

**XXV**

**TECMUN Jr.**

---

International Police  
Organization

“Cuando pones la proa visionaria hacia una estrella y tiendes el ala hacia tal excelsitud inasible, llevas en ti el resorte misterioso de un ideal. Custódiala; si la dejas apagar no se reenciende jamás. Y si ella muere en ti quedarás inerte; frío. Solo vives por esa partícula de ensueño que se sobrepone a lo real y que te hace sentir vivo”.

José Ingenieros, *El hombre mediocre*, Buenos Aires, 1913.

Delegados, embajadores, jueces, ministros, fiscales y compañeros:

Dentro del cosmos de la modernidad, entre las corrientes de la paz y el conflicto, yacen miles de hombres como tú y como yo, hambrientos de cambio, deleitados con la ficción irrisoria de un mañana distinto. Nuestra realidad es fruto de los sueños de los visionarios de antaño y nuestros ideales son las líquidas y abstractas partículas que cristalizarán la realidad de los hombres del futuro. No es hasta que reflexionamos acerca de la naturaleza de este proceso de transición que valoramos las verdaderas implicaciones de nuestras acciones.

No somos más que individuos aislados entre la masa social, sin embargo, no es esta individualidad lo que genera el cambio, por el contrario, las ideas son la fuerza motriz que marca la senda de las revoluciones; son las ideas aquellas que impulsan la materialización del cambio. No obstante, si demeritásemos el valor de la potencia personal, nos encontraríamos con la nada, pues, no existe revolución que haya sido emprendida sin conciencia individual. Es esta suma de unidades lo que empodera la raza humana y nos aproxima a la evolución perpetua.

TECMUN es el crisol que funde las perspectivas personales en una gran razón colectiva. Es aquella entidad viva que congrega a visionarios aislados en una red de sueños, esperanzas y acciones. Hago un llamado categórico hacia todos ustedes, exigiéndoles que jamás dejen morir sus ideales, pues la decadencia del deseo contrae el desgarramiento del cambio, que conducirá a la muerte de nuestro espíritu y, al cabo, a la muerte perpetua e irreversible de nosotros mismos.

Delegados, nosotros hacemos la diferencia. Vivamos con unidad, conciencia e ideales.

---

Kevin Zamora González

Secretario General

XXV TECMUN Jr.

Delegados, embajadores, jueces, ministros, fiscales y compañeros:

El lenguaje en México, el tejer redes complejas de ideas, debería ser lugar tanto de acuerdo como de disenso. En un país inundado por el silencio, ¿qué prosigue? Es sencillo: el silencio puede ser chispa y llama. Cuando el eco que este provoca se hace tan intenso que nos ahoga, reaccionamos. A lo largo de la historia, hemos formado un círculo de víctimas y victimarios en México. Desgraciadamente, México suele ser la víctima. Mi México el vencido, al que le duele, el que llora y sangra, pero ni así responde. ¿Es esta razón para desistir de intentar cambiarlo? No. ¿Es esta razón para volverse victimario? Tampoco. Esas son dos grandes lecciones.

Recientemente, tras una serie de cambios estructurales, después de hacer y deshacer durante años, de tirar todo y empezar desde cero, podemos decir que el mexicano es mejor deshaciendo que haciendo. Empero, esto no es algo intrínsecamente malo —en el desorden también hay un orden y un nuevo desorden nos debería guiar a un mejor orden. Esa es la gran peculiaridad de México, o de menos, la que he observado: incluso cuando todo va mal, cuando se está cayendo el país (literal o metafóricamente), intentamos ordenarlo. Vamos, nos organizamos, ayudamos y todo regresa a la normalidad. Sin embargo, este fenómeno no es necesariamente bueno debido a otra gran característica: los mexicanos tendemos a olvidar. Cuando contamos con minutos de paz, no pensamos, ni nos cuestionamos cómo fue que los obtuvimos. Somos hedonistas al por mayor —preferimos simplemente disfrutar del placer que nos brinda el bienestar. Eso no es incorrecto, no importa regocijarte ante algo. El problema reside en solo vivir el momento, sin reflexionar antes el pasado o el futuro. Por eso te propongo, tú que estás ahí (idealmente escuchando, leyendo) usar el lenguaje, tu discurso, como espacio de disenso. Cuestionate tu entorno, el porqué de las cosas. Sí, busca el orden dentro de nuestro sublime desorden. Participa. Lee. Sé. Modifica tu actitud conforme a lo que vayas descubriendo. No obstante, si no lo harás, da espacio a los que sí, porque los que ya nos cansamos de los ciclos en México, de la injusticia, de que todo y nada pase somos más. Ya basta de que el silencio en México duela, hay que regresarle su voz a las víctimas. Tú, yo, nosotros que sí podemos hablar: unámonos en la otredad. Ese dolor que alguien más siente, hazlo tuyo y habla por él, sé por él y lucha por él. *Bajo la lluvia / que me quema la piel / s e r é. En el agua herida: / n o s o t r o s / s e r e m o s.*

---

Daniela Rivera Guerrero  
Subsecretaria de las Agencias Especializadas y Organismos Regionales  
XXV TECMUN Jr.

Dear delegate:

I have been here before. I remember I was 13 years old, and yes, I was scared. I have never been so scared in my life. It's difficult, I know, to stand up in front of others just to establish your point of view, feeling that your ideas are wrong, that you are not good enough. But dear delegate, you are. Your ideas are worth to listen, your points of view are not wrong just because they are different and you are stronger than you think. I hope you can remember this words for the followings three days, but also for the rest of your life. The world has changed a lot since I was sitting there the first time, with a nameplate of the People's Republic of China. Unfortunately, it has not changed for good. Nowadays, you have more challenges to deal with that the ones that I had when I was younger. Society is losing its values, corruption is taking control of the most vulnerables cities, discrimination is an issue with which we must deal each day of our lives, and we are destroying our planet as if there was no tomorrow.

Today, I'll ask you to do me the biggest favor I have ever asked for: be the difference. In a world that is surrounded with monotony, be the difference. The world is immense, there are no borders. Be a free soul each day of your life, and leave a piece of yourself in the lives of others. Have strange ideas that nobody would think of, be original, be curious. In a world that is full of insecurities, be the difference. Be happy, share your smile with each person you have the chance, because you don't know who can need it, maybe even you could need theirs. Be loyal to who you are, to what you think, because then nothing could be strong enough to tear you down. Help with whatever you can if there is someone who may need you. Help your family, friends, and even strangers. In a world fueled by demons, be human, be the difference. Be respectful with your loved ones, with the ones that have hurt you, and with the ones you hate. Have empathy, be kind and be honest. Please, save the values that make us virtuous. Change the world being the difference.

I have grown with the dream of leaving a better world for the future generations, but we won't be able to do it alone. I'm still scared, afraid that anything that I could say might not enrich the way you live your life, that it might not be saved in your memory, in your hearts. I'm afraid that the world could still falling apart, and I'm afraid of not being the difference that I proposed myself to be. Despite all, I got hope, and hope is the only thing stronger than fear. More than ever, raise your voice for what is unfair, spread your words in each corner of every beating heart, be brave enough to express yourself, because no matter what anybody tells you, words and ideas can change the world. Make them listen to you.

---

Ivana Naomi Millán Flores  
President of the International Police Organization  
XXV TECMUN Jr.

---

# Outline of the International Police Organization

The International Criminal Police Organization (INTERPOL) was created in 1923, with the main vision of becoming the organization responsible for facilitating international police cooperation, in order to make the world a safer place. It has its General Secretariat based in Lyon, France, and has become the world's largest international police organization, having nowadays one hundred ninety member countries with the mission of preventing and fighting crime through innovation and cooperation on police and security matters. The organization main objective is to deal with international impact issues, such as terrorism, cyber crimes, genocides, human trafficking, among others, and uses response teams, criminal intelligence analysis, border management, color notices, data exchange and forensics to ensure the success of police operations in order to arrest as many criminals as possible.

## **Topic A**

---

Measures to track down and prevent  
Ransomware cyber attacks after the  
appearance of the global virus *Wanna cry*

During the past May, the presence of a new virus ransomware type was detected worldwide. WanaCrypt0r, better known as Wanna Cry virus, infected more than 150 countries and more than 300,000 civilians computers in a matter of days, becoming the biggest cyber attack in the history of Internet. Since then, the international community has been looking for measures to prevent and track down future ransomware cyberattacks against critical infrastructure, public services and global economy, taking into consideration the struggles that the Wanna Cry virus created and the lack of preparation shown by the countries to deal with this malware, even though when this is not the first time that a threat of this magnitude affects their territories. Until now, none government has been able to identify the origin of the virus or its creator, however there are signs of a potential link between the Lazarus Group (recently linked to North Korea) and the global cyber attacks.

### ***Background of the countries involved***

Spain is the third most common victim of cyber attacks worldwide, just after the United States and the United Kingdom. Only during 2016, the country suffered more than 70,000 incidents of this type, affecting individuals, infrastructure and institutions (Benítez, 2017). Based on its statistics, Spain has considered cyberwar as one of its most important areas of action. As a result, since December 2013, there is a National Cybersecurity Strategy and a National Cybersecurity Council in charge of coordinating all the ministerial departments and agencies that are competent in this field.

On December 23, 2015, Ukrainian power companies experienced power outages that impacted a large number of customers in Ukraine. The reports showed the presence of the BlackEnergy (hereinafter referred as BE) malware in Ukrainian companies and in a variety of critical infrastructures. The event took place during the ongoing Russian-Ukrainian war, and it is attributed to the Russian hacking group known as “Sandworm”. The virus infected the companies networks using spear-phishing emails including the BE malware, which had the ability to damage critical parts of a computer hard drive and disrupt industrial control systems. Thereby, this hackers were able to compromise the information systems from the different companies involved and temporarily suspended the electricity supply to about 230 thousands people during a period of six hours.

On November 2016, the British government announced the implementation of the new five-year National Cyber Security Strategy (hereinafter referred to as NCSS) backed by a £1.9 billion investment, with the specific purpose of managing cyber threats in the country. On February 2017, as part of the NCSS, the National Cyber Security Center was inaugurated by the British government with the main goal of creating a single body to increase cyber security at a national level. Two months later, the United Kingdom Government statistics revealed that almost seventy percent of the large companies of the country were hit by cyber attacks during 2016. During this time, the most common methods of infection were the distribution of fraudulent emails followed by viruses and malware ransomware type.

Cybersecurity has been a problem for US national security since the 1990s, nevertheless, the threats which represented a real problem started to appear at the beginning of the new millennium. On February 2005, a cyber attack affected the Bank of America and its 1.2 million accounts. Since then, banks, shops, universities, public services and health centers have become common targets for the cyber criminals. In 2013, the discount retail chain “Target” experienced one of the biggest hacks in the history of the country when the hackers exposed the data from up to 40 million accounts, including credit cards information, passwords and physical addresses. Finally, in 2015, the health insurance company “Blue Cross” was hacked and 11 million files from their patients were left uncovered.

Most of these cybercriminals used a technique called “spear phishing”, which consists on sending emails with files or links attached to a malicious site that exploits a vulnerability on the system, in order to get access to the internal network of a company or public services. Since the events of 2015, the Department of Defense started a new cyber strategy, in order to have effective response capabilities to deter an adversary from initiating an attack, to deny a potential attack from succeeding and strengthen the resilience of U.S. systems to resist it if it penetrates the United States’ defenses.

According to the Organization of American States and its report on Cybersecurity Trends in Latin America and the Caribbean, during 2013 Brazil was the most affected Latin American country due to cyber crimes, and had to absorb a debt of more than eight thousand million dollars. The same study revealed that, México was the second most economically affected country, with losses of three thousand million dollars. With thirteen percent of its



servers attacked and an average of 7.96 attacks per server , Mexico is also in the Top ten of the countries most attacked on the Internet.

### ***Background of the virus***

#### *Ransomware*

The Ransomware, also known as Rogueware or Scareware, is a type of malicious software that blocks the access to a computer system and keeps data encrypted until a ransom is paid. It can infect the system through an email attachment or through the browser if the user visit a webpage infected with this type of malware. A Ransomware infection can be prevented by having all the protection softwares updated, nevertheless, there is always the threat of a zero-day attack. This attacks exploit a software security weakness that neither the users or the developer may be aware of.

In the past five years there have been six similar cases using the ransomware program, each one worse than the last one. In 2012, the “Reveton” virus was spread mainly in North America and various European countries. It locked a computer system and displayed a fake warning from different law enforcement agency, alleging that the computer was used for illegal purposes. The only way of unlocking the computer was by paying a fine of two hundred dollars. The next year, during September 2013, the “CryptoLocker” virus began to lock computers with a password that enable the users to have access to their data. The password was shown just after the users paid an amount of almost 10 bitcoins , and the users could recover their information. On 2014, the malwares “CryptoLocker.F”, “CryptoWall” and “TorrentLocker” took control mainly over Australia, the United States and Turkey, infecting more than twenty thousand users through a mail that avoided all the anti-virus systems available. Between April 2015 and March 2016, “Fusob” had approximately fifty-six percent of accounted mobile ransomwares, becoming one of the major families of its kind. The malware used the same infection system than “Reveton” pretending to be an authority, and extorted the users to pay a fine from a hundred to two hundred dollars, otherwise the users would face a fictitious charge.

#### *Petya*

Petya, also known as NotPetya, ExPet and Nyetya, is a malware that surged in 2016, a year before the Wanna Cry attacks. This malware forced the system infected to reboot, and

after the computers came back online, false notes about repairing the system appeared until a ransom note appeared. Petya was deployed into an important amount of computers but could spread only through a local network, therefore the risk of infection after an hour was low. A new version was created to have a deniable cover of ransomware, which attack was launched on the 28th of July of the present year. Moreover, the malware also locks the whole disk instead of only the files, thus, the disk becomes practically useless.

According to the Swiss government agency, Ukraine, Russia, the United Kingdom and India are the most affected countries of this new hack. Also some companies from Italy, Poland, Germany and the United States have been affected by the malware, which applies almost the same system of infection from Wanna Cry, and also asks for a ransom of three hundred dollars paid in bitcoins. Almost 30% of the companies and institutions attacked are in Russia and another 60% in Ukraine. Ukraine's Security Service said the attack was done by the same Russian hackers who attacked the Ukrainian power grid in December 2016, even when this information is not confirmed yet by any other authority.

After the Wanna Cry ransomware attack, the international community remains on guard for another wave of cyberattacks. According to the Organization of American States, the latin american region is highly vulnerable to future attacks of this nature due to the lack of a cybersecurity strategy and the absence of command centers and cybersecurity controls to prosecute this type of crimes. In addition, since the accusations made by the United States about the involvement of Russia in the cyberattacks that affected the presidential elections, the diplomatic relationships between this both countries were decreased to their minimum. At the same time, the relations between its neighboring country, Ukraine, are worse than ever after the past cyber attacks to its power companies, and the European Union is still applying economic sanctions to Russia due to the Russian-Ukrainian conflict.

### ***The Wanna Cry virus***

On May 12th, 2017, the first sign of the virus came from the headquarters of the Spanish operator “Telefónica”, where the employers noticed that their internal network was compromised. It was a program that sequestered the files of their computers using the Windows software, and asked for an economic ransom in bitcoins, in order to release the data. The National Cryptologic Center made a declaration alerting the situation and clarifying

basic concepts about the hack and the virus. Meanwhile, more than 1,000 cases were already confirmed by that time only in Spain.

Hours later, there were reports that the virus also attacked at least sixteen different hospitals in United Kingdom. The nation's National Health Service was severely impacted during the hack, forcing the nation to shut down everything but emergency services in hospitals all around the country. The virus also arrived to the United States. The American company "FedEx" confirmed that its systems were experiencing interference due to a malware.

On May 13, the French company "Renault", the Japanese company "Nissan" and the Russian Interior Ministry were hit by the infection. By this time, the virus was already spread over 100 different countries and affecting more than 90,000 computers with Windows software. The same day, the American company Microsoft published a patch in order to prevent the infection in computers that were not yet affected. Microsoft revealed that companies and organizations that did not install a critical security patch published two months prior to the expansion of the attack were vulnerables to the infection of the virus.

On May 15, China detected a new virus mutation that passed through the security measures implemented after the first attack, while the Europol confirmed the increment of the number of victims to 230,000 in 179 countries. Meanwhile, independent researchers found similarities between the ransomware virus Wanna Cry and some codes that were used by the cybercriminals "Lazarus Group" linked to North Korea.

### *The NSA*

Microsoft condemned the actions of the NSA after it was established that the cyber attack exploits a vulnerability that the agency discovered in Windows. The vulnerability was developed as a tool for the arsenal of digital weapons from the NSA, which later happened to be distributed in Internet by a group that calls itself "Shadow Brokers". The defect was known by both the NSA and the Central Intelligence Agency since last year, but most of the information was kept in secret. Since then, Microsoft has released an update of its products to cover the gap discovered by the agency, nevertheless, many users and corporations still had the old versions of the software, which facilitated the spread of the virus all around the world.

### ***The International Police organization and the advanced cybercrime.***

Technology is evolving, and with time, more and more criminals are taking advantage of the anonymity and speed of the Internet to use it in their favor, in order to commit crimes without any physical or virtual border. Developed attacks against computer systems and softwares are becoming a real threat, and are continuously evolving, leaving thousands of victims worldwide and affecting the global economy. The International Police Organization ( hereinafter referred as INTERPOL ), with the help of a bilateral cooperative relationship with any law enforcement agency and private industry, has the duty to investigate and find the responsables of these advanced cybercrimes. INTERPOL is notably positioned to advance the fight against cybercrime on a global scale through proactive research into emerging crimes, the latest training techniques, and development of innovative new policing tools.

#### *Previous actions*

On May 12th, 2017, immediately after the confirmed attacks, the United Kingdom authorities transferred the first information collected related to the malware, its features, and mitigating actions to be taken, via the INTERPOL National Central Bureau in Manchester, and it was in constant circulation through all the 190 member countries via an INTERPOL Purple Notice. On May 19th, in Lyon, France the INTERPOL hosted a virtual conference with all the affected countries. Here, it was revealed that all the responses from the member countries dealing with the virus were being collated and analysed by a critical incident cell established at the INTERPOL Global Complex for Innovation in Singapore. Finally, on June 07th, the INTERPOL held a meeting in Madrid, Spain to gather 49 cyber experts from 31 different countries in Europe, Asia and Oceania, in order to establish a global response to the Wanna Cry attack. The delegates that assisted to the meeting were updated on the past INTERPOL-led operation focused on cybercrime across the ASEAN region.

---

## *References*

1. Burgess, M. (2017). What is the Petya ransomware spreading across Europe?. Retrieved July 15, 2017. Web. <<http://www.wired.co.uk/article/petya-malware-ransomware-attack-outbreak-june-2017>>
2. Chappell, B. (2017). 'Petya' Ransomware Hits At Least 65 Countries. Retrieved July 15, 2017. Web. <<http://www.npr.org/sections/thetwo-way/20>>
3. Ghosh, S. (2017). The massive 'Petya' cyberattack has hit 64 countries so far and there's no kill switch this time. Retrieved July 15, 2017. Web. <<http://www.businessinsider.com/petya-cyberattack-hit-64-countries-no-kill-switch-2017-6>>
4. Graham, L. (2017). A 'state actor' was behind the ransomware attack and could trigger military response. Retrieved July 15, 2017. Web. <<http://www.cnbc.com/2017/06/30/petya-ransomware-attack-nato-says-state-actor-to-blame.html>>
5. Hackett, R. (2017). Watch that globe-circling, business-crushing malware wreck computers. Retrieved July 15, 2017. Web. <<http://fortune.com/2017/06/30/petya-ransomware-video>>
6. MalwareTech. (2017). MalwareTech. Retrieved July 15, 2017. Web. <<https://www.malwaretech.com/2017/06/petya-ransomware-attack-whats-known.html>>
7. Mascarenhas, H. (2017). 'Petya' ransomware: Full list of countries affected by the massive global cyberattack. Retrieved July 15, 2017. Web. <<http://www.ibtimes.co.uk/petya-ransomware-full-list-countries-affected-by-massive-global-cyberattack-1628086>>
8. McGoogan, C. (2017). What is WannaCry and how does ransomware work?. Retrieved July 15, 2017. Web. <<http://www.telegraph.co.uk/technology/0/ransomware-does-work>>
9. Solon, O. (2017). 'Petya' ransomware attack: what is it and how can it be stopped?. Retrieved July 15, 2017. Web. <<https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how>>
10. Fontinelle, A. (2017). Zero Day attack. Retrieved July 19, 2017. Web. <<http://www.investopedia.com/terms/z/zero-day-attack.asp#ixzz4nDvM>>
11. Palazuelos, F. (2017). Petya, a virus even more dangerous than WannaCry. Retrieved July 19, 2017. Web. <[https://elpais.com/tecnologia/2017/06/28/actualidad/1498639459\\_556568.html](https://elpais.com/tecnologia/2017/06/28/actualidad/1498639459_556568.html)>

**12.** Shieber, J. (2017). UK National Cyber Security Center issues new statement on cyberattack. Retrieved July 19, 2017. Web. <<https://techcrunch.com/2017/05/14/uk-national-cyber-security-center-issues-new-statement-on-cyber-attack>>

## *Glossary*

---

### **A**

**Anonymity:** A situation in which a person is not known by or spoken of by name.

**Average:** A standard or level that is considered to be typical or usual.

### **B**

**Bilateral:** Pertaining to, involving, or affecting two or both sides, factions, parties

**Bitcoin:** A type of cryptocurrency or a digital currency produced by a public network rather than any government.

### **D**

**Deter:** To prevent or discourage someone from doing something.

### **E**

**Exhort:** To strongly encourage or persuade someone to do something.

**Exploit:** To use something for your own benefit.

**Export:** Send goods or services to another country for sale.

### **F**

**Fraudulent:** Intended to deceive people for the purpose of obtaining money or property.

### **I**

**Innovative:** New and different.

**Investment:** The act of putting money, effort, time, etc. into something to make a profit or get an advantage, or the money, effort, time, etc.

### **L**

**Lack:** A condition of not having any or enough of something, esp. something necessary or wanted.

**Launch:** To begin, or to introduce a new plan or product.

## M

**Malware:** Computer software that is designed to damage the way a computer works.

## N

**Nevertheless:** Despite what has just been said or referred.

## P

**Patch:** A piece of software code that can be applied after the software program has been installed to correct an issue with that program.

## R

**Ransom:** A sum of money demanded in exchange for someone or something that has been taken.

**Ransomware:** Software designed by criminals to prevent computer users from getting access to their own computer system or files unless they pay money.

**Reboot:** To switch off and then start again immediately, or to make a computer do this.

**Resilient:** Able to improve quickly after being hurt or being ill.

## S

**Struggle:** To work hard to do something.

## T

**Target:** A target is a person or group attacked in some way.



**Threat:** A statement that someone will be hurt or harmed, if the person does not do something in particular.

**Track down:** To find something or someone after looking for them in a lot of different places.

## V

**Virus:** A program that is intended to prevent the computer from working normally.

**Vulnerable:** Able to be easily hurt, influenced, or attacked.

## W

**Worldwide:** Existing or happening in all parts of the world.

### *Guiding Questions*

---

1. How was your delegation affected by the Wanna Cry virus?
2. Which are the cybersecurity strategies of your delegation?
3. How is your delegation related with the International Police Organization?
4. Which were the measures taken by your delegation to affront the Wanna Cry virus?
5. Which is the context of your delegation regarding cybercrimes?

## **Topic B**

---

New drug trafficking routes and smuggling methods used by organized crime groups in West Africa and Asia

---

*By: Ivana Naomi Millán Flores*

During the past May, new smuggling methods and trafficking routes to Europe were discovered inside West Africa and Asia. For years, both regions have been submerged in several political, economical and social crises, leaving the countries with the ideal conditions for any organized crime group to start their own drug trafficking route. The lack of funds, education and commercial activity created a low development level inside this countries, and as a result, their citizens searched for a better way to earn a living, finding their solution inside the illegal drug trafficking. In some countries, no legitimate commercial activity has the potential to generate incomes comparable to the drug trade. This has become a threat with the power to not only disrupt the international political sphere, but to alter the governability and stability worldwide. Smuggling methods are evolving too, making it even more difficult to track down, arrest and seize the illicit drugs. The fear that insurgents and extremists groups throughout the region would be in a position to facilitate trafficking, thus drawing resources to their cause and increasing the violence, had made the international community to create strategies in order to fight back this menace.

### **Background of the countries involved**

Guinea-Bissau is the world's fifth poorest nation in the world. The lack of prisons and the few police available have created a perfect environment for organized crime. After 13 years of fight, it won its independence from Portugal and spent more than 20 years under the control of a dictatorship, until military rebellion tried to liberate the country. Continuous crises and two wars brought economical and social instability to the country, of which it has not recovered. Since then, most of the citizens live in precarious conditions. People do not have access to electricity or water supplies, they can't afford cars or even bus fares. In the past years, Colombian drug cartels have been focusing on this country, turning it into a transit hub for the cocaine trade out of Latin America to Europe. The profit of the drugs trade inside Guinea-Bissau is greater than the national income, becoming the "first narco-state" considered by the United Nations.

Other West African country that moved into drug trafficking was Nigeria in 1980, as Asian and Latin American drug traffickers searched for alternative travel routes to Europe. Africa was not a common production site for either heroin or cocaine, and African couriers did not provoke suspicions at airports in Europe and North America in the early 1980s. On

1982, the first arrest of heroin traffickers in Nigeria took place at the Murtala Muhammad International Airport in Lagos. During Muhammadu Buhari government in 1984, death penalty was introduced for drug smugglers, originating the first wave of Nigerian drug traffickers to Ghana. Ghana is located on West Africa's Gulf of Guinea and between 1980 and 1990, the extension of Nigerian drug smuggling networks lead to the detection of more than 1,744 illegal deals in narcotics. During 1990, the World Bank touted the country as a model for structural adjustment programs, causing an economic recession that affected small business owners, that with the pass of the years, turned to drug trafficking. By 1992, the number of Ghanaians raised to 100 (World Bank, 2004).

Mali is one of the biggest nations located in West Africa and shares borders with Niger. As other West African nations, Mali passed through a crisis after gaining its independence from France in 1960. The crisis left the nation with social and economic instability until democratic elections took place during 1992. In 2012 a *coup d'etat* was launched by national officers. All of this characteristics made Mali a transit hub for drug trafficking from South America towards Europe. In 2011, the G8 launched the Action Plan on Transatlantic Drugs Trafficking in order to stop the transatlantic cocaine trade, focusing on West African routes.

Based on the statistics shown during the last decade, the international community started to take actions in the matter. The African Union developed the Plan of Action on Drug Control which seeked to strengthen continental and international cooperation in drug control issues. In January, 2013, the West African Commission on Drugs was created. This Commission had as main objective to analyse the drug trafficking information collected, in order to deliver an authoritative report and policy recommendations to tackle the problem.

In Asia, Afghanistan and Turkey are two of the most important countries in the matter of drug trade. For years, Afghan heroin has entered Europe via what is known as "the Balkan route". This well organized and corrupted route is an overland path that passes through Iran, Greece and up through Serbia, Hungary, and other countries in the Balkans. Also, during 2009, Afghanistan produced 6,900 tons of opium, which was the 95 percent of the global supply for that year (UNODC, 2016). Afghanistan has been a source of heroin during years, but it was since the US-led invasion of the country in 2001 that the poppy production started

to disturb the international community, taking into consideration that only during that year Afghan growers cultivated almost 8,000 hectares of poppy plants. By 2014, that number escalated to more than 224,000 hectares (UNODC, 2016). Turkey's threats have nothing to do with the production or consumption of narcotics, but they have to do with drug trafficking, and it's considered a matter of national security. For decades, Turkey has been part of "the Balkan route" and passed through challenges related to the trade and use of illicit drugs. A variety of drugs are trafficked through Turkey towards Europe each year.

### **Background of the conflict**

Drugs demand in Europe has doubled in the last decade, just like its price. Stronger laws and the tightening of security controls at Europe in the mid-2000s created a situation where the use of direct smuggling routes was not possible anymore, what lead Latin American and Asian countries to found new smuggling routes in West Africa. Only in 2010, more than 3000 methamphetamine couriers traveled from West Africa to Europe, carrying about 360 million dollars in drugs (UNODC, 2013). In the case of heroin, it is produced in two main areas: the Golden Triangle, through Thailand, Burma and Laos, and the Golden Crescent, through Afghanistan, Iran and Pakistan. This main areas use " the Balkan route" to enter Europe and only during 2010 had a profit of more than 1.4 billion dollars.

Due to the free movement of people and goods throughout the Economic Community of West African States (hereinafter referred as ECOWAS) countries, any type of drug or illicit good has big possibilities of entering or exiting one of this territories without passing through any kind of border controls. In the 1990s, the West African Regional Security Initiative (hereinafter referred as WARSI) was created with the main goal of assisting the 15 ECOWAS official members in order to generate an effective criminal justice and civilian security sectors. WARSI focuses on this countries with economical problems to develop correctly their security sectors and to counter transnational organized crime with the assistance of specialized units. Also, in 2014, an airport communications project called "AIRCOP" was launched. The project was focused on establishing a new effective communication line between immigration areas and aviation security, relied on the International Police Organization's (hereinafter referred as INTERPOL) I 24/7 communication system.

Between 1998 and 2003, each year 600 kilograms of cocaine were seized throughout Africa, but since 2006 the trend has been increasing, and only during the first nine months of last year it reached 5.6 tonnes of cocaine. Since 2003, 99% of all drugs seized in Africa have been found in West Africa (Stewart, 2013) In 2008, the Economic Community of West African States (hereinafter referred as ECOWAS) created a Regional Action Plan in order to address the growing problem of illicit drug trafficking, organized crime and drug abuse in West Africa. Nowadays, Nigerian organized criminal networks have been detected in almost every country in East Asia, and still being a major player in moving cocaine and heroin, not only to European territory, but also worldwide. Nigeria is also dealing with a terrorist insurgency led by Boko Haram, which remains the cause of the insecurity in some regions of the nation, and corruption still facilitating criminal activities.

### **New smuggling methods and drug trafficking routes**

During 2017, “Operation Lionfish” was launched by the INTERPOL with the main objective of identifying drug trafficking across Asia and the Pacific, focusing specifically on airports with a second phase to targeting land and sea borders. Operation Lionfish was created with the help of INTERPOL’s Africa-Middle East-Asia Pacific Project (hereinafter referred as AMEAP), being a five-year project providing a coordination platform for a range of anti-drug trafficking initiatives led by INTERPOL. It was coordinated by an Operational Coordination Unit inside the Global Complex for Innovation in Singapore, with the help of representatives from the different involved countries, the World Customs Organization, and the cooperation from more than 2,000 police and customs officials across 14 countries. During the first week, the operation revealed new networks of West African and Asian organized crime groups, which were behind the trafficking in methamphetamines, cocaine, cannabis and heroin. By the end of the two-weeks operation, a total of 350 kilograms, 50 liters and 2,175 tablets of this illicit drugs were seized, worth an estimated of 18 million dollars.

Authorities from the United Arab Emirates identified an increasing smuggling method in the region, which consisted on swallow condoms packed with liquid cocaine. This method was harder to detect by traditional x-ray or computed tomography in comparison with the more conventional ones. To this discovery followed the one of 9 kilograms of methamphetamine hidden inside a shipment of soft toys, which resulted on the arrest of 13

individuals from West Africa, Mongolia and China. In Nigeria, an individual was arrested for attempting to import drugs helped by his contacts in the aviation and maritime systems, and a new cocaine trafficking route via Ethiopia with destination to Asia was detected. Meanwhile, it was reported that in Ghana, 61% of the cocaine left the country by boat and 39% by air, and was usually transported inside unsuspecting objects, such as speakers, while the traffickers used multiple fake passports to access different countries (UNODC, 2016). Law enforcement officials report that traffickers are exploiting Ghana's unguarded and maritime border, offloading large shipments at sea onto small fishing vessels which carry the drugs to shore undetected. Also traffickers from all West Africa started flying narcotics directly into Mali with the help of small aircrafts that airdrop cocaine into prearranged locations. After the findings, the INTERPOL send a new Purple Notice to all 190 member countries about this modus operandi and methods for their detection.

The contraband flow of illicit drugs into Europe is so extensive that its wholesale value on arrival in the region exceeds the national security budgets of many countries in West Africa. A large number of methamphetamine couriers on flights between West Africa and Europe have been reported since 2008, but there has also been an increase in the amount of heroin transiting West Africa through commercial air couriers, most of it destined also to Europe.

### **The International Police Organization response to drug trafficking**

Organized crime is transforming. Traditional structures are being replaced by criminal networks that change operations and modify their work models based on demand, profitability, incentives and opportunities. Drugs demand is increasing worldwide, as well as its trade. The drug trade is a present threat inside all our member countries, implicating growers, producers, couriers, suppliers, dealers and even users. The International Police Organization focuses on the most commonly trafficked and used drugs, in addition to precursor chemicals.

INTERPOL's essential role is to identify new drug trafficking trends by following criminal organizations and their operations worldwide, maintaining a close relation with non-governmental organizations that have a counter-drug mandate and national law enforcement agencies. Trafficking routes are becoming more efficient, more varied and find easier borders



to cross, increasing the global abuse and accessibility to drugs. As a measure to support its 190 members in the fight against the increasing changes in organizing and emerging crime, the International Police Organization (hereinafter referred as INTERPOL), has developed the five-year Organized and Emerging Crime Strategy, which focuses on enabling countries to target and disrupt transnational criminal networks, while they identify and respond to emerging criminal threats.

#### *Previous actions*

On March 24th, 2017, in Lyon, France the INTERPOL initiated the Operation Lionfish III, which achieved 357 arrests with the help of 5,000 law enforcement officials inside 13 member countries from latin america and West Africa. Also 55 tonnes of drugs bound for Europe and 20 clandestine laboratories were dismantled and three tonnes of precursor chemicals were seized during the operation with the help of the INTERPOL's Criminal Networks unit and the exchange of cross-checking information against INTERPOL's global databases in real time.

On 2006, the INTERPOL created the Asian Organized Crime project, which counts with coordinated operations focused on crime networks. The project also counts with the Asia-Pacific Expert Group on Organized Crime in order to exchange information related to new crime trends and strategies, while law enforcement agencies from all around the world share intelligence and experiences on the matter. Later, on 2013, the Project Fortaleza on the Latin American and Caribbean countries was created, focusing on reinforcing the region's capacity to detect, track, report and prohibit new drug trafficking routes, providing police forces with the necessary tools in order to safeguard national borders and to maintain their national security.

---

## *References*

1. ISSAfrica. (2012). Drug trafficking and the crisis in Mali. Retrieved July 27, 2017. Web. <<https://issafrica.org/iss-today/drug-trafficking-and-the-crisis-in-mali>>
2. Tran, M. (2013). Mali: a guide to the conflict. Retrieved July 27, 2017. Web. <<https://www.theguardian.com/world/2013/jan/16/mali-guide-to-the-conflict>>
3. Akyeampong, E. (2005). Diaspora and drug trafficking in west africa: A case study of Ghana. Retrieved July 27, 2017. Web. <<https://blackboard.angelo.edu/bbcswebdav/institution/LFA/CSS/Course%20Material/BOR6306/Readings/BOR%20CRII%206306%20Africa%20and%20Ghana%20as%20Case%20Study.pdf>>
4. Asiedu, K. (2016). Drugs trafficking: Ghana is major transit point for cocaine. Retrieved July 27, 2017. Web. <<http://www.pulse.com.gh/news/drugs-trafficking-ghana-is-major-transit-point-for-cocaine-un-report-id5208282.html>>
5. Bureau of international narcotics and law enforcement affairs. (2014). Ghana. Retrieved July 27, 2017. Web. <<https://www.state.gov/j/inl/rls/nrcrpt/2014/vol1/222893.htm>>
6. Mogelson, L. (2012). The Corner Where Afghanistan, Iran and Pakistan Meet. Retrieved July 29, 2017. Web. <<http://www.nytimes.com/2012/10/21/magazine/the-corner-where-afghanistan-iran-and-pakistan-meet.html>>
7. Asia. (2017). Interpol operation across 14 countries unearths new routes, methods for drug trafficking. Retrieved July 29, 2017. Web. <<http://www.straitstimes.com/asia/se-asia/interpol-operation-across-14-countries-unearths-new-routes-methods-for-drug-trafficking>>
8. Hamilton, K. (2016). The golden age of drug trafficking. Retrieved July 29, 2017. Web. <<https://news.vice.com/story/drug-trafficking-meth-cocaine-heroin-global-drug-smuggling>>
9. Cengiz, M. (2017). Turkey has a major drug problem-here's how to get a handle on it. Retrieved July 29, 2017. Web. <<https://www.brookings.edu/blog/order-from-chaos/2017/04/05/turkey-has-a-major-drug-problem-heres-how-to-get-a-handle-on-it/>>

## *Glossary*

---

### **A**

**Address:** To speak or write to someone, or to direct information to someone.

### **C**

**Cross-checking:** to check something, such as data or reports from various angles or sources to determine validity or accuracy

**Coup d'etat:** The sudden, violent overthrow of an existing government by a small group.

### **E**

**Evolve:** To change or develop gradually.

**Extremist:** Someone who has an opinion or ideas that seem unreasonable to most people.

### **I**

**Illicit:** Illegal or disapproved of by society.

**Insurgents:** A person who revolts against civil authority or an established government; especially a rebel not recognized as a belligerent

**International political sphere:** The term may refer to a political claim to exclusive control, which other nations may or may not recognize

### **L**

**Lead:** To manage or control a group of people; to be the person who makes decisions that other people choose to follow or obey.

**Legitimate:** Allowed according to law, or reasonable and acceptable.

### **P**

**Policy:** A set of ideas or a plan for action followed by a business, a government, a political party, or a group of people.

**Poppy plants:** Opium Poppy plant.

## **R**

**Rebellion:** Violent action organized by a group of people who refuse to accept their government's power and are willing to use force to oppose it.

## **S**

**Seize:** To take using sudden force.

**Smuggling:** To import or export secretly contrary to the law and especially without paying duties imposed by law.

## **T**

**Tighten:** To strongly control something.

**Touted:** To solicit, peddle, or persuade importunately.

**Trafficking:** The activity of buying and selling goods or people illegally.

### *Guiding Questions*

---

1. How is your delegation related to West African and Asian drug trafficking routes?
2. Which are your delegation's security measures regarding smuggling methods inside international airports?
3. How is your delegation affected by drug trafficking in Europe?