UNODC

MOSMUN XIV

Presidents:

Emiliana Castaño and Alejandro Gutiérrez

unodc@montessori.edu.co

Index.

- # Welcoming letter.

"Every great dream begins with a dreamer. Always remember, you have within you the strength, the patience, and the passion to reach for the stars to change the world." — Harriet Tubman.

Esteemed delegates,

With immense pleasure and profound gratitude, we extend a warm welcome to each of you as you embark on this extraordinary journey at the XIV edition of MOSMUN. As your presidents, we are deeply honored to have been entrusted with the responsibility of guiding you through this experience.

MOSMUN, more than just an academic endeavor, is a life changing academic event that empowers us to transcend personal boundaries and embrace our roles as global citizens.

It is a platform where we can confront the pressing challenges of our world, equipping ourselves with the intelligence, conviction, and diplomatic finesse needed to navigate the complexities of the diplomatic world.

As your presidents, we encourage you to embrace this opportunity with enthusiasm, to showcase your capabilities, and to learn from your mistakes to become the best delegate you are able to be. Embrace MOSMUN as the opportunity to grow personally, for it is within these walls that you will cultivate the skills and forge the connections that will shape your future as global leaders.

We expect nothing less than your absolute best during each session of debate, but more importantly, we hope that by the culmination of this extraordinary experience, you will emerge as individuals empowered to make a meaningful impact on the world. With immense faith in your potential, we wish you an enriching and transformative journey at MOSMUN.

Sincerely, your Presidents,

Alejandro Gutiérrez and Emiliana Castaño.

Emiliana Castaño Moreno
+57 (350) 825 0384

Alejandro Gutiérrez
+57 (302) 361 7555

• Introduction to the committee

2.1 Historical Background

The committee of UNODC which stands for The United Nations Office on Drugs and Crime is the global leader in the fight against illicit drugs, transnational organized crime, terrorism and corruption as proclaimed by the United Nations. This committee was established in 1997 as the merging of two already existing offices of the United Nations which were the United Nations Centre for International Crime Prevention and the United Nations International Drug Control Programme, and it was initially conformed by more than 500 functionaries world wide.

As a result of the creation of the UNODC committee it was set as an objective the committee by the Secretary General that the organization needs to focus and enhance the capacity of the United Nations to face and address the interrelated issues of drug control, crime and international terrorism in all forms while also educating people on the world about the dangers that drug abuse brings. In order to achieve this there are three main pillars that this committee stands for which are health, security and justice for all.

Since the UNODC was put into effect it has worked exhaustively in order to achieve the general and specific objectives of the committee which are Strengthening the judicial and legislative capacity.

1. Assisting countries in reducing drug trafficking.
2. Enhancing the capacity of Government institutions and civil society organizations in order to prevent drug use and the spread of related infections.

3. Enhancing the capacity of Government institutions and civil society organizations in order to counter attack trafficking of persons and smuggling of immigrants.
4. Creating awareness and reducing the incidence of domestic violence.
5. Promoting victim empowerment.

2.2 Functions and objectives

As previously stated the general objective of UNODC is to enable the Organization to focus and enhance its capacity to address the interrelated issues of drug control, crime and international terrorism in all its forms. As well as cooperating with the member countries to achieve the 2030 Agenda for Sustainable Development and the 17 Sustainable Development Goals (SDGs) at its core, and specifically the objective that recognizes that "the rule of law and fair, effective and humane justice systems, as well as health-oriented responses to drug use, are both enablers for and part of sustainable development." However of course the UNODC has some specific strategic objectives that it looks forward to achieving the previously mentioned goals.

● Topic A: Combat against transnational and extraterritorial jurisdiction in the cyberspace

a. *Glossary:*

Human Right: rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status.

The Interest of Justice: the reason for case dismissal used when the judge decides that justice will be best served when the case is dismissed.

The Principle of Complexity and Expense: the complexity and cost to produce something which is complex is more expensive than something that is lower quality or produced at a slower speed.

Satellite litigations: one or more lawsuits that are related to a major lawsuit being conducted in another court.

Extradition: the removal of a person (typically referred to as a fugitive) from a requested jurisdiction to another jurisdiction for criminal prosecution or punishment.

b. *Introduction to the topic*

Cybercrime is defined by the Britannica dictionary as: “The use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.” (Dennis, 2024) This has become an international crisis, having negatively impacted the world since technology became a crucial part of our daily lives. As technology evolved, so did crime, migrating to the aforementioned and using it as a tool to continue and further expand illegal activities, making it easier to carry out various crimes without being detected.

Technology, which was meant to make our lives easier, ultimately gave the possibility for groups outside of the law to continue committing crimes and created the opportunity for new crimes to surface. Knowing this, it is important to note that cybercrime also brings a big

international component to it, since it is not something that countries are able to contain and tackle within its borders, but furthermore it is an issue that recognizes no geography; with the use of technology such crimes have the power to reach the whole world due to its decentralized nature; these crimes may violate multiple jurisdictions and affect various countries at the same time, having in mind that it occurs on an international platform which is the internet itself, making it an issue of international relevance.

This problem continues to expand despite there already being established international and national regulations which don't seem to have the effect that the countries were expecting, since cybercrime continues to be an issue that expands and affects the world on a global scale every day. E-crime has led to a rise in the use of extraterritorial and transnational jurisdiction when countries are not supposed to do so, cybercrime is leading to the violation of sovereignty as well as multiple international principles; as for example the principle of international law, human rights, the justice of interests, the principle of complexity and expense, as well as the fundamental goals of criminalization, which work all together in order to avoid the application of extraterritorial and transnational jurisdiction, however a violation of these previously mentioned principles and agreements is evident. The alternative of expanded subjective territorial control and enforcement is certainly fraught with challenges, but in the long term, it is without a doubt the most effective way to combat cybercrime. Nevertheless, not all countries seem to be in favor of this idea, which is why cybercrime continues to be an unsolved topic which has to be tackled by the UNODC committee and The United Nations as soon as possible.

c. *Historical Background.*

The development of the internet from its origins is closely linked to the historical trajectory of addressing issues of transnational and extraterritorial jurisdiction in cyberspace. When the internet first started, which was originally named ARPANET in the late 1960s, it was used to support both military strategic requirements and academic research. Nevertheless, as the digital world expanded in the 1990s, a paradox developed: conventional legal systems built on the idea of territorial jurisdiction found it difficult to address the globalized, linked character of cyberspace. The difficulty was managing the conflict between the old, geographically restricted concepts of legal authority and the global connections of the virtual world.

The 1990s saw an extraordinary increase in the number of people using the internet, which also led to an increase in e-commerce. The seamless movement of data across national borders made a coherent international legal response every time more necessary. One of the first attempts at an official legal framework managing cyberspace and cybercrime was the 2001 introduction of the Convention on Cybercrime by the Council of Europe, also known as the ***Budapest Convention.*** However the road to legal harmonization and improved international cooperation turned out to be complicated, since multiple countries such as The Russian Federation refused to sign this convention because they argued that this convention would violate its sovereignty. The complex interpretation and application of these agreements proved to be an obstacle, as national laws were frequently conflicted, making it difficult to prosecute cybercrimes successfully and obstructing international cooperation.

Since the internet has no borders nor geographic origin, deciding which jurisdiction is best to monitor cross-border cybercrimes has become a difficult task, taking into account that

a big question is created which is if cyberspace enters in the jurisdiction of a country, or if it is a public platform that every country can intervene upon, making it an international concern for the countries on how to proceed when a cybercrime occurs. This was especially evident in situations involving cyberattacks that were sponsored by states, because giving out blame for the attacks to particular state actors increased the complexity of the situation. At the same time, the presence of private organizations and people in cyberspace further confused national borders. The lack of an internationally recognized legal framework made matters worse by depriving the private sector of a set of guiding principles. Coherent and efficient responses to transnational jurisdiction issues were hampered by conflicting national laws and the lack of international conventions governing private sector operations in cyberspace.

d. Current situation.

States are mostly geographical in nature. Criminal jurisdiction follows this unconditionally. Conventional ideas of area and jurisdiction are existentially challenged by cyberspace, which definitionally transcends borders because of its decentralized nature and its lack of geographical position. One response from states to the increase in cybercrime has been to extend their criminal jurisdiction across international borders to include alleged cybercriminals living overseas. This has been carried out on one or more extraterritorial bases, the issue that this response has is that the states carry it out either openly or in secret, keeping it from the rest of the international community. This Jurisdiction use in cyberspace is mainly due to the constant series of crimes that happen in it.

- ***Cybercrime Influence.***

The phenomenon of cybercrime continues to extend and expand even after decades of long national and international regulations. EUROPOL stated; “The threat landscape has also evolved, attribution is complex in cyber contexts, cybercrime is growing in scope, number of attacks, financial impact and sophistication, jurisdiction is problematic, and the range of offenders and threat actors continue to grow” (Europol, 2021). In particular, it is suggested that it is inappropriate to treat the use of extraterritorial and transnational jurisdiction as standard or customary components of the fight against cybercrime. It comes with imperfections, inefficiencies, and occasionally injustices. It takes away from the best course of action, which is to rely on the legal system and law enforcement. The exercise of subjective territorial authority is almost certainly the most effective long-term solution, however it does bring multiple challenges which have to be tackled rapidly before this solution can be implemented.

Its influence is based on the fact that cybercrime has no borders, this makes it easier to affect transnational and extraterritorial jurisdiction. Traditional ideas of jurisdiction are complicated by cybercriminals' ability to operate across international borders due to the interconnection of the digital world. Legal authorities face a great deal of difficulty when perpetrators start assaults from one jurisdiction, and target victims in another, while utilizing infrastructure in a third jurisdiction or state. To successfully battle and lessen the worldwide effects of cybercrime, joint, cross-border initiatives are required due to its transnational component.

Due to the intricate nature of cybercrime, investigations and prosecutions face jurisdictional difficulties. There are disparities in how different nations handle cyber threats

due to differences in their legal systems and capacities for law enforcement. It becomes complex to determine which jurisdiction has the power of acting over a cybercrime occurrence, which causes administration conflicts and makes it difficult to capture and persecute attackers. These issues are worsened by the lack of uniform worldwide laws and regulations, which gives cybercriminals the opportunity to take advantage of legal gaps and avoid responsibility over their crimes, if a concrete legal framework which covers all of the cybercrimes its restrictions and its limits isn't put in place, it is very difficult for the international community to be able to stop the cybercrime crisis to continue expanding.

Building strong legal frameworks and promoting increased international cooperation are necessary to address the impact of cybercrime on jurisdiction. International accords, such as the Budapest Convention on Cybercrime, are designed to standardize legal frameworks and promote collaboration across national boundaries. But creating a thorough, internationally recognized legal system is still a difficult task. Establishing standards that strike a balance between national sovereignty and the necessity of collective action to successfully tackle cyber threats is the subject of ongoing discussions. The way forward is to promote international cooperation and agreement in order to modify legislative frameworks to meet the dynamic needs posed by cybercrime in the digital era.

- ***Cybercrime principles.***

In response to the challenges posed by the borderless nature of cybercrime, the international community has developed a set of extraterritorial jurisdiction principles. These principles allow states to assert jurisdiction over cybercrimes even if the crime was committed outside of their territory. The most common extraterritorial jurisdiction principles in cybercrime include:

- The nationality principle: A state can assert jurisdiction over a cybercrime if the offender is its national, regardless of where the crime was committed.
- The protective principle: A state can assert jurisdiction over a cybercrime if the crime causes significant harm to its interests or security, regardless of where the crime was committed.
- The effects principle: A state can assert jurisdiction over a cybercrime if the crime produces harmful effects within its territory, regardless of where the crime was committed.

The application of extraterritorial jurisdiction principles in cybercrime cases is complex and often contested. States may disagree on the interpretation of these principles, and there is a risk of conflicts of jurisdiction. Moreover, the exercise of extraterritorial jurisdiction can raise concerns about sovereignty and the potential for abuse of power.

- ***Human Rights Involvement***

Transnational jurisdiction's assumption may cause or assist a violation of an accused cybercriminal's human rights, a higher danger of such a violation, or the potential that an infringement will go unremedied, according to a persuasive argument against it. However, an accused's rights may also be violated in the course of a subjective territorial prosecution. Since that legislation was in effect at the time of the alleged offense, it is doubtful that a violation will be tried in the subjective state after rendition. Furthermore, there can be differences in how the respective states interpret human rights, which would be biased against the accused. It has been proposed that this is the case with respect to United Kingdom (UK) to United States (US) practice, for instance, with relation to "special administrative measures," which are discussed below. Developed both in that particular environment and more widely as a body of established jurisprudence. When arguments based on human rights have been made against the assumption of international jurisdiction, this has come to light.

Typically, the cases start in satellite human rights litigation or extradition hearings. The main thrust of these arguments is that, either because of the accused's removal from the state that is being requested (a domestic case) or because of the treatment she will receive in the state that is being requested (a foreign case), rendition will result in a breach of her human rights.

Notable examples in the body of jurisprudence addressing challenges to global jurisdiction involve cybercrimes. This is due to their propensity to have international ramifications and the possibility of a tenuous connection between the accused, his actions, and the state wishing to assert jurisdiction. The Gary McKinnon case is one of the first cases in the UK. In the US, he had been accused of fraud and other computer-related offenses. While in the UK, he had broken into several computer systems in the US. He was a British national with Asperger's syndrome who had never been to the US for inquiry into his alleged offenses. McKinnon was contained in the US with the intention of preventing his extradition concerning his entitlement to a just trial. In the end, it did not succeed in court. The fact that very high standards must be met in order to successfully oppose extradition on the grounds of human rights was somewhat relevant. Notably, the Home Secretary, James Cleverly, is responsible for immigration, the police, and other matters relating to the safety of the United Kingdom. He had some discretion at that time in McKinnon's case when deciding whether to extradite.

[1]

Finally, to clarify the more punctual and common violations of The Universal Declaration of Human Rights in the cyberspace are going to be stated ahead:

[1] Asperger's Syndrome: is the former name of a developmental disability that affects how people behave, see and understand the world and interact with others. People with this developmental disability may have special interests, repetitive behaviors and under or over react to sensory input. (HealthDirect, 2020)

- Freedom of expression: States may use extraterritorial jurisdiction to censor online content that they deem objectionable, even if the content is protected by freedom of expression norms in other countries.
- Privacy: States may use extraterritorial jurisdiction to collect or monitor the communications of individuals who are not within their physical territory, raising concerns about unwarranted surveillance and intrusions into privacy.
- Due process: States may assert extraterritorial jurisdiction over cybercrimes without providing fair and due process which is to have harmonized national substantive cybercrime laws that criminalize cybercrime, as well as national procedural cybercrime laws that set the rules of evidence, and criminal procedure protections to individuals who are accused of these offenses.
- Right to assembly: States may use extraterritorial jurisdiction to disrupt or prevent online gatherings or forums, even if these activities are protected by the right to assembly.

- ***Legal Framework***

The current legal framework in cyberspace encompasses various legislative and regulatory aspects related to cybersecurity, data protection, and cybercrime. Governments are increasingly focusing on enacting national legislation to address cybersecurity issues, including regulatory requirements, cybercrime legislation, and human rights impact assessment. International law also plays a crucial role in governing cyberspace, addressing issues such as attribution and accountability for cyber activities conducted by states and other actors. However, there are ongoing debates about the use of force in cyberspace, with discussions around the legality of "hack-back" or counter hacking techniques to prevent cyber attacks. Cybersecurity laws and regulations cover a wide range of issues, including cybercrime, preventing attacks, specific sectors, corporate governance, litigation, insurance,

and investigatory and police powers. Additionally, federal information security laws and standards, privacy laws, and regulations, as well as cloud computing security and acquisitions, are integral parts of the legal framework for cybersecurity.

There are three key elements in the division of the current legal framework in the cyberspace that encompasses a large range of legal principles:

- National Laws: To address cybercrime, cybersecurity, and other challenges related to cyberspace, many national laws have been passed by various nations. These laws frequently address cybercrime prevention and prosecution, data protection, and intellectual property protection.
- International Treaties: A number of international treaties, such the Budapest Convention on the Recognition of Electronic Signatures and the Council of Europe Convention on Cybercrime, deal with concerns relating to cyberspace. These agreements offer a shared foundation for collaboration and national legal harmonization.
- Non-Binding standards: A variety of non-binding standards govern state conduct in cyberspace in addition to official treaties. Multi-stakeholder organizations like the Global Commission on the Future of Cyberspace frequently create these norms, which represent an agreement on appropriate state conduct in the digital sphere.

e. Past resolutions

Budapest convention: The Budapest convention was the first convention and international resolution which seeked to battle and eradicate cybercrime by harmonizing national laws, encouraging cooperation of the international community and enhancing investigative techniques. It was adopted by the council of Europe in 2001 and entered into force on July 1, 2004. The convention aims for the vision of a free internet with appropriate

criminal justice when misused. Some key concepts of the convention is the Technology neutral language which allows the technology to cover offenses, identity theft, terrorsim, spam, etc. On the other hand, The convention ensures that restrictions on data and the protection of personal information are defined narrowly as well as specifying that only criminal activities can be investigated on the internet. This made this convention a guideline for multiple countries to base their internal legislation on.

UN general assembly resolution on the cybercrime treaty: In the year 2021, the United Nations General Assembly passed a resolution which was titled "Countering the use of information and communications technologies for criminal purposes". This resolution had the intention of outlining the terms for multilateral negotiations to draft a landmark global treaty against the rising threat of cybercrime.

Group of Seven's (G7) Declaration on Responsible States Behavior in Cyberspace (Lucca Declaration): In the year 2017, the G7 (Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States) who agreed on this declaration, which committed states to cooperate in exchanging information about crimes occurring through the internet, while assisting each other to prosecute terrorist and criminal use of ICTs, as well as implementing other cooperative measures to address cyber threats.

UN Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security: In the year 2015, the UN GGE (Group of governmental experts) released a report after over a year of negotiations concerning the use of ICTs for criminal purposes and explaining its intentions of tackling such issue.

f. QARMAS.

- What measures has your delegation taken in order to regulate and prosecute Cybercrime?
- Does your country have internal jurisdiction regarding cybercrime? If so, What is it?
- Has your country signed any of the previous resolutions regarding this topic?
- Has your country suffered cyberattacks sponsored by other nations?
- Has your delegation made attacks on another nation through cyberspace?
- What are the measures that are enforced on your country when a cybercrime takes place?

4. Topic B: Measures for the prevention of amphetamine-based drug captagon and its traffic in the Middle East.

a. Glossary:

Captagon: a highly addictive amphetamine-type drug that is largely produced and consumed in the Middle East, especially Syria and Lebanon.

Amphetamine: class of highly addictive stimulant drugs that speed up the messages traveling between the brain and the body.

Assad regime: The Assad regime refers to the government of Syria, which has been controlled by the al-Assad family since 1970. The regime is a highly personalist dictatorship that governs Syria as a totalitarian police state.

b. *Introduction to the topic:*

The amphetamine crisis in the middle east has become a raging topic in the past few years, since the rapid spread of amphetamine based drugs consumption, continues to leave at its pace multiple deaths, and civilians which struggle to find help recovering from such harsh addiction. As the addiction rates continue to increase it comes to the attention of the international community that the most commonly used drug in the Middle East is Captagon, which is an amphetamine based drug that is most consumed in countries such as Syria and Lebanon, however, tends to be a very popular drug all around the Middle East. Captagon is commonly recognized for its sleep loss, and lack of hunger effects, and this is one of the reasons for this drug to be highly known and consumed. From students staying up all night, to professionals hoping to stay focused during a prolonged number of hours, the popularization of this drug has all kinds of publics, making it especially dangerous. Used from partying all night, to weight loss, and sleep deprivation on its consumers, Catagon has become a threat to public health, alarming the international community.

c. *Historical background:*

Captagon was initially created as a brand name for a psychoactive medicine created in Germany in the 1960s, by a company recognized as Degussa Pharma Gruppe to treat narcolepsy and other similar conditions. Captagon was made of an amphetamine type stimulant named Fenethylline which is a central nervous system stimulant, with multiple effects such as: feeling euphoria, being more active and talkative, can cause confusion, hallucinations, nausea, vomiting, seizures, high blood pressure, and high heart palpitations, fatigue, multiple withdrawal symptoms, as well as long lasting physical and mental issues

which require medical attention. However, captagon was discontinued on the global market as a medicine to treat various illnesses, nevertheless, the currently consumed captagon is a counterfeit version of the medicine which used to contain Fenethylline, the illicit version of the drug is believed to be caffein with other fillers, which allegedly generates focus and staving off of sleep and hunger.

The issue with captagon addiction came to be recognized as an international problem when over a billion pills of Captagon were seized in Arab countries only in Asia between 2019-2022. Its production, trafficking and consumption entrenched in the region of the middle east. This issue is especially recognized in Syria after multiple reports about the Syrian government being involved on the Captagon trade market, and using such involvement to fund the regime, and since the onset 2011 conflict Syria has suffered multiple sanctions due to its participation on the traffick of this drug, even receiving the name of "narco-state." The situation of Syria with the traffic of Captagon led to diplomatic leverage, making foreign ministers from Egypt, Iraq, Saudi Arabia, and Jordan to begin negotiations with Syria in order to curb the growing rates of traffic and Captagon consumption.The implication of the state of Syria with the traffic of Captagon has also brought various geopolitical implications, since Syria has also acquired the power to push the trade into other regions or countries. The drug trafficking of Captagon has also affected regional diplomatic decisions and discussions, as some Arab countries are gravely concerned and look to address the issue actively.

d. Current situation:

Authorities throughout the entire region have linked the constant consumption, production and trafficking of Captagon with several negative consequences including security, health and

geopolitical impacts, leading the authorities to ask for help from the international community in order to address this issue which is getting out of hand. Some of the consequences that have been recognized as part of the issue with Captagon are:

1. Security impacts: The proliferation of Captagon has increased the security concerns, after over a billion pills of Captagon were seized in Arab countries in Asia between 2019-2022. As well as its link to various Syrian officials and regional actors, the trade of captagon has also been linked to multiple militant groups as well as becoming a powerful source of revenue for the Syrian government which continues to be labeled as a narco-state because of its involvement with the illegal drug market.

2. Health impacts: The captagon consumption and production represents a risk to human health since it is a highly addictive amphetamine based substance which implicates several secondary effects that represent a threat to human health. Its production could also have very grave impacts to human health since its illicit production often involves the use of many bulking agents and adulterants. Because of its wide public it also represents a threat to human health when being used constantly and even by younger groups of people, it could even have an implication of drug abuse on underage kids which often find the consumption of such drugs on parties or public gatherings, it could even be offered as a way to stay up all night, or to loose weight having grave implications on their brain and body development, as well as leading them to consume such drugs with disregard for its side effects.

3. Geopolitical impacts: Because of the participation of the Syrian government on the Captagon trade market as well as various state actors has brought multiple

geopolitical implications. The Syrian government has the power to push the trade of the Captagon drug into the countries and into other regions exacerbating the problems. Additionally, generating a great corruption concern since the money of the Captagon commercialization is being introduced into the Syrian government making profit from illegal activities, highlighting that the exports from Syria continue to grow every year with the drug providing financial support to the Assad regime's war machine. The drug issue has also affected multiple diplomatic discussions since multiple Arab countries have tried to address the topic.

It is important to recognize Hezbollah which is a great Shiite Muslim political party and militant group in Lebanon,which works as both a militant group and a political party, has also been reported as a large manufacturer of the drug, raising concerns as well because of its great connection to the Assad regime in Syria. The group has been greatly accused of being involved in the Captagon trade market with reports indicating that Hezbollah and other Iranian militias facilitate the fabrication of this drug. Nevertheless, Hezbollah's leader, Hassan Nasrallah, has denied these reports, stating that the group is not involved in the drug trade and that Captagon and other types of drugs are religiously prohibited. However, the involvement of this group on the production of such drugs continues to be an international concern because of some Arab league members raising suspicion about the implication of such a group in the production and trafficking of the drug.

e. Past Resolutions

Due to this problematic being so recent in time, there's not many resolutions or past events that develop´s it, but last year the United States Congress published a complete resolution of it.

H.Res.836 - 118th Congress - The resolution calls on the US government to strengthen the Middle East's ability to break up and stop the illegal manufacture and distribution of the stimulant known as captagon, which is related to amphetamines, as well as the synthesis of precursor chemicals. It draws attention to how, throughout the previous five years, the captagon market in the Mediterranean-Gulf region has expanded to become an industrial-scale unlawful trade. It names ministerial-level cooperation in manufacture and smuggling, as well as the Assad regime's role in boosting numerous criminal networks, armed organizations, mafia syndicates, and autocratic nations, as major factors driving the illicit trafficking of captagon. The resolution points out that bad actors like the Assad government, Hezbollah, and militias with ties to Iran have access to alternate funding sources thanks to the illegal captagon trade. It describes an incident in which captagon pills were found in the pockets of Hamas militants who were believed to have been under the effect of the drug during an attack in Israel in October 2023. The resolution highlights how the Assad administration and those who support it profit greatly from the illegal production and trafficking of captagon, which is thought to be worth over $10 billion. It recognizes that captagon transit and destination nations face difficulties in enforcing interdiction measures and emphasizes the danger that illegal captagon production and trafficking hubs in Syria and Lebanon pose to the border security of US friends and partners. The resolution also acknowledges the rise in captagon pill seizures in recent years by regional allies of the United States such as Saudi Arabia, Jordan, and Iraq. It also highlights the lack of any official or functional regional mechanism or platform for intelligence sharing and collaboration to

counter, dismantle, and disrupt the illicit captagon trade. These factors together highlight the need for increased interregional and intraregional coordination in the Middle East to counter the proliferation of captagon. Lastly, the resolution asks the US to support more regional collaboration in the fight against drugs, namely the illegal captagon trade.

f. QARMAS:

- Has your delegation intervened or been linked to any Captagon trafficking?
- Has your delegation been affected from this amphetamine crisis?
- What type of drugs are legal in your Country?
- What are the rates of amphetamine-based drugs used in your delegation?
- Is there any relations from your delegation to any of the middle east countries involved? If so, what are they?

*g. **Support Links:***

Title: The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted.

Language: English

Summary: This article exposes why prosecuting cybercrime using transnational and extraterritorial jurisdiction, meaning that a country applies its laws to acts committed

outside its borders, is something that should be avoided. The article mentions a case where six people were extradited to the US and given harsh sentences for cybercrimes, which is something that violates their human rights. The article also highlights the importance of the approval of a protocol to improve cooperation E between countries on sharing evidence for cybercrime investigations.

Link: https://www.tandfonline.com/doi/full/10.1080/13600869.2022.2061888

Title: EU Competition law and extraterritorial jurisdiction – a critical analysis of the ECJ's judgment in Intel

Language: English

Summary: This article discusses ECJ'S competition in intel case on the jurisdiction of EU competition law. Traditionally, EU competition law applied to companies within the EU or those with subsidiaries there. The Intel case involved Intel's anti-competitive practices outside the EU affecting the EU market.

The ECJ introduced the "qualified effects test" to establish jurisdiction in such cases. This means the EU can have jurisdiction if a company's actions outside the EU have a direct, substantial, and foreseeable effect within the EU. The author says that this decision is necessary because it is consistent with the concept of "conduct forming part of an overall strategy" already used in EU competition law. Furthermore, it allows the EU to regulate anti-competitive behavior in a globalized economy.

Link:

https://www.tandfonline.com/doi/full/10.1080/17441056.2020.1840844?src=recsys

Title: H. RES. 836

Language: English

Summary: H. Res. 836 is a resolution from the 118th Congress (2023-2024) expressing to the United States government the urge to focus on disrupting the production and trafficking of captagon, an amphetamine-type stimulant, in the Middle East. It expresses the will of the house of representatives to resolve such issue, however, it does not have any power of law, nevertheless it explains the necessity to resolve this raging issue.

Link: https://www.congress.gov/118/bills/hres836/BILLS-118hres836ih.pdf

References:

Arnell, P. (2022, June 8). *Prosecution of Cybercrime*. Tandfonline. https://www.tandfonline.com/doi/full/10.1080/13600869.2022.2061888

Berkes, A. (2019, June 7). *Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside Its Effective Control*. Cambridge Core. https://www.cambridge.org/core/journals/israel-law-review/article/abs/human-rights-obligations-of-the-territorial-state-in-the-cyberspace-of-areas-outside-its-effective-control/A485442EA8B55100F398BD14924DBD0A

Council of Europe. (n.d.). *Budapest Convention - Cybercrime*. The Council of Europe. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Dennis, M. A. (2024, March 8). *Cybercrime | Definition, Statistics, & Examples*. Britannica. Retrieved March 15, 2024, from https://www.britannica.com/topic/cybercrime

Digwatch. (n.d.). *UN OEWG in 2023 - DW Observatory*. Digital Watch Observatory. https://dig.watch/processes/un-gge

Europol. (2021, November 11). *Internet Organised Crime Threat Assessment (IOCTA) 2021 | Europol*. Europol. Retrieved March 15, 2024, from

https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

HealthDirect. (2020, November). *Asperger's syndrome | healthdirect*. Healthdirect. Retrieved March 15, 2024, from https://www.healthdirect.gov.au/aspergers-syndrome

Hollis, D. (2021, June 14). *A Brief Primer on International Law and Cyberspace*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763

Hollis, D. (2021, June 14). *A Brief Primer on International Law and Cyberspace*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763

Interpol. (n.d.). *Cybercrime - Crimes*. Interpol. https://www.interpol.int/en/Crimes/Cybercrime

Lieberman, E., & Padilla, C. (2023, June 28). *What Does the G7 Do?* Council on Foreign Relations. https://www.cfr.org/backgrounder/what-does-g7-do

Nguyen, T. (2020, September 29). *The Structure of Cybercrime Networks*. Tandofline. https://www.tandfonline.com/doi/full/10.1080/0735648X.2020.1818605?src=recsys

Ryngaert, C. (2023, May 22). *Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts*. Cambridge Core. https://www.cambridge.org/core/journals/german-law-journal/article/extraterritorial-enforcement-jurisdiction-in-cyberspace-normative-shifts/3F1E5EED62283DB200D2F6026A6CE951

T-CY/Council of Europe. (n.d.). *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY - Cybercrime*. The Council of Europe. https://www.coe.int/en/web/cybercrime/parties-observers

United Nations. (2011, December 12). *Cybersecurity: A global issue demanding a global approach | UN DESA | United Nations Department of Economic and Social Affairs*. the United Nations. https://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html

University of Oxford. (n.d.). *Dimension 4: Legal and Regulatory Frameworks | Global Cyber Security Capacity Centre*. Global Cyber Security Capacity Centre. https://gcscc.ox.ac.uk/dimension-4-legal-and-regulatory-frameworks

UN/Meetings Coverage. (2021, May 26). *General Assembly Adopts Resolution Outlining Terms for Negotiating Cybercrime Treaty amid Concerns over 'Rushed' Vote at Expense of Further Consultations | Meetings Coverage and Press Releases*. Meetings Coverage and Press Releases. Retrieved March 14, 2024, from https://press.un.org/en/2021/ga12328.doc.htm

Zelger, B. (2020, November 15). *EU Competition law and extraterritorial jurisdiction*. Tandofline. https://www.tandfonline.com/doi/full/10.1080/17441056.2020.1840844?src=recsys