikileaks case, its declarations could have complicated the power of U.S. diplomats to obtain sincere comments of the local informers from all around the world. Some of these revelations seem to have increased the vulnerability of weak regimes and, for this purpose, the organized cybercrime was, without any doubt, a threat to its security. It is yet to be seen if this is going to improve or affect U.S. security.

CONCLUSION

If cybercrimes or organized cybercrime were committed on a larger scale, it would lead to the undermining of the the confidence of the main public or private institutions. The key question is when the nature and the scale of the cybercrime activity (organized or not) becomes a threat to security. The question is not whether a nation is safe or not, but if a specific circumstance can contribute to an improvement or a reduction of security.

It is worth stressing that in this sense a lot of these cybercriminals that now operate in the cyberspace, alone or within organizations, were competent experts before working in the cybercrime. What is interesting is the relatively small role that conventional organized crime groups played until now in cybercrime. The main role of the Internet technology seems to be accidental, as a mean of communication and record keeping.

There are examples of conventional criminal organizations in which experts take part in Information Technologies for specific tasks. (This model of commitment is not different from the one of large scale drug dealers who contract professional chemists to help them in the perfection of heroin or in the production of synthetic drugs.)

In the meantime, digital technology application in the direct criminality is more and more sophisticated and accessible. There are plenty of hackers for hire in the cyberspace. The potential of malicious code kits or exploits ready for the use or to be sold in the organized crime market is already significant and it will probably increase. These kits can be rent but also the lender can even offer support for users and they can provide also regular updates as part of the service agreement. There is no doubt that conventional organized criminal, which has increased during the digital era will adopt technology as a regular practice, if they did not do it yet, for mundane purposes as well as illicit.

Given the actual omnipresence of digital technology, its accessibility by criminal organizations and its evident use for a great range of criminal purposes, there is no doubt that the potential threat to national and international security will persist and, in fact, it will intensify.

The worries about the vulnerability in the digital field explain why developed countries and international organizations have developed cybersecurity strategies in their legislations. In the Spanish case, last December 5th, the nation joined the group of countries with the approval of the "Estrategia de Ciberseguridad Nacional" (Spanish National Cybersecurity Strategy).[14] It deals with the field of cybersecurity in a more detailed way, even if it is already taken into account in the "Estrategia de Seguridad Nacional" (Spanish National Security Strategy) approved on May of the current year.[15]

María José Caro Bejarano
IEEE Senior Analyst

[14] The *"Estrategia de Ciberseguridad Nacional"* can be consulted at the following website: http://www.lamoncloa.gob.es/NR/rdonlyres/680D00B8-45FA-4264-9779-1E69D4FEF99D/255433/20131332_completo_05dic13_0955h.pdf.

[15] The *"Estrategia de Seguridad Nacional"* can be consulted at the following website: http://www.lamoncloa.gob.es/NR/rdonlyres/0BB61AA9-97E5-46DA-A53E-DB7F24D5887D/0/Seguridad_1406connavegacionfinalaccesiblebpdf.pdf.