XXIV
TECMUN Jr.

Commission on Crime Prevention and Criminal Justice

Outline of the Commission on Crime Prevention and Criminal Justice

The Commission on Crime Prevention and Criminal Justice (CCPCJ) was established by the Economic and Social Council (ECOSOC) resolution 1992/1, upon request of General Assembly (GA) resolution 46/152, as one of its functional commissions. The Commission acts as the principal policymaking body of the United Nations in the field of crime prevention and criminal justice.

ECOSOC provided for the CCPCJ's mandates and priorities in resolution 1992/22, which include improving international action to combat national and transnational crime and the efficiency and fairness of criminal justice administration systems. The CCPCJ also offers Member States a forum for exchanging expertise, experience and information in order to develop national and international strategies, and to identify priorities for combating crime.

Topic A

Measures to counter cyber crime, making emphasis on cyber warfare as an emerging problem on the global agenda and its consequences on national and international law

By: José Antonio Martínez Caldera

Background

Nowadays, the presence of technology has an aspect on the daily life of millions of people. and the transnational organized crime was not left behind. Organized criminal groups use the technology to threaten peace and human security, violates human rights and undermines the development of societies on the world (UNODC, N.D.).

The cyber warfare is defined as any action by a nation-state to infiltrate another state's computer network with the purpose of causing some sort of damage (UNICRI, 2015). Known as the fifth domain of warfare (UNICRI, 2015). It consists of three menaces, online acts of espionage, online sabotage, attacks on Supervisory Control and Data Acquisition (SCADA) networks and Nuclear Control Institutes (NCIs).

Also, the increasing rate of the use of internet by terrorist groups through the misuse of big data and hacking of robotics technology damages the life of millions of people all around the world. The lack of coordinated legislation and policies towards this emerging problem shows no answer.

Criminals tend to use these methods to steal credit card information and money. Moreover, the Internet has become a breeding ground for criminal activity related to copyright and intellectual property rights, violating the privacy and confidentiality of different actors on the international community.

The security of confidential and private information from public and private sector has social, economic and political impact. Since it is information regarding to a single entity, a cyber attack is considered a violation to the national security and must be punished with all the weight of the law.

Cyber warfare

Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks. This is a new kind of warfare since the mugger can attack a country, violating its national security, without going to war.

However, nowadays is very difficult to differentiate between cyber warfare and just a cyber attack since any State takes credit of the attacks, normally, it is only related to a single actor or a single group but never a country, hence, the term *cyber war* has been misused. According to Dr. Thomas Rid, professor of King's College London affirms that Prime ministers and presidents call it an act of war but everything falls into a political decision.

So, we need to understand what does an act of war means. Any act by a State that would effectively terminate the normal international law of peacetime and activate the international law of war (Turns, N.D.). Hence, to consider a cyber attack as an act of war, any State needs to openly accept the perpetration, wanting to change or affect the network of other country.

Having said that, we must consider that an intromission on the confidential private information of a country is a violation to its national integrity, it must be punished, in the national and international level, according to the rule of law and respecting the sovereignty of each country.

According to United States Agency of International Development[1], there are four "cyber weapons" which attackers use in order to enter into the nation's network. (1) Viruses, (2) Worms, (3) Trojan Horse and (4) Backdoors. This group is denominated as malicious malware and are used by criminals as a cost effective method to make money.

Online acts of espionage

For the governments, looking after confidential and classified information has become a very hard work to do. The espionage, one of the three areas of cyber warfare, regards to the infiltration to their networks and spread of this information into the Internet.

This is a problem of national security because it threatens to the sovereignty of the country. According to an article of *The Atlantic Magazine* of 2014[2] establishes that there are two types of cyber espionage (1) Computer Network Exfiltration (CNE), involves only spying by taking notes of the actions and (2) Computer Network Attack (CNA), actions designed to destroy or otherwise incapacitate enemy networks.[3]

According to an interview made to the U.S. Attorney General Loretta Lynch affirmed that fighting economic espionage is a top priority of the Department of Justice.

[1] Cyber Crime: Its Impact on Government, Society and the Prosecutor: http://pdf.usaid.gov/pdf_docs/Pnada641.pdf HYPERLINK "http://pdf.usaid.gov/pdf_docs/Pnada641.pdf"

There's No Real Difference Between Online Espionage and Online Attack: http://www.theatlantic.com/technology/archive/2014/03/theres-no-real-difference-between-online-espionage-and-online-attack/284233/ HYPERLINK "http://www.theatlantic.com/technology/archive/2014/03/theres-no-real-difference-between-online-espionage-and-online-attack/284233/"

[2]

Online sabotage and online espionage are, somewhat, correlated and it is common that one leads to the other.

[3]

> *"When it comes to economic espionage, this is in fact a tremendous problem because ... be they individuals or be they state actors ... essentially they're stealing from future generations also. We take these matters very seriously... It is a matter of priority for us." (Lynch, N.D)*

Online espionage attempts to the national security of the countries by creating national and international uncertainty in relation with the flow of information. Also, as an issue of national security matter, it must be punished with the full weight of law, respecting international agreements and the rule of law.

Online sabotage

According to United Nations Interregional Crime and Justice Research Institute (UNICRI), the sabotage is defined as the use of the internet by one nation state to disrupt online communications systems of another nation state (e.g. military communication networks) with the intent to cause damage and disadvantage.

Online sabotage has three levels, according to the report of *Manupatra*[4] in relation with online attacks, (1) Data interception, the mugger targets a person for later on use that information for an attack (2) Data alteration, when the information is intercepted, it is tampered before it is retransmitted or reach its destiny (3) Data selling, information that is sold to a third party, usually includes passwords, bank information or any other confidential information.

This problem, as mentioned before, affects the private and the public sector and it can has social, political and economic aspect, affecting and breaking international relations with the misuse and/or alteration of information. The online sabotage has as main purpose alter or give the wrong use to information flowing on the Internet.

Taking into consideration that online sabotage plays a role in cyber warfare, this issue can have serious political impact by the infiltration on confidential national documents, by consequence, violating its national integrity. However, there is no specific legislation to punish this kind of cyber warfare.

[4] On-line-Crimes and their impacts http://www.manupatra.co.in/newsline/articles/Upload/779E337A-DDF8-41AE-ACA4-89F3CB746F2D.pdf HYPERLINK "http://www.manupatra.co.in/newsline/articles/Upload/779E337A-DDF8-41AE-ACA4-89F3CB746F2D.pdf"

Attacks on SCADA networks and NCIs

Supervisory Control And Data Acquisition (SCADA) networks are national industrial control systems –computer systems (consisting of hardware, software and communication components) designed to monitor and control various critical infrastructures or facility-based processes. They include the computer-based systems that run such critical infrastructure as power generation plants and transmission networks, refinery plants, oil and gas pipelines, and transport and communication systems (UNICRI, N.D).

Normally, connecting control networks with a larger corporate network makes easier for managers to complement plant operations with business goals and improve efficiency. Unfortunately, this has open a path for hackers to introduce into this networks and harm or modify plant's process control systems.

According to Dell's annual threat report of 2014[5], United States of America, United Kingdom and Finland are the most susceptible countries to violation into their SCADA networks with *51,258*; *69,656* and *202,322* attacks respectively in 2014. In accordance with the same report, the most common way in which criminals attack SCADA networks is because an improper restriction of operations with a 25%.

There are different ways in which SCADA networks can be bothered. As previously mentioned, the most common way is an improper restriction of operation but there are other ways, for example, in second place we found with a 9.09% an improper input validation and information exposure.

> *"Since companies are only required to report data breaches that involve personal or payment information, SCADA attacks often go unreported,"* said Patrick Sweeney, executive director of Dell Security. *"As a result, other industrial companies within the space might not even know a SCADA threat exists until they are targeted themselves."*

Dell Security Annual Threat Report. https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf HYPERLINK "https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf"

5

Also, violations of Nuclear Control Institutes (NCI) is on the growth. The costs of production of nuclear plants are higher than a non-nuclear one[6]in the United States (2011). Hence, the nuclear plants rather use an analog system of security than an electronic update believing that it will avoid a cyber attack.

Despite this, it has not avoided cyber attacks and sabotages to the nuclear facilities in different countries are a reality. For example, the attack to the nuclear plant of Natanz, Iran, in 2010 causing a malfunctioning of the plant and been called as the first cyber attack in history using an informatic worm.

Measures taken by the international community

In order to adapt to the new tendences of the world, including the use of Internet, the international community has developed different networks or measures to answer to these necessities. From private to public, both sectors have to comply and integrate cyber security as a top priority.

All or most of the countries, guided by the new tendences of the world, need to adapt their facilities, networks and employees in order to respond to them. The use of Internet is not anymore a luxury, it has become a necessity.

- 13th UNITED NATIONS CRIME CONGRESS

On 2015, during the 13th United Nations Crime Congress celebrated in Doha remarked the relevance of cyber crime. *"Cybercrime has become an established threat to the security of States and individuals alike,"* (Lungameni, 2015). During this congress, was developed a strategy in which developing countries could counter the lack of capacities towards cyber attacks and other forms of cybercrime.

Actually, the strategy developed during this congress has not been implemented yet but the ideal of prepare and capacitate Latin American countries against the different cyber attacks is the same. The main goal of this strategy, as it was established on the proposal, was a collaboration between States to counter cyber crime and the different cyber attacks.

In the same congress was adopted a resolution regarding the *Thirteenth United Nations Congress on Crime Prevention and Criminal Justice* [7] in which was established on the global

Nuclear plants in United States of America (2011) http://large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdf HYPERLINK "http://large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdf"

6

Draft Doha Declaration on integrating crime prevention and criminal justice into the wider United Nations agenda to address social and economic challenges and to promote the rule of law at the national and international levels, and public participation:

agenda to counter cyber crime, touching several points about the use of technology as a tool for the sustainable development of society.

Furthermore, point 09 subsection (a) which proposes to strengthen the capacities of the judiciary and law enforcement institutions, and to adopt legislative and administrative measures to adequately prevent and counter new, emerging and evolving forms of crime at the national, regional and international levels.

In addition, point 09 subsection (b) proposes to explore specific measures designed to create a secure and resilient cyber environment, to prevent and counter criminal activities carried out over the Internet, to strengthen law enforcement cooperation at the national and international levels.

- HORIZON 2020

It is a financial instrument implementing an innovation-friendly environment aimed at securing Europe’s global competitiveness. It is a six years plan (2014-2020) and its main goal is to create sustainable and inclusive growth jobs, also adapting the European Union to the new tendences of the world.

As a part of this project, it was created a public-private alliance on cyber security in which 450 millions of euros will be destined to impulse new strategies to allow the European Union reinforce against cyber attacks and impulse the competitivity of the European industry on cyber security.

In this way, this investment looks for boosting the confidence on the digital economy by creating small and medium enterprises dedicated to developing software in relation with cyber security. This actions will give assurance to an emerging market, as it is, the digital economy.

- X SUMMIT of LATIN AMERICAN and CARIBBEAN COMMUNITY of POLICE INTELLIGENCE (CLASP)

Latin America also noticed the emerging growth of cybercrime as a national security matter and has made several congresses in order to counter it. Knowing all or most of the existing threats and planning strategies has been the subject of discussion. Also, it is a relation in public-private cooperation in order to attack this problem.

http://www.un.org/ga/search/view_doc.asp?symbol=A/CONF.222/L.6 HYPERLINK "http://www.un.org/ga/search/view_doc.asp?symbol=A/CONF.222/L.6"

This summit was celebrated in Panama and several subjects regarding crime were discussed, including cyber crime. *"The globalization is leading us to a more technological police and the exchange with this type of summits has opened our horizon" (Castillo, 2015)*

Javier Castillo, subdirector of the national police of Panama during the summit also pointed that they are looking forward for the collaboration with Netherlands, United States of America and Spain because of their previous experience on the subject. The commissioner Gilberto Glenn, Director of Police Intelligence of Panama, remarked that cybercrime has gained space on the different working areas nowadays.

- SECURED

The SECURED project proposes an innovative architecture to achieve protection from Internet threats by offloading execution of security applications into a programmable device at the edge of the network such as a home gateway or an enterprise router. It involves 27 EU Member States.

The main objective of SECURED is to design and prototype a credible and secure execution environment in order to create for the users a medium in which they can develop in a safer way. This network was created to protect the user from traffic or different kinds of cyber attacks.

However, all of these measures need to be applied, tested and proved in a national level to reach the international one. The collaboration between States is crucial to create a safe network of transport of confidential information. Unifying efforts in order to achieve a common goal that will benefit all.

- CONVENTION ON CYBERCRIME

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation. Adopted by the Council of Europe in 2015.

Cases of cyber attacks

- SONY PICTURES ENTERTAINMENT

In 2014, the main operational system of Sony Pictures Entertainment was hacked by a group so-called *Guardians of Peace,* this attack robbed several unreleased movies and confidential electronic mails of the company. Also, as a consequence of this perpetration, the company was extorted for the criminals for not to sell the confidential information.

This cyber attack was seen, according to the spokesman of the White House Josh Earnest, as a “serious issue of national security”. The alleged participation of the government of North Korea in the attack was the main accused because of the film *“The Interview”*[8], produced by Sony Pictures Entertainment.

- INDIAN GOVERNMENT AND MILITARY EMAILS HACKED

In 12 July 2012, occurred the biggest cyber attack to India’s history. Over 10,000 emails from top government officials and were hacked on a single day. Confidential information, like IDs of officials working in the Project Management Office (PMO), defence, external affairs, home, finance ministries, as well as intelligence agencies. was stolen that day.

Four days before the attack, the Indian government was warned of several malware introduced into their networks but they ignored it. Different associations dedicated to prevent cyber crime, like National Critical Information Infrastructure Protection Centre (NCIIPC) and National Security Agency (NSA) notified the Indian government.

The government of India qualified this attack in the D4[9] level and named it as a national security matter. All or most of the information of people involved on the government and paramilitary forces were revealed and affected with this attack.

The Indian government has taken different measures to punish and prevent cyber crime, making emphasis on the rule of law. As a punishment, according to the Indian Penal Code, it will give two years of prison to a person captured because of any type of cyber crime. Also proposed a coordination with Data Security Council (DSCI), NASSCOM and Cyber Forensic Labs in order to track down hackers.

- IRAN’S NUCLEAR FACILITY ATTACKED BY STUXNET

Stuxnet is a computer worm, allegedly designed by the government of the United States and Israel, arranged to infiltrate into industrial control systems that are used to monitor and control large scale industrial facilities such as power plants, waste processing systems among others. According to Edward Snowden, former NSA contractor, said that it was created to destroy centrifuges in Iran.

[8] Movie in which is narrated a complot to murder the north korean leader, Kim Jon-un

[9] destroy, disrupt, deny and degrade

In June 2010, Iran's Natanz nuclear facility was infected by Stuxnet. The aim of this attack was to disrupt the nuclear facility in Natanz, Iran. Known as the first cyber attack from one country to another, it has perturbed the international community.

Alex Gibney, who has worked on WikiLeaks, Enron and Scientology believes the secret world of state sponsored cyber warfare has Hiroshima-like consequences for humanity.

> *"The potential threat from these kinds of cyber weapons is huge, especially when you start talking about shutting down electric power grids,"* he said. *"I'm not talking about the threat to me personally, but the threat to all of us. We're just at a point where everyone is starting to recognise the potential calamity."* (Gibney, 2010)

- ANONYMOUS

Anonymous is an organized international movement of online activists who share similar social and political ideals. Anonymous goal is to give access to information, free speech, and transparency, and also supports various anticorruption and anti-authoritarian movements. This group does not has a specific leader.

To understand Anonymous' actions we need to know that they are activists, this refers to a group of persons that express their point of view, in favour or against, towards a controversial subject in an active manner (hence the name, activism). Most of the times, is about a political decision that affects that group of people.

Their movement, so-called "hacktivism", goes against governmental agencies, commercial entities among others. According to their philosophy, they hack the network of the entity, through Internet, they are against to create pressure on the group and make a change, most of their actions are in favour of the freedom of speech and free access to information.

Some examples of Anonymous' attacks are (1)Against the government of Argentina in 2012, (2) Tunisia operation between 2010 and 2011, (3) Against the government of Chile in 2012, (4) Iranian election protests in 2009. Of course, these are not all the attacks this activist group has realized around the world but is an example of their scope.

Moreover, cyber crime is a problem that not only affects a single entity, sector or group, it has shown that it can alter a whole country in social, economic and political aspect. From private sector to public sector, both have to collaborate in order to track down these perpetrators that attempt to the national security of different countries.

The role of the governments towards this problem is to create jurisdiction and laws, in national and international level, in order to respect the rule of law and safeguard their national integrity. Since the new tendencies of the world mark the use of technologies and Internet, States have to prepare to all the dangers and mitigate, as long as possible, this emerging crime.

Impact of cybercrime

This emerging crime has different perspectives and different reasons to be carried out. It is important to remark that this problem has three main perspectives in which affects the international community. The following points will explain how cybercrime affects in the social, economic and political level to the international community.

This issue has shown that it can have different perspectives and involves every sector of the society. Since it affects both sectors, it is essential a public-private collaboration in order to respond to this crime. First working from the national level to reach an international level.

- SOCIAL

The impact on the society is the fear and uncertainty in relation of the cyber attacks can occur at any moment. According a report of EFE AGENCY of 2015, 43.3% of the whole global population has access to internet. The difference varies between developed country, developing countries and other countries denominated "least developed".

Moreover, the access to Internet per home is, on developed countries, 81.3%, developing countries, 34.1% and finally 6.7% in least developed countries. In fact, the number of users of Internet in developing countries has doubled in the last lustrum (2010-2015).

Taking into consideration these numbers, it means that there are more than 3,000 million of people connected to Internet, sharing and exchanging information, and people that can hack into the personal information of the population is the greatest impact on society in relation with the use of Internet.

The interception of personal information and after the extortion using that information is a problem with the use of Internet and flow of data. Also, bank accounts and assurances have been assaulted by cyber attacks.

It is needed plans that answer to this problem in a short, medium and long term in order to create national and international legislation that totally respects the rule of law and national sovereignty of each Member State. Taking into consideration the measures already taken and how the international community has responded to them.

- ECONOMIC

"Cyber Crime Is The Greatest Threat To Every Company In The World", these were the words that IBM's CEO used to refer to hackers nowadays. According to the report of the World

Economic Forum (WEF) affirms that a great part of cyber crime goes undetected, especially, industrial espionage.

On the same report shows that cybercrime is estimated to cost the global economy more than USD $400 billion a year by losses of economic assets by criminals. These costs are expected to continue to rise. Actually, by 2019, it is projected that the economic impact of cybercrime rise until USD $2 trillion a year (WEF, 2016).

Similarly, a cyber attack can devastate a whole country's economy by hacking and sabotaging the national finance and stocks, and no one will know who was the guilty, since cyber crime shows no face, cyber attacks to government's facilities are a common target of attackers. Also, the attack of a private company has a direct impact on the public sector, so it concerns to both sectors measures to respect the rule of law in relation with cyber crime.

On the other hand, there are other assets that can be lost and in a long term, create a sort of economic damage. For example, the loss of intellectual property, theft of financial assets and sensitive business information, additional costs for securing networks, the reputational damage to the hacked company.

> *"We believe that data is the phenomenon of our time. It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true – even inevitable – then cyber crime, by definition, is the greatest threat to every profession, every industry, every company in the world."* (Rometty, 2016)

- POLITICAL

As it was mentioned before, a type of cyber warfare is online espionage and according to a report of U.S. Agency of International Development[10], it is demanded by a State to gain some kind of advantage over a competing adversary. This problem generates distrust between States all around the world.

Also, we need to consider that there are internal and external cyber attacks and both affect and create uncertainty in all the levels of the government. The internal threats refer to an internal employee who caused great damage to the government from the inside and external is, as previously mentioned, an attack from a third party using Internet to enter into a nation's networks.

[10] Cyber Crime: Its Impact on Government, Society and the Prosecutor: http://pdf.usaid.gov/pdf_docs/Pnada641.pdf HYPERLINK "http://pdf.usaid.gov/pdf_docs/Pnada641.pdf"

Governments, supposedly had contracted hackers in order to make an intromission into others nations' networks and gain an advantage in the international market. Likewise, any State has openly accepted the intromission into others country's networks. This problem refers to online espionage and online sabotage, however, the Internet already plays an important role on the international arena.

Another key thing to remember is to respect the rule of law of every single country in order to create legislation that suits to each country. Fighting cyber crime must be a common goal to achieve between governments and the collaboration between States is essential, always respecting the rule of law and seeking for the criminal justice to be accomplished.

It is important to add that national and international judicial systems need to be adapted to the new global tendencies in order to punish this crime, making emphasis on cyber warfare. Taking into consideration that a violation into the different governments' networks is an aggression to the national security and integrity to the country, it must be punished with all the weight of the law.

References

1. UNODC. (2016). Commission on Crime Prevention and Criminal Justice. Retrieved 01 July 2016. From https://www.unodc.org/unodc/en/commissions/CCPCJ/
2. UNICRI. (n.d.) . Cyber threats. Retrieved 03 July 2016. From http://www.unicri.it/special_topics/securing_cyberspace/cyber_threats/explanations/
3. McAfee Center of Strategic and International Studies (2013) The economic impact of cybercrime and cyber espionage. Retrieved 03 July 2016. From https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf
4. UNICRI. (n.d.) .Cybersecurity and Technology Misuse. Retrieved 03 July 2016. From http://www.unicri.it/special_topics/securing_cyberspace/
5. Lennon, Mike. (2015). Attacks Against SCADA Systems Doubled in 2014: Dell. Retrieved 03 July 2016. From http://www.securityweek.com/attacks-against-scada-systems-doubled-2014-dell
6. UNICRI. (n.d). Current Activities. Retrieved 03 July 2016. From http://www.unicri.it/special_topics/securing_cyberspace/current_activities/
7. Dell. (2015). Dell Security Annual Threat Report. Retrieved 03 July 2016. From https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf
8. Kesler, Brent. (2011). The Vulnerability of Nuclear Facilities to Cyber Attack. Retrieved 04 July 2016. From http://large.stanford.edu/courses/2015/ph241/holloway1/docs/SI-v10-I1_Kesler.pdf
9. Nuclear Energy Institute. (2016). Policy Briefs-Cyber Security for Nuclear Power Plants. Retrieved 04 July 2016. From: http://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-Strictly-Regulated-by-NRC;-No-Addit
10. Pariyani, Rakesh. (2013). On-line-crimes and their impacts. Retrieved 04 July 2016. From: http://www.manupatra.co.in/newsline/articles/Upload/779E337A-DDF8-41AE-ACA4-89F3CB746F2D.pdf
11. Schneier, Bruce. (2014). There's No Real Difference Between Online Espionage and Online Attack. Retrieved 04 July 2016. From:

http://www.theatlantic.com/technology/archive/2014/03/theres-no-real-difference-between-online-espionage-and-online-attack/284233/

12. Informador. (2014). Ciberataque a Sony, grave asunto de seguridad nacional: Casa Blanca. Retrieved 05 July 2016. From: http://www.informador.com.mx/entretenimiento/2014/566038/6/ciberataque-a-sony-grave-asunto-de-seguridad-nacional-casa-blanca.htm
13. UN News Centre. (2015). UN conference weighs efforts to combat cybercrime, create safer digital world. Retrieved 06 July 2016. From: http://www.un.org/apps/news/story.asp?NewsID=50610#.V31QaLjhDtQ
14. Commission on Crime Prevention and Criminal Justice. (2015). Thirteenth United Nations Congress on Crime Prevention and Criminal Justice. Retrieved 07 July 2016. From: http://www.un.org/ga/search/view_doc.asp?symbol=A/CONF.222/L.6
15. European Commission. (2014). What is Horizon 2020?. Retrieved 07 July 2016. From: https://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020
16. Cinco días. (2016). Bruselas destina 450 millones para reforzar a Europa contra los ciberataques. Retrieved 07 July 2016. From: http://cincodias.com/cincodias/2016/07/05/tecnologia/1467721879_002980.html
17. Sin Embargo, equipo de Redacción. (2015). Policías de América unen esfuerzos para combatir trata personas y cibercrimen. Retrieved 07 July 2016. From: http://www.sinembargo.mx/13-08-2015/1448818
18. Ajmer Singh, The Indian Express. (2012). Over 10,000 email IDs hit in 'worst' cyber attack. Retrieved 09 July 2016. From: http://archive.indianexpress.com/news/over-10000-email-ids-hit-in-worst-cyber-attack/1046874/
19. Press Information Bureau, Government of India, Ministry of Women and Child Development. (2015). Several steps taken by the Government to prevent cyber crimes including those against women . Retrieved 09 July 2016. From: http://pib.nic.in/newsite/PrintRelease.aspx?relid=132545
20. Michael B Kelley. (2013). The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought. Retrieved 10 July 2016. From: http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11
21. Rand Corporation. (2014). Cyber Warfare. Retrieved 11 July 2016. From: http://www.rand.org/topics/cyber-warfare.html
22. REUTERS. (2016). Economic espionage a 'tremendous problem' -U.S. attorney

general. Retrieved 12 July 2016. From: http://www.dailymail.co.uk/wires/reuters/article-3664769/Economic-espionage-tremendous-problem-U-S-attorney-general.html

23. EFE Editors. (2015). Un 43,3 % de la población mundial tiene acceso a internet. 12 July 2016, Retrieved: EFE AGENCY From: http://www.efe.com/efe/america/tecnologia/un-43-3-de-la-poblacion-mundial-tiene-acceso-a-internet/20000036-2777245
24. Center for Strategic and International Studies. (2014). Net Losses: Estimating the Global Cost of Cybercrime; Economic impact of cybercrime II. 12 July 2016. Retrieved: Intel Security. From: http://www.cyberriskinsuranceforum.com/sites/default/files/pictures/rp-economic-impact-cybercrime2.pdf
25. Morgan, Steve. (2016). Cyber Crime Costs Projected To Reach $2 Trillion by 2019. 12 July 2016. Retrieved: Forbes. From: http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#59ae7d7f3bb0
26. Morgan, Steve. (2015). IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World'. 12 July 2016. Retrieved: Forbes. From: http://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#747954f13548
27. Dr. Nicholas Gilmour. (2015). Why we need new ideas in the fight against cybercrime. 12 July 2016. Retrieved: World Economic Forum. From: https://www.weforum.org/agenda/2015/03/why-we-need-new-ideas-in-the-fight-against-cybercrime/
28. U.S. Agency of International Development. (2015). Cyber Crime: Its Impact on Government, Society and the Prosecutor. 12 July 2016. Retrieved from: http://pdf.usaid.gov/pdf_docs/Pnada641.pdf

Glossary

B

Backdoors (malware): A backdoor is a technique in which a system security mechanism is bypassed undetectably to access a computer or its data.

Breeding ground: A place where something develops easily, especially something unpleasant

C

Copyright: The right to use or make copies, licenses or any type of work from any work or project created from an other person that it is actually protected.

Cyber warfare: Activity of using the internet to attack a country´s computers in order to damage things such as communication and transport.

E

Espionage: The activity of discovering secret information about a country that is fighting or competing

H

Hacking: The activity of using a computer illegally to get into another computer system to read the information kept

Hacktivism: The activity of getting into the computer systems without permission in order to achieve political aims.

I

Infiltrate: To secretly become part of a group in order to get information or to influence the way that group thinks or behaves.

Intellectual property: Someone's idea, invention, creation, etc., that can be protected by law from being copied by someone else

Intromission: Getting deeper/insider a situation

M

Malware: It is any type of malicious software that tries to damage a computer, phone or tablet. It is mostly used to steal personal information, money, among others.

Mugger: A person who attacks people in order to steal their money

P

Policymaking: The activity of deciding on new policies, especially by a government or political party.

R

Regarding: It is and expression in which it refers of taking in consideration an issue or aspect

Rule of law: It's a system in which 4 principles are upheld:

- Everyone (government, private entities as well as individuals) is accountable under the law.
- The laws are clear, just, and stable. They are applied evenly, and protect fundamental rights.
- The law's enactment process is accessible, efficient, and fair.
- Justice is delivered competent, ethical representatives who have adequate resources, and reflect the communities they serve.

T

Transnational: Involving several nations

Transnational Organized Crime: Refers to those self-perpetuating associations of individuals who operate not only in one state for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part illegal means.

Trojan Horse: A computer program that has been deliberately designed to destroy information, or allow someone to steal it.

V

Virus: Small software programs that spread from one computer to another, and interfere with computer operation.

W

Worms: A computer worm is a self-replicating computer program that penetrates an operating system with the intent of spreading malicious code. Worms utilize networks to send copies of files to other computers.

Topic B

Illegal traffic of precious metals on the European Union and its role as a source to finance organized transnational criminal groups

By: José Antonio Martínez Caldera

Introduction

According to the 25th CRIME COMMISSION TO FOCUS ON CRIMINAL JUSTICE RESPONSES TO TERRORISM, the increasing circumstance of illicit trafficking in precious metals in the European Union takes advantage of the loopholes in the national and international legislation. This kind of metals represent ideal commodities for funding criminal activities because of their effortless movability and high value on the market. Also, the European Union has no law enforcement towards this emerging global crime.

Taking into consideration the resolution 2013/38 of the Economic and Social Council, more specifically, point two which establishes *"Invites Member States to consider utilizing the United Nations Convention against Transnational Organized Crime in combating transnational organized crime and its possible links to illicit trafficking in precious metals;"*. It is important to remark the actual measures taken by the international community in order to collaborate to find solutions in the short and long term.

Knowing that precious metals are those that are found in nature and are not combined with other metals and they have a big value, as long as these metals are used for art, jewelry and coinage. Some examples are gold, silver, rhodium, platinum, palladium among others, they have a great value on the market.

Member States are exhorted to cooperate in order to attack a common problem on their agenda, as it is trafficking of precious metals, that has as consequence the financing to criminal groups. However, this criminal groups have different sources for obtaining money, the precious metals are high valued on the market.

This issue makes part of some of the varieties that "*Global Maritime Crime*" has and the interlinked levels of organized criminal actors that operate within and across national and international borders. It is important to remark that there are several crimes related with mining of precious metals e.g. corruption, money laundering, linkage with other criminal or terrorist group.

Financing organized transnational criminal groups is an affair that should be taken into consideration. As long as the measures taken to prevent crime have not been efficient, it is necessary to collaborate between Member States of the European Union in order to work on criminal justice and respect the national and international rule of law. Making emphasis on maritime law.

Role of precious metal in history

Throughout history, precious metals have been high valued because of their natural beauty and radiance, they are considered as a symbol of purity, value and royalty (Asociación Española de los Metales Preciosos, N.D). The precious metals can not be mixed or combined with other metals and they are rare to find.

Nowadays, precious metals like gold or silver are used as the standard for currency worldwide and jewelry and fine jewelry creates great demand of these metals, because of their shortage, they are high demand on this field.

According to World Gold Council (WGC), at the end of 2015, the demand of jewelry accounted for 57% of gold. The same council remarked that the tendence about gold is to give gold as a gift to mark festivals and weddings. The relevance of gold, one of the principal and most famous precious metals, has been remarkable and tends to mark a celebration.

Illicit trafficking of precious metals

Gold, silver and the Platinum Group Metals (PGM)[11] are are the ones addressed by United Nations Interregional Crime and Justice Research Institute (UNICRI) in order to face this emerging crime as a source of financing transnational criminal groups. The lack of coordination in the national and international levels creates gaps that these criminal groups take advantage.

According to the *Desk Review*[12] established by UNICRI in order to counter the illicit trafficking of precious metals says that the extraction of precious metals can be divided in three mining scales, (1) Artisanal Small-Scale Mining (ASM), (2) Small Scale Mining (SSM) and (3) Large Scale Mining (LSM).

ASM consists on a manual work done by small groups of miners, normally this activity is only made for local markets and local consume. SSM is a more mechanized process in which some machine are used without reaching an international level; the manual work here comes to a diminution. Finally LSM that consists on high level of technology used by international companies of mining and its goal is to reach the international market.

However, most of the countries that produce and extract the precious metals do not have the infrastructure. A group of gold and PGM refiners are located on non-mining countries,

Platinum Group Metals: Platinum, Palladium, Rhodium, Ruthenium, Iridium and Osmium.

[11]

[12] Desk review: http://www.unicri.it/special_topics/metals_gemstones/Preliminary_Desk_Review.pdf HYPERLINK "http://www.unicri.it/special_topics/metals_gemstones/Preliminary_Desk_Review.pdf"

this creates the necessity to transport the unrefined and semi-refined metals to other places. This is used by criminal groups to intercept the ships. (UNICRI, N.D.)

According to the *Technical Assistance Report Anti Corruption and Anti-Money Laundering of the International Monetary Fund* [13] (IMF), illicit trafficking of precious metals and money laundering are strongly linked because the gold can be used as money in the laundering systems based on commercial transactions.

Actors involved

According to UNICRI, there are five main actors involved on the trafficking of precious metals. UNICRI has made this division in order to know all the interlinked levels of organized crime, all the agents involved, intermediary companies and buyers and bulk buyers on the national and international levels.

- LEVEL I

This level refers to the manual illegal extraction of precious metals, most of the times are immigrants or other workers from neighbour countries that previously worked on that underground mine (Known by UNICRI as runners). The metals extracted are not totally refined because of the lack of infrastructure and machine work they employ.

- LEVEL II

On this level attributes to the people who buy, in a small scale, the precious metals extracted by the people of level I (Known by UNICRI as middlemen). According to UNICRI, they give some kind of logistical support (protection, food, materials, transport etc…) in order to take away the metals from the mines. And later on, they sale it to national traders of metals.

- LEVEL III

On the third level, the national buyers can get the precious metals from two sources, by runners or middlemen. The advantage from middlemen are the quality and the quantity they can give to this buyer. However, these national buyers sell all the precious metals to the next level of hierarchy. Their job is to transport the product to wealthy syndicate traders.

- LEVEL IV

The fourth level the local syndicate buyer process, contains and packages the product in order to be smuggled to national. regional or international traders. The metals are put into bags,

Technical Assistance Report-Anti-Corruption and Anti-Money Laundering, 2015: https://www.imf.org/external/pubs/cat/longres.aspx?sk=43077.0 HYPERLINK "https://www.imf.org/external/pubs/cat/longres.aspx?sk=43077.0" weighed and after, sold. When the metal is on the ship, sometimes they use legitimate companies or front companies, they falsify the information about the cargo.

- LEVEL V

Finally the last level is the transnational criminal traders of precious metals. On this level, they use legitimate companies in order to refine the metals illegally. These entities are capable of dealing with national and international imports and exports, this creates the international market of precious metals.

According to *Freedom from Fear*[14], establishes that the success of these illegal market depends on the highly sophisticated export routes, participation of some governments and global companies. There is no specific national or international legislation in order to punish and respect the rule of law.

Transnational Organized Crime

According to UNODC, the organized crime threatens peace and human security, violates human rights and undermines economic, social, cultural, political and civil development of societies around the world. The transnational organized crime manages a huge quantity of money worldwide and costs a great amount of innocent lives. (UNODC, N.D.)

Organized crime has reached an international level and has approached to damage macroeconomic aspects such as trafficking, illicit good can be transported from one continent to another, permeating government agencies, corruption and infiltrating in business and politics (UNODC, N.D)

According to the National Security Council of the United States of America (NSC) ensures that the transnational organized crime damage the public safety, public health, democratic institutions and economic stability all around the globe. Due to the criminal networks that are expanding, also the diversification of activities from these groups.

The interests of transnational criminal groups have infiltrated into the government levels in order to obtain several benefits, this is often accomplished through direct bribery; setting up shadow economies; infiltrating financial and security sectors through coercion or corruption; and positioning themselves as alternate providers of governance, security, services, and livelihoods.

In other words, NSC assure that developing countries are more susceptible to be infiltrated into their levels of governance because of the weak rule of law they have. The Illicit

Illicit trafficking of precious metals and its destabilizing factors in systems of affected countries: http://f3magazine.unicri.it/?p=598 HYPERLINK "http://f3magazine.unicri.it/?p=598"

Financial Flows (IFF) of money is undercutting the sustainable development of society and creating, particularly, damage in the context of weak and developing States, according to *The Global Initiative Against Transnational Organized Crime* [15].

- GLOBAL MARITIME CRIME

Crime is also present on the ocean and sea, and it represents a huge threat to sailors, traders, tourists and seafarers. Taking into consideration that most of the commercial trades and business are made by sea and the increasing rate of maritime crime damages this economic activity. Using the high seas in order to perpetuate transnational organized crimes.

As previously mentioned, countries producers of precious metals not always have the facilities or infrastructure to refine and purify them, hence, they must send them to other countries like United Kingdom, Belgium, Italy among others. For instance, the transport of precious metals in an unrefined way makes them a perfect target for criminal groups.

According to *Freedom from Fear*, countries like South Africa and China have no capabilities to refine and purify the precious metals they produce. Those countries send them to European countries. However, in the mean term, the cargo is intercepted by criminal groups and then sold to the Black Market.

Maritime law

According to the University of Southampton (N.D), the maritime law deals with the commercial, regulatory, insurance and environmental aspects of trade. Furthermore it handles with the competition between States for marine living and nonliving resources which create friction and possibly conflicts.

This area of law involves different aspects in the rule of law, e.g. contracts, bailment, tort among others. Also, it has to deal with different international and regional conventions as well as it comprehends two or more States in order to safeguard shipping and commercial routes of both parts.

In 2015, UNODC established the *Global Maritime Crime Programme* [16] in order to work on law enforcements that ensures that seas are not a safe space for criminals. This

Illicit Financial Flows: http://globalinitiative.net/programs/financial/ HYPERLINK "http://globalinitiative.net/programs/financial/"

Global Maritime Crime Programme: https://www.unodc.org/documents/Piracy/15-07385_AR_ebook_Small.pdf HYPERLINK "https://www.unodc.org/documents/Piracy/15-07385_AR_ebook_Small.pdf"

16

programme has as main goal eradicate the impunity on the seas in order to track down transnational threats, such as trafficking and smuggling.

Industries affected

According to the International Maritime Organization (IMO) the international maritime commerce must be efficient and fair, always seeking for internationality. According to IMO, the maritime commerce represents approximately 80% of the global transport of goods, also being the most efficient, cheapest and safest.

For instance, the presence of maritime criminals disturbs the commercial interaction between nations. Affecting the sustainable development of society by creating insecurity on the principal commercial routes. Taking into consideration that some of the precious metals produced on the European Union are transported by sea, but not only the countries producers of precious metal, also there are countries on the European Union that are dedicated to refine metals to purity.

IMO affirms that in view of this situation, criminal groups intercept the ships with these metals unrefined or semi-refined and it makes easier to pass undetected through regional and international borders. However, maritime law has no specific legal coordination between States in order to punish these organized criminal groups all around the world.

Furthermore, according to UNICRI, the mining industry is the principal affected by this crime because of the illicit extraction of these metals. Most of these perpetrations are made by ASM because it requires only manual work in a small scale activity, however, this represents a cost for mining companies.

According to *Precious Metals Program* by UNICRI [17], the illegal traffic of gold represents tax scams. For example, companies gold or any other precious metal as an export-tax rebate.

Countries dedicated to precious metals

According to *World Mining Data 2016*[18], the raw precious metals that are produced by the top mining countries are gold, PGM and silver. Also, the data gathered by World Mining Congress

Precious Metals Program-Tax scams: https://pm.unicri.it/pm-public-portal/case-studies-database/tax-scams HYPERLINK "https://pm.unicri.it/pm-public-portal/case-studies-database/tax-scams"
17
World Mining Data, 2016: http://www.wmc.org.pl/sites/default/files/WMD2016.pdf HYPERLINK "http://www.wmc.org.pl/sites/default/files/WMD2016.pdf"

(WMC) affirms that the plentiful supply of minerals and other raw materials under a fair market conditions is essential for a well.functioning of economy.

Also, WMC accepts the global challenges of the mining industry of precious metals and the importance of collaboration between States in order to work in regional and international legislation in order to make this economic activity grow.

In order to participate in the international arena, the European Union has established the "European Innovation Partnership (EIP) on Raw Materials". Its purpose is to provide high-level guidance to Member States on innovative approaches related to raw materials in the national and regional level.

- RUSSIA (PRODUCER-REFINER)

According to *Thomas White International* [19], one of the branches in which mining industry is based are the precious metals. According to the same report, the mining industry in Russia constitutes iron, steel, aluminium and precious metals, also having a great reserve of PGM (Platinum Group Metals).

Also the mining industry plays an important role on Russia's economy, according to *Thomas White International,* it consists on a 14% of exports, just below of natural gas and oil. It is important to remark that since the decade of 1990's, the mining industry has being privatized.

The gold production on Russia has had a constant growth in the past six years. According to *Union of Gold Producers in Russia* in the examination of the gold mining during 2013 and 2014[20], between 2008 and 2014[21] the production of gold increased 66.8 mined tonnes. By adding the Byproduct and Secondary we have an increase of 98.2 tonnes of gold produced.

- UNITED KINGDOM (REFINER)

According to the British Geological Survey, United Kingdom has lost its potential of mining on the last century and the ores left on that territory have not the potential to cover the global

[18] Sitting on a Gold Mine: Metals and Mining in Russia: http://www.thomaswhite.com/global-perspectives/sitting-on-a-gold-mine-metals-and-mining-in-russia/ HYPERLINK "http://www.thomaswhite.com/global-perspectives/sitting-on-a-gold-mine-metals-and-mining-in-russia/"

[19] Overview of the gold mining industry in Russia in 2013-2014: http://investinrussia.com/data/files/sectors/0_EY-gold-mining-industry-in-russia.pdf HYPERLINK "http://investinrussia.com/data/files/sectors/0_EY-gold-mining-industry-in-russia.pdf"

[20] In 2008 were mined 163.9 tonnes and in 2014 were 230.7 tonnes

[21]

demand of precious metals. However, the gold and silver mining industry are still working on this territory.

Moreover, according to a report from *The Telegraph*[22] the outsourcing of mining companies looks more profitable than doing it on United Kingdom's territory because of the abundance and availability of precious metals. In addition, on 2008, the so-called last mine of gold and silver was reopened because, according to *The Guardian*[23] of the high value of gold and silver on the market.

- SWEDEN (PRODUCE-REFINER)

According to a Geological Survey of Sweden in 2015, it is the leader country on ore mines and metal producers of the European Union. According to SveMin, in 2012 Sweden is part of the top suppliers of silver for the European Union. In accordance with the same report of SveMin, since mining is seen as a key part for a sustainable development, it contributes in a great amount to the national GDP.

According to EuroMine Expo, the northern part of Europe, including Sweden, have a huge amount mines that are underexploited. The international community has worked to find a way in which mining industry becomes a vital force in national, regional and international development.

However, these are just a few examples of countries dedicated to the mining industry of precious metals, it is a problem regarding the European Union and it is relevant a collaboration between States in order to cover and solve the loopholes on international legislation and respect the rule of law of Member States.

Main sources of financing of criminal groups

Transnational criminal groups have reached a huge economic power (UNODC, 2011). Some of the activities in which these groups earn money are from narcotraffic, smuggling, extortions

[22] Questor share tip: Randgold Resources gold shares soar on solid results: http://www.telegraph.co.uk/business/2016/02/18/questor-share-tip-randgold-resources-gold-shares-soar-on-solid-r/ HYPERLINK "http://www.telegraph.co.uk/business/2016/02/18/questor-share-tip-randgold-resources-gold-shares-soar-on-solid-r/"

UK's last gold mine set to reopen: https://www.theguardian.com/business/2008/jun/29/mining1 HYPERLINK "https://www.theguardian.com/business/2008/jun/29/mining1"

23

and trafficking (UNODC, 2011). According to UNODC, the earnings of these so-called business is of 2.1 billion dollars a year.

According to TERRORIST FINANCING from Financial Action Task Force (FATF)[24], transnational criminal groups raise funds through: legitimate sources, including through abuse of charitable entities or legitimate businesses and self-financing, criminal activity, state sponsors and activities in failed states and other safe havens.

However, these types of funding can be divided in two; (1) from above: in which large-scale financial support is aggregated centrally by states, companies, charities or permissive financial institutions; (2) from below: in which terrorists fundraising is small-scale and dispersed, for example based on self-financing by the terrorists themselves using employment or welfare payments.

Moreover, *The Global Initiative Against Transnational Organized Crime* affirms that gold plays a significant role on the Illicit Financial Flow (IFF) as a source of the high profit-low risk nature of the gold trade makes. The same organization highlighted that gold represents an attractive financial solution for engaging in anonymous financial transactions, moving illicit funds, and laundering money.

According to *Havoscope*[25], trafficking of metals represents an income to criminal groups of USD 2.3 billion in 2013. Having gold as the main precious metal involved in most of the cases.

Precious metals legislation

In accordance with UNICRI, Member States have noticed that the illegal traffic of precious metal is linked to other forms of crime such as terrorism, trafficking of weapons, smuggling of migrants inter alia. Taking this into consideration, Member States have to collaborate in order to create laws in national level in order to reach the regional and international level in order to punish this crime.

- UNITED NATIONS CONVENTION AGAINST CORRUPTION

With the objective of prevent and improve the capacity to cooperate between the States parties, the General Assembly adopted the “United Nations Convention Against Corruption” on

Terrorist financing: http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf HYPERLINK "http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf"

24

Metals and minerals smuggling: http://www.havocscope.com/tag/metals-and-minerals/

October 2003 at the UN Headquarters in New York. It shall be open to all States for signature from 9 to 11 December 2003 in Merida, Mexico, and at the UN Headquarters until 9 December 2005.

During this convention, three main points were highlighted, (1) Promote and strengthen measures to prevent and combat corruption more efficiently and effectively, (2) Promote, facilitate, and support international cooperation and technical assistance in the prevention of and fight against corruption, including in asset recovery and (3) Promote integrity, accountability and proper management of public affairs and public property. Key words: **Prevention, Criminalization, International cooperation, Asset recovery**

- 25th CRIME COMMISSION TO FOCUS ON CRIMINAL JUSTICE RESPONSES TO TERRORISM

In 2016, during this session of Commission on Crime Prevention and Criminal Justice (CCPCJ) was debated the criminal justice responses to prevent and counter terrorism in all of its forms and manifestations. Member States and international organizations, like United Nations Interregional Crime and Justice Research Institute (UNICRI) or International Centre for Criminal Law Reform and Criminal Justice Policy (ICCLR), participated on this commission.

For instance, the international community have realized the emerging impact of transnational criminal groups on the different sectors of society. These criminal groups have reached an international level and is a problem that affects the Member States by countering through cutting off their finances and confronting the crimes committed, as established during the commission.

Also during the commission was highlighted the relevance of locate and reduce the sources of financing and establish a global strategy in order to cut and attack transnational crime in all of its manifestations all around the world.

References

1. UNODC. (N.D.). Commission on Crime Prevention and Criminal Justice. Retrieved 01 July 2016. https://www.unodc.org/unodc/en/commissions/CCPCJ/
2. UNICRI. (2016). Technical Report on Strengthening the Security and Integrity of the Precious Metals Supply Chain. 16 July 2016, from: UNICRI website: http://www.unicri.it/news/article/2016-05-25_Technical_Report_on_Strengthening
3. AreaCiencias Equipo de edición. (N.D.). METALES PRECIOSOS. 17 July 2016, From AreaCiencias Website: http://www.areaciencias.com/geologia/metales-preciosos.html
4. Southampton Law School . (2016). LLM Maritime Law - 1 yr(s). 18 July 2016, From University of Southampton Website: http://www.southampton.ac.uk/law/postgraduate/taught_courses/courses/LLM_maritime_law.page
5. IMO. (2016). Introduction to IMO. 18 July 2016, From International Maritime Organization Website: http://www.imo.org/es/About/Paginas/Default.aspx
6. Elias B. Rudnikas. (2014). Derecho marítimo y delitos en alta mar. 18 July 2016, From: LeyMaritima Web: http://www.leymaritima.com/derecho-maritimo-y-delitos-en-alta-mar/
7. Legiscomex. (2007). El mercado de Joyeria en Europa. 18 July 2016, From PROEXPORT COLOMBIA Website: http://antiguo.proexport.com.co/vbecontent/library/documents/DocNewsNo8844DocumentNo7295.PDF
8. Pérez, Ana Lilia. (2011). Crimen organizado trasnacional: ganancias y lavado a la alza. 19 July 2016, de CONTRALÍNEA Sitio web: http://www.contralinea.com.mx/archivo-revista/index.php/2011/11/24/crimen-organizado-trasnacional-ganancias-y-lavado-al-alza/
9. UNODC. (N.D). Organized Crime. 19 July 2016, de UNODC Sitio web: https://www.unodc.org/unodc/en/organized-crime/index.html
10. OECD. (2008). Financial Action Task Force . 19 July 2016, de FATF Sitio web: http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf

11. WGC. (2016). Global gold jewellery market. 19 July 2016, de World Gold Council Sitio web: http://www.gold.org/jewellery/global-gold-jewellery-market
12. Urban-Klaehn, Jagoda. (2014). Gold in Poland - How much Gold is there in Goldwasser?. 19 July 2016, de Polishsite Sitio web: http://www.polishsite.us/index.php/history-and-people/history-16th-18th/472-gold-in-poland-how-much-gold-is-there-in-goldwasser-.html
13. National Security Council of the United States of America. (N.D). Transnational Organized Crime: A Growing Threat to National and International Security. 20 July 2016, de National Security Council Sitio web: https://www.whitehouse.gov/administration/eop/nsc/transnational-crime/threat
14. Programs . (2015). Illicit Financial Flows. 20 July 2016, de The Global Initiative Against Transnational Organized Crime Sitio web: http://globalinitiative.net/programs/financial/
15. GIFF and Elle Lev. (2015). GIFF: Illicit Financial Flows from Gold. 20 July 2016, de The Global Initiative Against Transnational Organized Crime Sitio web: http://globalinitiative.net/portfolio-posts/giff-illicit-financial-flows-from-gold/
16. Council on Foreign Relations. (2013). The Global Regime for Transnational Crime. 20 July 2016, de Council on Foreign Relations Sitio web: http://www.cfr.org/transnational-crime/global-regime-transnational-crime/p28656
17. UNICRI. (2015). Illicit Traffic in Precious Metals and Traceability and Ethical Origin of Coloured Gemstones. 21 July 2016, de UNICRI Sitio web: http://www.unicri.it/special_topics/metals_gemstones/
18. Bishop, Peter. (2016). Illicit trafficking of precious metals and its destabilizing factors in systems of affected countries. 21 July 2016, de Freedom From Fear Sitio web: http://f3magazine.unicri.it/?p=598
19. Desk Review by UNICRI. (2015). Promoting an international strategy to combat illicit trafficking in precious metals . 21 July 2016, de UNICRI Sitio web: http://www.unicri.it/special_topics/metals_gemstones/Preliminary_Desk_Review.pdf
20. UNICRI. (N.D). The Challenge. 22 July 2016, de UNICRI Sitio web: https://pm.unicri.it/content/challenge
21. Thony, Jean-Francois. (2002). MONEY LAUNDERING AND TERRORISM FINANCING: AN OVERVIEW . 23 July 2016, de International Monetary Fund Sitio web: https://www.imf.org/external/np/leg/sem/2002/cdmfl/eng/thony.pdf

22. UNODC. (2016). 25th Crime Commission to focus on criminal justice responses to terrorism. 23 July 2016, de UNODC Sitio web: https://www.unodc.org/unodc/en/frontpage/2016/May/25th-crime-commission-to-focus-on-criminal-justice-responses-to-terrorism.html
23. UNICRI. (N.D.). Illicit Traffic in Precious Metals and Traceability and Ethical Origin of Coloured Gemstones. 23 July 2016, de UNICRI Sitio web: http://www.unicri.it/special_topics/metals_gemstones/
24. UNODC. (2015). GLOBAL MARITIME CRIME PROGRAMME: Annual Report 2015. 25 July 2016, de UNODC Sitio web: https://www.unodc.org/documents/Piracy/15-07385_AR_ebook_Small.pdf
25. ICCLR. (2016). 25th Session of the UN Commission on Crime Prevention and Criminal Justice. 25 July 2016, de International Centre for Criminal Law Reform and Criminal Justice Policy Sitio web: http://icclr.law.ubc.ca/topics/25th-session-un-commission-crime-prevention-and-criminal-justice
26. UNODC. (2016). 25th Crime Commission to focus on criminal justice responses to terrorism. 25 July 2016, de UNODC Sitio web: https://www.unodc.org/unodc/en/frontpage/2016/May/25th-crime-commission-to-focus-on-criminal-justice-responses-to-terrorism.html
27. Thomas White International. (2011). Sitting on a Gold Mine: Metals and Mining in Russia. 03 August 2016, de Thomas White International Sitio web: http://www.thomaswhite.com/global-perspectives/sitting-on-a-gold-mine-metals-and-mining-in-russia/
28. Federal Office of Police fedpol. (N.D.). Money Laundering Reporting Office Switzerland (MROS). 03 August 2016, de Swiss confederation Sitio web: https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/geldwaescherei.html
29. Khrustalev, Evgeni . (2015). Overview of the gold mining industry in Russia in 2013-2014. 03 August 2016, de Union of Gold Producers of Russia Sitio web: http://investinrussia.com/data/files/sectors/0_EY-gold-mining-industry-in-russia.pdf
30. Kelbie, Paul. (2008). UK's last gold mine set to reopen. 04 August 2016, de The Guardian Sitio web: https://www.theguardian.com/business/2008/jun/29/mining1
31. SveMin. (2012). A vision of growth for the Swedish mining industry. 05 August 2016, de SveMin Sitio web: http://www.svemin.se/MediaBinaryLoader.axd?MediaArchive_FileID=41275b65-4979-4c39-bdb5-34053a57e6b7

32. C. Reichl, M. Schatz, G. Zsak. (2016). WORLD-MINING-DATA. World Mining Congress, Volume 31, 255. 09 August 2016, De World Mining Data 2016 Base de datos.

Glossary

A

Asset: Something that a person or company owns that has a value.

B

Bailment: The right to take possession temporarily of someone else's property.

Bulk buyers: A person that buys in a high amount

C

Coinage: A set of coin of different values used in a country`s money system.

Commodity: A product that you can buy or sell.

E

Exhort: To strongly encourage someone to do something.

H

Hierarchy: A system or organization in which people or things are arranged according to their importance.

I

Illicit: Illegal, an action not allowed by the law

L

Loophole: A mistake in an agreement or law which gives someone the chance to avoid having to do something.

M

Macroeconomic: The financial and economic systems of a country

O

Outsourcing: A situation in which a company employs another organization to do some of its work, rather of using its own employees to do it

S

Smuggle: To take something into or out of a place in an illegal or secret way.

T

Trafficking: The activity of illegally buying and selling goods, such as drugs and weapons

Transnational: A system that involves several nations.