Committee: Disarmament and International Security Committee (GA1)

Issue: Preventing transnational organized crime via cyber threats

Student Officer: Selina Karatza

Position: Co-Chair

PERSONAL INTRODUCTION

Dear Delegates,

My name is Selina Karatza, I am a 10th grade student at CGS, and it is my utmost honor and pleasure to be serving as Co-Chair of Disarmament and International Security Committee in the 5th session of ACGMUN. For me, MUN is not just an educational simulation. Through MUN, I have been given the motivation to push myself out of my comfort zone and develop not only as a student but as an individual too. I believe that it provides us all with the valuable opportunity of becoming a part of a worldwide community, enabling us to obtain a much more global understanding of the world. That said, it constitutes a great passion of mine. The 1st Committee of the UN General Assembly tackles some of the most urgent issues, concerning international security and disarmament. Thus, the actions that are to be taken in the context of this committee refer to peacekeeping and tackling instances that endanger international security.

This study guide discusses the issue of "Preventing transnational organized crime via cyber threats". Throughout this guide, I delve into issues such as the various different types of cyber threats namely cyber-attacks, cybercrime and cyberwarfare, the alarming need to distinguish the three terms in order to counter cyber threats and the challenges associated with defining TOC. Additionally, I discuss the history and development of transnational cybercrime, elaborate on some of the most significant occurrences of transnational cybercrime throughout history, and examine two incidences through the lens of two case studies. Finally, I make reference to the transnational nature of cybercrime and the significant issues we confront in terms of global cybersecurity. As a consequence, while proposing solutions to this specific problem, a variety of elements must be addressed. While this study guide covers several areas of the subject, it should not be considered the only source of knowledge throughout your research. Having said that, you are highly advised to perform comprehensive study on the topic to ensure a thorough understanding of it. Of course, if you have any queries or require additional explanations, please feel free to contact me at the following email address: selinak2006@gmail.com

Kind Regards, Selina Karatza

TOPIC INTRODUCTION

The invention of the internet and its subsequent predominance in nearly all spheres of national and global politics, have spawned a new threat environment in the international arena. The whole contemporary way of life, from national socioeconomic systems to national security systems, is now almost fully reliant on real-time internet access, which is susceptible to all kinds of fluctuations in cyberspace.

Having said that, the issue of cyber threats has risen to prominence in public discourse in recent years as cybercrime has become ingrained in the global threat environment, conjuring visions of malicious and highly sophisticated online activities. More recently, it has been associated with the notion of “organized crime”. There has since been debate and dispute about whether this kind of crime is a descendant of conventional organized crime or a development of it in the online world. This puzzling predicament has been deteriorated by the lack of conclusive evidence attesting to and supporting either theory. Unequivocally, technological advancements have historically been leveraged to the criminal community's benefit. The critical issue now is whether such advancements have solely enhanced physical crime or have resulted in the emergence of a new generation of conventional, but digital, organized crime.

However, addressing cybercrime is not the main purpose of this guide – rather, the main purpose is to delve into the concept of transnational organized cyber threats. The transnational dimension of organized crime has been consistently noted and characterized as a concerning trend. Historically the realm of criminologists, lawyers, and sociologists, the immense profits and power gained by today's prominent criminal organizations and networks have placed cybercrime at the forefront of the global community's security agenda. This is the "dark underbelly" of globalization, in which criminal groups are believed to have benefitted not only from the more open global economy, but also from the development of sophisticated tools, strategies, and connections capable of hampering governmental efforts to restrict their operations. These are conventional organized crime operations carried out on a wider scale, and now constitute a danger to every nation-state involved. In essence, Transnational Organized Cybercrime (TOC) networks are becoming more involved in cybercrime, which cost governments and businesses billions of dollars each year, pose a danger to business and government computer networks, and erode global faith in the international security system, whilst also posing an increasing hazard to the general population and key infrastructures.

Finally, the commercial and governmental sectors' current security measures fall well short of providing an effective level of protection against these threats since they have failed to predict how, TOC networks would evolve into a strategic danger to governments, society, and economy. Additionally, at an international level, an out-of-date understanding of TOC fails to account for the strategic implications of TOC and to guarantee that peace initiatives and crime-fighting activities do not clash. Due to the underlying global character of the Internet and other components of the information infrastructure, a proper transnational response to these transnational concerns is an urgent and pressing imperative.

DEFINITION OF KEY TERMS

Computer worm

A computer worm is a kind of malware that is developed to replicate itself and spread to other computers whilst staying active on compromised systems. It can proliferate without human intervention and does not require affiliation to a software application to inflict harm.

Cyber infrastructure

Cyber infrastructure is a set of information technology systems and software, physical and information assets, procedures, and individuals that are all associated via software and innovative networks to enhance academic efficiency and increase previously unimaginable knowledge advancements and findings.

Cyberspace

Cyberspace is a term that alludes to the digital computing world, and more precisely, to an electronic medium that enables digital communication. Cyberspace is often comprised of a huge computer network consisted of several international computer sub-networks that provide data communication and exchange. Cyberspace's primary characteristic is that it is an interactive and virtual environment open to a diverse variety of individuals.

Cyber-security

Cyber-security is the employment of technology, procedures, and policies to safeguard mission-critical systems, networks, programs, devices, and sensitive data from cyber threats. Cyber-security measures are intended to counter threats to networked systems and applications and to diminish the likelihood of their occurrence, regardless of whether the threats originate within or outside of an organization.

Digital Forensics

Digital forensic science is a subfield of forensic science concerned with the recovery and study of data recovered from digital devices used in cybercrime. In essence, digital forensics is the process of locating, conserving, evaluating, and recording digital evidence, aiming to enable evidence to be presented in a court of law when necessary.

Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service attacks are a type of cyber-attacks that focus on overloading a network, hence rendering it unable to function. The main targets of this type of attack are government websites and company websites.

BACKGROUND INFORMATION

The difficulties in defining Transnational Organized Crime (TOC)

The first challenge that States faced was defining what constitutes transnational organized crime, and it quickly became evident that trying to offer a unified definition would be fruitless. Organized criminal organizations are continually adapting to changes at local, national, and worldwide levels and shifting their operations based on a cost-benefit analysis of available unlawful possibilities. Rather than defining crimes, states have chosen to define actors. That said, the United Nations Convention against Transnational Organized Crime aims to address both the present and future demands of criminal justice. More precisely, in order for it to be classified as TOC, a crime must be perpetrated by an organized group of three or more individuals that has existed for an extended length of time, acts in conjunction with the intent of committing at least one significant crime, and seeks, directly or indirectly, financial or other material gain. Additionally, in our efforts to define transnational organized crime, we have established that, in broad terms, transnational crimes are those that are planned, directed, controlled, executed, or have impacts beyond national borders. More precisely, according to article 3 of the Organized Crime Convention[1], a crime is considered transnational if it meets at least one of the following conditions: it is committed in more than one State, it is

[1] United Nations Convention against Transnational Organized Crime,

https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf committed in one State but a big part of its preparation, planning, direction, or control occurs in another State, it is committed in a one State but involves an organized criminal organization that operates in multiple states, or it is committed in a single state but has significant consequences in another state. Thus, there are two primary criteria for determining the Convention's area of application: first, the offenses included must be international in nature, and second, they must involve an organized criminal group.

The phenomena of transnational Cybercrime

The history and evolution

Nations have long been at odds, from trade wars to brutal conflicts. Cyber threats, on the other hand, are a relatively new phenomenon. More precisely, cyber security concerns have grown in importance on a global scale. When the first legitimate computers were launched in the early 1900s, no one anticipated their eventual strength or the extent to which they would help the countries that benefitted. As with nuclear weapons, governments had to learn how to use this new technology to their advantage, as well as how to communicate with one another regarding in such new ways. Information was no longer geographically restricted. People gained new methods for acquiring intelligence, while malicious programmers, or else known as hackers gained the ability to disrupt critical national events, with elections serving as a great example.

Major incidents of transnational organized crime

The Morris worm was the first known attack against the world's cyber infrastructure. Robert Tappan Morris was a graduate student interested in determining the "size" of the internet. Thus, he developed a type of software in 1988 that went from computer to computer and transmitted signals back to the server. However, Morris was unaware that the software had developed a worm. It overwhelmed and rendered computers inoperable. This was the first time a distributed denial of service attack was reported. Cyber-attacks have prevailed ever since, becoming an increasingly common occurrence, especially with the phenomenal growth of the internet.

Other significant cyber strikes include a denial-of-service attack on the Estonian government in 2007 in response to a dispute with Russia. Israel's government computer system was hacked in January 2009, amid a military conflict in the Gaza Strip. In 2010, a computer virus called “Stuxnet” was deployed to launch an undetectable assault on Iran's nuclear program, aimed at disabling the country's uranium enrichment centrifuges. In 2012, a Russian cyber-security company identified a global cyber-attack named "Red October," in which hackers acquired information through loopholes in Microsoft's Word and Excel programs. The malware amassed data from government embassies, research organizations, military bases, power companies, and nuclear and other key facilities". In 2014, Russia launched cyber-attacks in Ukraine after the annexation of Crimea by pro-Russian rebel groups and during the Ukrainian elections. Additionally, in 2015, Russia and China launched cyber-attacks on Germany and the United States of America. Moreover, the “WannaCry” ransom-ware attacks were recorded in 2017 and are said to have infected over 200,000 computers running Microsoft Windows in over 150 countries. Later that year, the “NotPetya” weaponized ransom-ware emerged as well, destroying information and wreaking havoc. In 2021, an Indian hacking group employed mobile malware to target around 150 people in Pakistan, Kazakhstan, and India, including those with ties to the Pakistan Atomic Energy Commission.

Examining Transnational organized Cybercrime through Case Studies

The 1999 Military Hacking in Kosovo

Anyone with a computer and Internet connection is a potential attacker in globalized, Internet-era warfare. NATO's first significant relevant military action occurred in the aftermath of the internet's phenomenal rise in the 1990s. The 1999 Military Hacking in Kosovo was the world's first large-scale Internet conflict. As NATO aircraft started bombing Serbia, various pro-Serbian hacker organizations, including the so-called "Black hand”, began attacking NATO's Internet infrastructure. Although it is uncertain if any of the hackers originated from inside the Yugoslav military, their claimed objective was to impede NATO military activities. The “Black Hand”, which took its name from a pan-Slavic secret club that aided in the outbreak of World War I, said it could identify NATO's most critical systems and would seek to destroy all data on them by hacking. The group claimed success on at least one machine belonging to the United States Navy and asserted that it was later taken down.

Throughout the conflict, NATO, the US, and UK computers were all assaulted through denial-of-service attacks and virus-infected email. In the United States, the White House website was attacked, prompting an inquiry by the Secret Service. While the US claimed it suffered no harm due to the attack, the UK acknowledged to losing at least some database information. The strikes on NATO's headquarters in Belgium constituted a publicity coup for the hackers. NATO's public relations website for the war in Kosovo was almost inaccessible for many days, whilst spokesperson Jamie Shea ascribed "line saturation" to Belgrade-based hackers. Finally, as the organization attempted to modernize virtually all of its computer systems, network assaults began to originate from all over the globe.

The 1994 Chechen propaganda

Since the start of the World Wide Web, pro-Chechen and pro-Russian groups have conducted a virtual war on the Internet simultaneously with their on-the-ground conflict. Chechen separatists, in particular, are credited with pioneering the use of the web as a medium for delivering effective public relations messaging. The strategically placed propaganda and other material, such as the account number for a war funding bank account in Sacramento, California, aided in uniting the Chechen diaspora.

However, the most successful material was anti-Russian, not pro-Chechen. Digital photographs of bloodied bodies influenced public opinion against Russia's alleged military abuses. In 1999, when justice Kremlin authorities were denying an assault on a Chechen bus that resulted in the death of several passengers, photographs of the event surfaced on the web. With the advancement of technology, Internet users were able to see streaming recordings of favorable Chechen military operations, including ambushes on Russian military convoys.

Subsequently, the Russian government acknowledged the need to enhance its online techniques. Moscow requested Western assistance in shutting down the biggest pro-Chechen website, and "the establishment of centralized military censorship related the north Caucasus conflict" was declared. Russian authorities were accused of increasing the cyber conflict during the second Chechen war which took place from 1999 to 2000, by hacking into Chechen websites. Some of the assaults' timing and complexity implied nation-state engagement.

Drawing the line between the three types of cyber threats: Cyber-attack, Cybercrime, Cyberwarfare

The need for the distinction

The reality of global interconnectedness has resulted in a plethora of international security issues pertaining to the internet as well as cyberspace. These issues are rapidly merging several facets of transnational cyber threats, such as cybercrime, cyberattack, and cyber warfare. As a result, there is an alarming need to differentiate between the three, that cannot be overlooked particularly in today's environment, given the difficulties of distinguishing the operations of conventional transnational criminals from cyber hostile acts. Thus, an enhanced knowledge of the many cyber risks is rendered of pivotal importance in the endeavors to minimize the possibility of inconsistent global reactions among states and preclude the highly disastrous effects that come with the employment of force in retaliation.

The words “cybercrime”, “cyber-attack” and “cyber-warfare” are frequently employed similarly without regard for their conceptual implications, breadth, and reach. Indeed, the triad is almost inextricably linked. Since the turn of the century, the dividing line between these three conceptions has been pushed almost to breaking point. This lack of clarity has hampered efforts to craft significant legal responses to international activity involving any of them. Nowadays, a single cyber operation may comprise one or more of these threats, depending on who began the act, the infrastructure attacked, and the offender's aim. For example, cyber-attacks are often begun using techniques that may constitute cybercrime in certain situations. Cyber warfare, on the other hand, must be commenced by a preceding cyber-attack. Indeed, it is impossible to determine with certainty if a particular cyber threat requires a military reaction in the form of self-defense or multilateral criminal investigation and collaboration in order to eliminate a transnational menace. That said, so as to appreciate the ways these notions are connected, it is essential to explore each independently.

Cyber-attack

Just as cyber-attacks span a broad range of the threat environment known as cyberspace, the term "cyber-attack" itself differs according to the viewpoint of the person describing it. According to the US Army's Cyber Operations and Cyber Terrorism handbook, a cyber-attack is defined as the deliberate use of disruptive activities, or the threat of such activities, against computers and/or networks with the intent to cause harm or further social, ideological, religious, political, or similar objectives, or to intimidate any person in furtherance of such objectives. Additionally, according to the handbook, cyber-attacks strive to complete four primary goals: loss of integrity, which allows for unauthorized modification of data, loss of availability where mission-critical information systems become inaccessible to authorized users, confidentiality breach, in which sensitive information is leaked to unauthorized users, and physical destruction during which information systems inflict real physical injury as a result of directives that produce purposeful system failures.

Despite the fact that the term “cyber attack” has a plethora of different definitions, the combined effect of these definitions is that the concept of cyber-attacks equates to the traditional equivalent of 'armed attack,' which involves the aspect of violence against the state's integrity and the attack's repercussion. The term "cyber-attack" is defined in a way that goes further than the conventional notion of desktops and laptops to include other artificial intelligence-based devices.

Furthermore, the term “political or national security purpose” is used to differentiate simple cybercrimes and cyber-attacks, particularly in instances where a cyber-activity begun by a non-state actor would otherwise comprise cybercrime, except that it is implemented with the goal of harming a state's political or national security objectives. Thus, the element that distinguishes cybercrime from cyber-attack is the objective of the cyber operation and not necessarily the actors' nature. Simply put, non-state entities, such as a government authority, may constitute both victims and perpetrators of a cyber-attack.

Cybercrime

The word “cybercrime” has also proved challenging to define, despite the fact that some elements of the crime are universally recognized. For example, cybercrime may be perpetrated exclusively by a non-state actor using a computer system and must contravene a state penal provision or international criminal law. However, unlike in the case of a cyber-attack, the offense does not intend to disrupt the operation of a computer network, nor does it have a political or national security motivation. Rather than that, cybercrime is defined as "any crime that is enabled or performed via the use of a computer network or physical device." Thus, the term "cybercrime" is very broad, encompassing a wide variety of illegal activities committed in cyberspace, such as online privacy violations.

Cyberwarfare

The term 'cyber warfare' is almost non-existent in official papers and is unaccepted internationally. A more comprehensive grasp of the term extends its applicability much beyond cyberspace, to encompass the physical impacts of cyber operations and assaults on the target state's essential infrastructure. With that in mind, we may define cyber warfare as state-on-state activity which occurs in cyberspace and is equal to an armed assault that may provoke a military reaction including the utilization of physical force. Additionally, the concept is defined as a cyber-attack that results in bodily harm or property damage just like a traditional armed attack would. Unequivocally, the notions of cyber warfare, cyber-attack, and cybercrime are inextricably linked. While cyber warfare must be preceded by a cyber-attack, cyber-crime may exist independently of either cyber-attack or cyber-warfare. Cyber war, on the other hand, may potentially constitute cybercrime.

The transnational dimension of Cybercrime

Cybercrime actions have a global component, including concerns of cross-border inquiry, sovereignty, jurisdiction, extraterritorial evidence, and the demand for international collaboration. A cybercrime offense takes on a global dimension when an element or significant consequence of the offense occurs in another jurisdiction, or when a portion of the offence's method of operation occurs in another area. From a merely technical point, all online communications are divided into "packets" that separate and commute via servers located throughout the world. Cybercrime extends beyond this technical, transnational dimension and involves senders who design their attacks and other crimes freely in order to take advantage of potential vulnerabilities inherent in the infrastructure's transnational nature. Namely, the significant number of potential targets of denial-of-service or other attacks, which facilitates attackers to inflict more damage with much less exertion than would have been needed to attack computers or users in a single state as well as the plethora of pervasive imbalances between states in the legal, judicial, or policy environment that surrounds cybercrime, and the dearth of international cooperation.

Primary challenges in transnational cyber security

Even though governments in developed and emerging nations are seen as determined and proactive in their endeavors to combat and deter cyber criminals from inflicting harm to their cyber infrastructure, the very essence of cyberspace involves various challenges in implementing cyber regulations in these countries. Simply put, the challenge lays in defining and determining political borders and perpetrators in cyber space.

Cyber-criminals and their strategies are always evolving, making it increasingly complex for governments and corporations to keep up with the constantly evolving techniques. Nonetheless, multilateral institutions lack the analytical and functional abilities required to adequately comprehend and respond to these attacks. They depend on crime-fighting strategies and national enforcement tools that were established to combat organized crime prior to the full realization of the linkages between crime, violence, and corruption.

Even when international organizations uncover criminal networks, they lack the resources and authority to interfere with domestic law enforcement instruments. According to Rob Wainwright, Director of Europol's Criminal Investigations of Cyber-Crimes, tracing and identifying the source of crime is not only challenging but frequently impossible due to the crime's borderless nature, which constitutes one of the major challenges facing the developing world. Additionally, in conjunction to widespread usage of pirated software to counter cybercrime, a lack of digital forensics skills and knowledge is another critical problem that has been unresolved for a long period of time. Because of the extensive usage of pirated software, which is more susceptible to viruses and malware, tackling cybercrime is deemed more arduous and challenging.

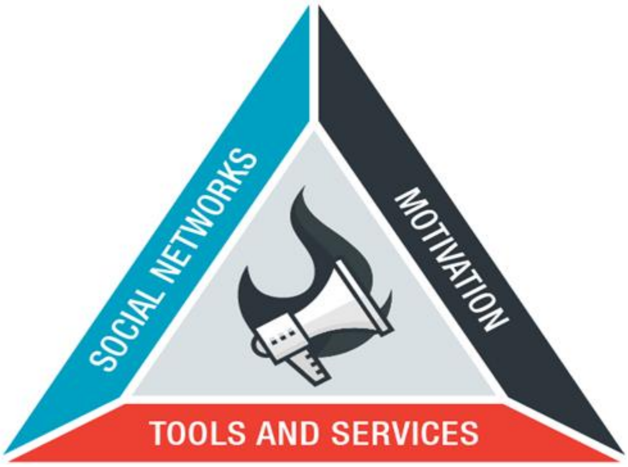

Figure 1: The Fake News Triangle[2]

Potential repercussions of cyber threats on the general population

Cyberattacks appear constantly in the headlines every day, and they frequently have far-reaching implications. Cyberattacks on vital infrastructure and healthcare systems damage more than just data; they may also cause havoc in the real world. The societal effect of a cyber breach may also be quantified by the service interruptions that occur as a result of the attack. These disruptions may be widespread or isolated, depending on the nature of the breach, but they are

[2] "Fake News and Cyber Propaganda: The Use and Abuse of Social Media." Trend Micro | Enterprise Cybersecurity Solutions, www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media

nevertheless extremely real and aggravating for the individuals affected immediately**.**

Cybercrime can be crippling for businesses. When a cyber-attack arises, a business may suffer significant financial and operational damage. Even after a cyber assault is resolved, the resulting harm persists. While many organizations may encounter a cyberattack throughout their operations, a large-scale cyber assault can cause severe damage to an organization's image. This ultimately results in lost contracts and customer connections, as the firm strives to rebuild its public image. Additionally, emotional repercussions such as depression, embarrassment, humiliation, or confusion are highlighted, while reputational impacts might include the loss of ruined customer connections, and significant media attention. On a related note, one could say that the most significant danger that may directly target and impact people is disinformation delivered as part of a cyberattack's bundle. While major social media companies have placed a heavy emphasis on disinformation, it still constitutes a naturally spread issue. Disinformation tactics continue to use networking infrastructure and routing services at many layers of the internet stack. Social media platforms often function as conduits and amplifiers for misinformation websites. Thus, misinformation and cybersecurity both include a large number of the private sector's and internet technological community's participants. These assaults are allegedly intended to compromise reputable information sources and to influence and divert public opinion, social media, and the press. This is accomplished through sowing suspicion, weakening commonly accepted society and democratic principles, and perhaps affecting the result of significant events such as elections.

MAJOR COUNTRIES AND ORGANIZATIONS INVOLVED

United States (US)

Transnational criminal organizations commit a broad array of crimes in the United States, the majority of which are directed at companies, consumers, and government programs. Additionally, cyber war is a component of their military policy, and a cyber-attack on the country would constitute a casus belli, a declaration of war. While they have carried out some strikes, they have also been the victim of several attacks and cyber threats. Thus, officials such as former secretary of Defense Leon Panetta, have emphasized the critical nature and threat of cyber-attacks and wars. They have already invested in cyber-security and have a vigorous cyber-defense system, which is upgraded on a regular basis owing to the magnitude of threats they face. Additionally, they have established a legislative framework for cyber-security, something that the majority of nations have yet to achieve. The US Department of Defense revealed in April 2009 that it has spent more than $100 million on cyber-attack repair and response. Furthermore, NATO established the Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallinn in 2007 in response to the cyber assault on Estonia. The CCDCOE aims to improve cyber investigation, development, and protection in the nation. Finally, prior to leaving office in 2016, the Obama administration committed $19 billion to cyber security research and development.

Russian Federation

Russia has been accused of several cyber-attacks against other states and has been accused of numerous big cyber strikes. It launched the 2007 attack on Estonia, the Paris-based broadcaster, all of its 12 channels were almost completely destroyed by Russian hackers, the 2015 cyber-attack on TV5Monde, the 2008 attacks on Georgia, and the cyber-attacks against Ukraine in 2014 aiming to disrupt the Ukrainian presidential elections. According to reports, Russian hackers meddled in both the 2016 presidential election in the US and the 2016 referendum on the United Kingdom's exit from the European Union. Throughout the election, a group of Russians sought for vulnerabilities in state voter records, hacked a major presidential campaign, the Democratic Congressional Campaign Committee, and the Democratic National Committee. Additionally, they disseminated politically divisive content on the internet and propagandized across all social media platforms, including Facebook and Twitter. In the UK, a team of academics revealed on Wednesday that over 150,000 Russian-language Twitter accounts tweeted tens of thousands of tweets in English asking Britain to leave the European Union in the days before last year's vote on the topic.

Russia has asserted that it has conducted some denial of service (DDOS) attacks as part of its defensive plan. Lastly, in recent years, Russia seems to have increased its reliance on cyber strikes as part of its security policy and has acquired far more computing capacity than other nations, which makes it especially formidable in the field of cyber defense.

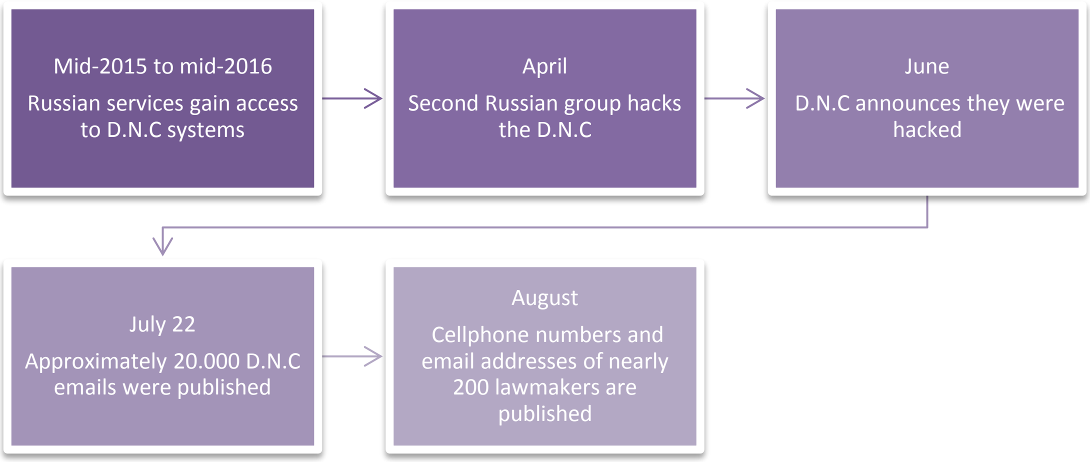
Mid-2015 to mid-2016
Russian services gain access to D.N.C systems
April
Second Russian group hacks the D.N.C
June
D.N.C announces they were hacked
July 22
Approximately 20.000 D.N.C emails were published
August
Cellphone numbers and email addresses of nearly 200 lawmakers are published

Figure 2: Timeline of a Probable DNC Intrusion by Russian Intelligence Services

People’s Republic of China

Transnational criminal organizations are becoming more engaged in all aspects of intellectual property theft in China, from manufacturing to distribution. Other networks are engaged in cybercrime, unlawful financial transactions, and drug trafficking. In terms of cybercrime, China was the victim of one of the greatest distributed denial-of-service attacks in history in 2010, when Iranian hackers hijacked a prominent search engine in order to perpetuate their political views. Thus, the country is particularly involved, seeing as it also constitutes a rising economy, which has allowed it to preserve cyber-security and render itself as one of the world's most protected and secure countries. Additionally, the government has superior technologies in place for protection against such assaults.

Pakistan

Pakistan is one of the most involved countries in cybercrime, despite the fact that they have a lengthy list of anti-cybercrime legislation. Each day, a substantial number of incidents are documented, ranging from account hacking to hazardous outcomes such as illegal and unauthorized financial transfers and withdrawals. That said, cybercrime in Pakistan is expanding in tandem with the exponential development in mobile phone use and internet access. Therefore, they have developed the National Response Center for Cyber Crime (NR3C) to monitor, trace, and apprehend cyber offenders. NR3C serves as a central point of contact for all domestic and international agencies investigating cybercrime in Pakistan. Additionally, it provides training and security education to government/semi-government and private sector institutions, in addition to hosting training workshops and conferences to educate users about cyber-attacks on their information resources, data breaches, and how to secure their systems against all such threats.

United Kingdom (UK)

TOC generates significant economic revenue in the United Kingdom, ranging between $32 and $64 billion each year. In terms of cybercrime, the UK has a history of waging war on cyber-terrorism and cyber-crime in general. It is involved and has made several attempts to resolve the issue. It is far from immune to the repercussions of cybercrime, however, and is suffering from a variety of hazards, including ransomware attacks, data breaches, and online fraud. Furthermore, the UK government announced the establishment of a new National Cyber Force (NCF) in November 2020 to combat the rising issue of cybercrime.

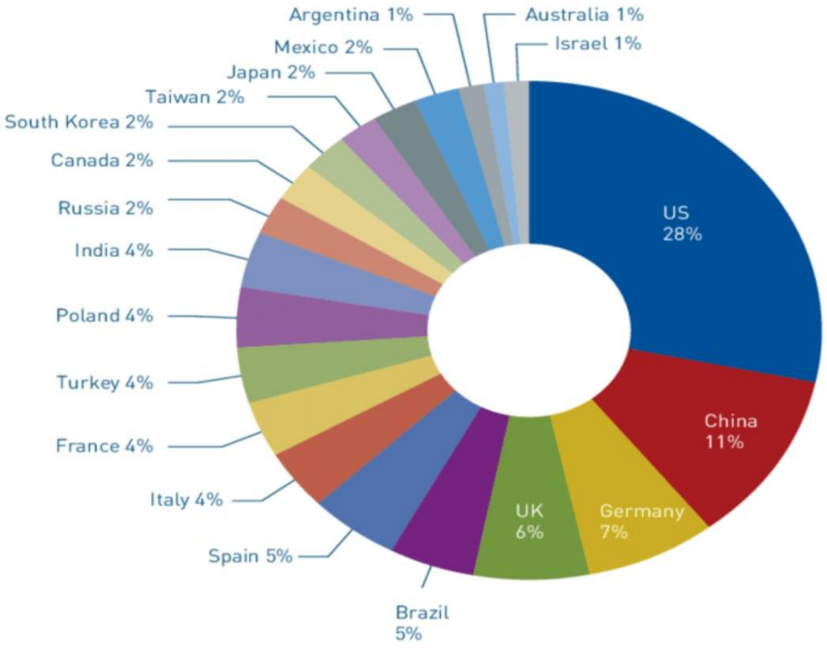

Figure 3: Top 20 Counties Generating Cybercrime[3]

Interpol

The International Criminal Police Organization, established on September 7, 1923, is an international organization that promotes international law enforcement cooperation and crime control. Interpol assists member countries in identifying, triaging, and coordinating their response to cyber threats by developing the Cyber Fusion Centre (CFC), which helps gather together cyber experts from law enforcement and industry to collect and analyze all accessible data on criminal activity in cyberspace in order to provide countries with cohesive, useful insight. By

[3] Top 20-Countries Generating Cyber Crime 15 - Researchgate.net. https://www.researchgate.net/figure/TOP-20-COUNTRIES-GENERATING-CYBER-CRIME-15_fig4_319677972

cooperating with private cybersecurity partners that offer up-to-date intelligence on attacks, patterns, and hazards, it enables police to respond with the most relevant and up-to-date threat information. By issuing reports, the CFC aids governments in creating preventive and disruption policies that prioritize the most immediate concerns while anticipating upcoming threats. In essence, it warns governments about emerging and impending cyber threats. Previously published papers detailed identified dangers such as malware, phishing, corrupted government websites, and social engineering fraud. Since 2017, they have filed over 800 police reports in more than 150 countries.

North Atlantic Treaty Organization (NATO)

NATO's establishment in 1949 to cope with the Soviet Union was one of the most significant occurrences. NATO was not created in response to cyber security concerns since such were not a major concern at the time. However, one of NATO's foundational principles is Article 5 of its charter, which says that any armed assault on one of its members is considered an attack on all. That said, they are now directing their efforts on cyber security risks as well. NATO asserts that they will adapt as cyber threats worsen. "Cyber threats to the Alliance's security are growing more frequent, complicated, damaging, and coercive"[4] according to their website. They will continue to adapt to the changing world of cyber threats, and they depend on robust cyber defenses to carry out the Alliance's key missions of collective security, crisis response, and collaborative security.

United Nations Office on Drugs and Crime (UNODC)

The United Nations Office on Drugs and Crime is a United Nations agency that was founded in 1997 as the Office for Drug Control and Crime Prevention through the merger of the United Nations International Drug Control Program (UNDCP) and the Crime Prevention and Criminal Justice Division. Through its support for national institutions and activities, the UNODC fosters long-term and sustainable development in the field of cybersecurity. UNODC specifically leverages its specialist knowledge in criminal justice system response to offer technical support in capacity development, deterrence and awareness raising, international collaboration, and

[4] Nato. "Statement by the North Atlantic Council in Solidarity with Those Affected by Recent Malicious Cyber Activities Including the Microsoft Exchange Server Compromise." NATO, https://www.nato.int/cps/en/natohq/news_185863.htm?selectedLocale=en

data gathering, investigation, and analysis pertaining to cybercrime. Additionally, the UNODC Global Program on Cybercrime offers targeted technical support to LEDC's in the areas of capacity development, mitigation and awareness building, international collaboration, and investigation of the phenomenon.

BLOCKS EXPECTED

Given that the topic does not include potential conflict or territorial disputes and lacks unambiguous sides or particular allies, the blocks that I expect to be formed will be determined by the general policies of the nations that comprise them. As a result, you are strongly advised against allocating nations with generally diametrically opposed policies to the same alliance.

Bloc A

The first alliance should include countries such as the United States, the United Kingdom, France, and Germany. Each of these nations has been a victim of some of the most significant cyber assaults in history and has therefore made significant endeavors to rectify the issue and continues to combat transnational organized crime in cyberspace on an individual basis. These nations' allies are also anticipated to join the alliance.

Bloc B

The second alliance should be comprised of states such as the Russian Federation, the People's Republic of China, and India, as well as their primary allies. As I previously stated in previous sections, all of these nations have been victims of cybercrime operations throughout history and are therefore highly invested in combatting the issue. Additionally, since some are significant economic powers, they have prioritized cyber-security on their security agenda, placing advanced systems in place to ward against such attacks.

TIMELINE OF EVENTS

Date	Description of event
1988	The Morris Worm attack, the first cyber assault to target global infrastructure occurred
1994	The cyber propaganda war in Chechnya between pro-Chechen and pro-Russian groups occurred. They waged a virtual war by spreading false information about one another, which caused public misunderstanding after their on-the-ground struggle.
1999	Following NATO's bombing of Serbia, pro-Serbian hackers began assaulting NATO's electronic networks. NATO, the United States, and the United Kingdom all had their computers attacked during the conflict.
November 1999	Hackers gained access to the Romanian Ministry of Finance's website in order to impose fraudulent taxes and manipulate the official exchange rate of the national currency.
December 1999	Five hackers in Moscow stole over 5,400 credit card details from online stores belonging to Russians and foreigners, extorting more than $630,000 before being apprehended.
November 2001	The United Nations Convention against Cybercrime was signed.
2007	Russia launched a distributed denial-of-service assault on the Estonian government.
May 2008	Estonia, Germany, Italy, Latvia, Lithuania, the Slovak Republic, and Spain formed the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE).
2010	The computer virus “Stuxnet” was deployed.
2012	The “Red October” attack struck
May 2014	Russia launched a Distributed Denial of Service (DDoS) assault on Ukraine.

March 2014	Russia launched a cyber strike on Ukraine and attempted to influence the country's presidential elections.
June 2015	Chinese hackers seized 21.5 million data records from the United States Office of Personnel Management
May 2017	WannaCry ransomware took place.
June 2017	NotPetya ransomware attack occurred.

RELEVANT UN RESOLUTIONS, TREATIES AND EVENTS

United States Convention against Transnational Organized Crime

The United Nations Convention against Transnational Organized Crime, which was enacted by the United Nations General Assembly in resolution 55/25 on 15 November 2000, is the primary international instrument in the battle against TOC, since it demonstrates Member States' acknowledgement of the gravity of the issues presented by it, as well as the importance of fostering and enhancing close international cooperation to address those problems. States that signed and ratified this convention undertake a series of measures against transnational organized crime, including the establishment of domestic criminal offenses, such as money laundering, corruption, and obstructing justice, the implementation of new and comprehensive frameworks for prosecution, mutual legal assistance, and law enforcement cooperation, and the promotion of educational assistance for the purpose of establishing or upgrading national law enforcement capabilities. [5]

General Assembly Resolution 55/23, January 2001

This resolution notes the importance of, inter alia, law enforcement collaboration in convicting international cases of criminal abuse of information technologies, and exchange of information among States.[6]

General Assembly Resolution 56/121, January 2002

This resolution invites all Member States to incorporate, as appropriate, the work and accomplishments of the Commission on Crime Prevention and Criminal Justice

[5] "United Nations Convention Against Transnational Organized Crime." United Nations : Office on Drugs and Crime, www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

[6] "General Assembly - Quick Links." 1226, www.research.un.org/en/docs/ga/quick/regular/55

and other multilateral institutions when creating national legislation, policy, and practice to counteract criminal misuse of information technologies.[7]

General Assembly Resolution 57/239, January 2003

This resolution underlines the critical need of facilitating the transfer of information technology and capacity development to LEDC's in order to assist them in implementing cybersecurity measures. [8]

General Assembly Resolution 65/230, December 2010

This resolution requests that the Commission on Crime Prevention and Criminal Justice develop an intergovernmental expert committee to undertake a thorough study into cybercrime and the reactions of Member States, the global community, and the private industry, such as the information exchange on national laws, technical support, and global collaboration with the goal of investigating opportunities for reinforcing current infrastructure and proposing new domestic, international and legal responses to cybercrime.[9]

General Assembly Resolution 67/189, December 2012

This resolution calls upon all Member States to enhance their efforts to collaborate, at the bilateral, subregional, regional and international levels to tackle transnational organized crime effectively as well as eradicate its potential repercussions.[10]

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

United Kingdom's National Cyber Force (NFC)

The National Cyber Force (NCF) is a joint venture between defense and intelligence that is responsible for directing in and through cyberspace to respond to threats, preclude and compete those who would do cause harm to the United Kingdom, and to ensure the nation's security. The UK intends to handle cyberattacks as part of its political, economic, and military actions, with the NCF at the forefront of that effort, therefore expanding the UK's competitive advantage as a competent, democratic cyber power. More precisely, the NCF seeks to address threats from terrorists, criminals, and governments that utilize the internet to threaten the

[7] "Combating the Criminal Misuse of Information Technologies :." United Nations Digital Library System, www.digitallibrary.un.org/record/454952.

[8] "Creation of a Global Culture of Cybersecurity :." United Nations Digital Library System, www.digitallibrary.un.org/record/482184

[9] "Un." www.cybercrimelaw.net/un.html.

[10] "UN General Assembly - Resolutions." Welcome to the United Nations, www.un.org/en/ga/67/resolutions.shtml

nation and other democratic countries, as well as risks that compromise the confidentiality, security, and availability of data and services in cyberspace. Finally, it intends to contribute to the United Kingdom's defense activities and to assist in the implementation of the nation's foreign policy objectives.

Federal Bureau of Investigation and the Internet Fraud Complaint Center (IFCC)

The FBI places a high premium on cybercrime investigations and is dedicated to ensuring that law enforcement and the private sector have the tools and safeguards required to counter these crimes. It recognizes that only strong collaboration and coordination among all sectors of government and private sector organizations can ensure the success of efforts to prevent cybercrime. The creation of a proactive approach to investigate Internet fraud via the establishment of an Internet Fraud Complaint Center (IFCC) as a single repository for criminal allegations was a critical milestone in the FBI's efforts to combat cybercrime. The IFCC is a collaborative effort between the FBI and the National White Collar Crime Center (NW3C), a not-profit organization financed in part by the Department of Justice. On a national and international basis, the IFCC is essential to appropriately detect, monitor, and prosecute emerging illegal activities on the Internet. It acts as a hub for the receiving, processing, and distribution of criminal complaints regarding Internet fraud. After Internet fraud reports are collected, they are analyzed, evaluated, and sent to the relevant law enforcement agency by IFCC staff.

Convention Cybercrime

The Convention on Cybercrime, often referred to as the Budapest Convention on Cybercrime, is the world's first international convention addressing Internet and computer crime. It was signed on 23 November 2001 and has 67 signatures at the moment. The Convention aims to harmonize the national criminal substantive law elements of offenses and related provisions in the area of cybercrime, the national criminal procedural law powers required for investigating and prosecuting such offenses, as well as other offenses committed with the aid of a computer system or evidence in digital form, by establishing a prompt and efficient system of international cooperation.

Europe’s Counter-disinformation strategy

Europe has expressed alarm over misinformation and propaganda, while cautioning that there are no simple solutions. Combating misinformation requires a concerted effort on the part of all European institutions. Thus, the EU is collaborating closely with online platforms to urge them to highlight authoritative sources, demote information that has been fact-checked as incorrect or misleading, and remove unlawful or potentially harmful content. For instance, Facebook has addressed the problem and released a report outlining their strategy for combating false news. Similar efforts are likely to be taken by a variety of stakeholders whose companies rely largely on information.

POSSIBLE SOLUTIONS

Without a doubt, cybercrime's transnational dimension necessitates a multinational response. In essence, individual states' acts are inadequate. Thus, all member states must concur on the types of activity that should be prohibited and introduce laws criminalizing such conduct.

Development of international policies

Cybersecurity and cyber peacekeeping are relatively new notions. While cyber-attacks and cyber threats have been around since the 1980s, cyber peacekeeping is a novel concept that is now being discussed and debated. What is apparent is that global regulations must be established in order to create and oversee cyber peacekeeping efforts. Cyber challenges are intensifying, necessitating the deployment of prompt cyber peacekeeping measures. As a result, the necessity of international collaboration is of pivotal importance. This may be accomplished via the development of cooperative international policies and legislation that facilitate the investigation and prosecution of cyber threats.

Redefining the definition of TOC and establishing internationally agreed upon definitions of the different kinds of cyber threats.

As previously stated, the dearth of internationally accepted definitions as well as the lack of clarity in the already existing ones, have impeded attempts to develop effective legal responses to international activity involving any of them. Thus, redefining and further clarifying the definition of TOC as well as the terms cyber-attack, cyberwarfare, and cybercrime, should be a primary objective.

Modifying the structure of networks and databases

When a network consists solely of a central server, a virus that compromises the server may easily infect the whole network. Now if this structure is modified to a decentralized and distributed database, attacks will affect just a single computer on the network, rather than all of them. A decentralized and distributed network is one that does not have a central operator and saves data not on a single computer, but on all computers that are connected to the network.

Developing joint operational tools

Multilateral institutions generally lack the analytical and operational capabilities essential to comprehend and react effectively to the developed edition of cybercrime. Thus, they rely on crime-fighting tactics that were built to combat organized crime before these strategically perilous links between crime, violence, and corruption were fully apparent. Subsequently, even when international organizations detect criminal networks, they have little to no resources and little power over national law enforcement instruments.

BIBLIOGRAPHY

"The 10th Cycon Hosts 700 Cyber Experts in Tallinn." *CCDCOE*, www.ccdcoe.org/news/2018/the-10th-cycon-hosts-700-cyber-experts-in-tallinn/.

Baltic Journal of Law & Politics - Sciendo.com. www.sciendo.com/pdf/10.1515/bjlp-2017-0001.

Common Challenges in Combating Cybercrime - Eurojust. www.eurojust.europa.eu/sites/default/files/Publications/Reports/2019-06_Joint-Eurojust-Europol-report_Common-challenges-in-combating-cybercrime_EN.PDF.

Comprehensive Study on Cybercrime - United Nations Office ... www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

Conference Agenda - Hoover.org. www.hoover.org/sites/default/files/uploads/documents/0817999825_267.pdf.

Convention on Cybercrime - Oas.org. www.oas.org/juridico/english/cyb_pry_explanatory.pdf.

Cyber Attribution: Technical and Legal Approaches and ... sites.tufts.edu/cilg/files/2018/09/attributiondraftsm.pdf.

"Cybercrime Presents a Major Challenge for Law Enforcement." *Europol*, www.europol.europa.eu/media-press/newsroom/news/cybercrime-presents-major-challenge-for-law-enforcement.

"Departments, Agencies and Public Bodies." *Departments, Agencies and Public Bodies - GOV.UK - GOV.UK*, www.gov.uk/government/organisations.

Digital Revolution, Cyber-Crimes and Cyber ... - Core. core.ac.uk/download/pdf/234677092.pdf.

"The FBI's Perspective on the Cybercrime Problem." *FBI*, FBI, 12 June 2001, archives.fbi.gov/archives/news/testimony/the-fbis-perspective-on-the-cybercrime-problem.

Fighting Cybercrime in the Two Europes - Cairn Int. www.cairn-int.info/article-E_RIDP_773_0503--fighting-cybercrime-in-the-two-europes.htm.

Fromiti. "Organized Crime Module 14 Key Issues: Features of the Convention." *Organized Crime Module 14 Key Issues: Features of the Convention*, www.unodc.org/e4j/en/organized-crime/module-14/key-issues/features-of-convention.html.

Fromiti. "Organized Crime Module 14 Key Issues: Features of the Convention." *Organized Crime Module 14 Key Issues: Features of the Convention*, www.unodc.org/e4j/en/organized-crime/module-14/key-issues/features-of-convention.html.

"Index." *United Nations : Office on Drugs and Crime*, www.unodc.org/unodc/en/cybercrime/index.html.

Machan/Liberty DP0 HMACCL0600 REV1 page151 - Hoover. www.hoover.org/sites/default/files/uploads/documents/0817939822_pt6.PDF.

Person. "Transnational Cyber-Security." *ArcGIS StoryMaps*, Esri, 17 May 2021, storymaps.arcgis.com/stories/0b8da27880644843a4dfa241c8a65e7e.

Pritchard, Stephen. "UK Defense and Foreign Policy Review Places 'Cyber' Front and Center." *The Daily Swig | Cybersecurity News and Views*, The Daily Swig, 16 Mar. 2021, portswigger.net/daily-swig/uk-defense-and-foreign-policy-review-places-cyber-front-and-center.

Siber Saldırıların Tarihçesi - NATO. www.nato.int/docu/review/2013/Cyber/timeline/TR/index.htm.

Sign In, storymaps.arcgis.com/stories.

"Significant Cyber Incidents." *Significant Cyber Incidents | Center for Strategic and International Studies*, www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

time, And for the first. "The inside Story of the Biggest Hack in History." *CNNMoney*, Cable News Network, www.money.cnn.com/2015/08/05/technology/aramco-hack/index.html.

Transnational Organized Crime (TOC) - Dni.gov. www.dni.gov/files/documents/NIC_toc_foldout.pdf.

Transnational Organized Crime - Ipinst.org. www.ipinst.org/wp-content/uploads/2015/06/toc_final.pdf.

"Transnational Organized Crime: A Growing Threat to National and International Security." *National Archives and Records Administration*, National Archives and Records Administration, obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime/threat.

"UK Cyber Security and Cyber Crime Statistics in 2022." *Comparitech*, 31 Jan. 2022, www.comparitech.com/blog/information-security/uk-cyber-security-statistics/.

"Un Resolutions." *ITU*, www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx.

"United Nations Convention against Transnational Organized Crime." *United Nations : Office on Drugs and Crime*, www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.

Written by Scott Shackelford, Associate Professor of Business Law and Ethics. "What the World's First Cyber Attack Taught Us about Cybersecurity." *World Economic Forum*, www.weforum.org/agenda/2018/11/30-years-ago-the-world-s-first-cyberattack-set-the-stage-for-modern-cybersecurity-challenges/.

Bedell, Crystal, et al. "What Is a Computer Worm and How Does It Work?" *SearchSecurity*, TechTarget, 30 June 2021, https://www.techtarget.com/searchsecurity/definition/worm.

"Fake News and Cyber Propaganda: The Use and Abuse of Social Media." *Fake News and Cyber Propaganda: The Use and Abuse of Social Media - Новости о Безопасности - Trend Micro RU*, 2017, www.trendmicro.com/vinfo/ru/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media

"Meddling in the Ballot Box: The Causes and Effects of Partisan Electoral Interventions." *The Institute for European, Russian, and Eurasian Studies (IERES)*, 2020, www.ieres.elliott.gwu.edu/project/meddling-in-the-ballot-box-the-causes-and-effects-of-partisan-electoral-interventions/.