Main Model United Nations Conference
Frankfurt am Main, Germany
17th Session
10th to 13th of March 2022

Challenges of a Changing Global Order – Responding to Emerging Conflicts

BACKGROUND GUIDE

CRISIS COMMITTEE

Ann Katrin Korb

Sebastian Renke

Main Model United Nations Conference 2022

1. Introduction

Honourable Delegates,

In the name of the entire team, we welcome you all warmly to the 17th Edition of the MainMUN here in the centre of Germany. We, Ann Katrin Korb and Sebastian Renke will be your chairs for the upcoming days, and therefore, we would like to use the opportunity to introduce ourselves.

I am Ann Katrin, part of MainMUN for seven years since a friend dragged me to one of the team meetings. I haven't left since. When I am not busy attending national and international MUNs either as a delegate, chair, or part of the press, I am studying American Studies in the Goethe University's Master program or working in marketing at a small women-led firm. As I have now filled every possible position in the MainMUN organising team, I can confidently say that chairing is the most fun, so I am looking forward to doing that this year again with you.

My name is Sebastian. I am a recent Goethe University alumnus in the field of political science. My MUN career started in 2015, and I have been excited ever since. After many conferences both as a participant and a member of the organisation team, I am now looking forward to chairing this particular committee and having good discussions and, further, a good time with all of you.

The topic to discuss at the MainMUN 2022 Crisis committee of Foreign Ministers will be:

Cyber Security as a Sitting Duck - Fighting Cyber Terrorism in the Digital Age?

The topic will be presented on the following pages, and we will be able to get into the topic with some optional guiding questions.

At MainMUN do not require position papers but we strongly advise writing them. Our own experience has shown that delegates who take the time to write position papers tend to be more prepared than those who do not. If you write a position paper and hand it in before the deadline you will also receive feedback from us which provides a unique opportunity to feel confident in your preparation.

Be aware that this Background Guide provides you with just basic information on the topic and you, especially as your country's head of delegation, are required to further inform yourself on the topic and your country's position (on the topic as well as your country's policies as a whole). As the system of an interconnected crisis can always take sharp turns, you need to be well prepared to represent your state in a diplomatic manner and you should also be prepared on the topics of the other committees as your fellow country delegation members might need feedback or support from you.

Delegates should keep in mind that while we take diplomatic conduct very serious at MainMUN 2022, the conference is also a simulation. Please be always courteous to your fellow delegates, even if you do not agree with their country's policies and try also to interact with delegates of member states who are important to your own, even if they are not represented by your friends. MUNs are a great place to form new friendships, which we have both experienced in the past, and we hope you get to experience this as well. Do not forget to lobby for your ideas in the committee and outside, as our experience shows that the best deals are made over food and coffee.

The MainMUN 2022 Crisis committee will observe the standard MainMUN Rules of Procedure for the committee work. In addition, the crisis committee will also follow a certain set of rules specific to the crisis and the heads of countries. You will be provided with those rules separately and will also be able to download them from our website.

If you have any remaining questions regarding the committee, feel free to contact us via the Mymun committee chat or later in the process via Ryver.

We are looking forward to the conference. We are excited to meet you all and we expect very interesting and fruitful debates.

With best regards,

Ann Katrin and Sebastian

2. The Crisis Committee at MainMUN 2022

The MainMUN 2022 Crisis committee will pose as this year's crisis committee. The Crisis committee will be staffed with the corresponding foreign secretaries of each represented country during the conference.

MainMUN is a Model United Nations with an interconnected approach. This means that the heads of the country delegations will most likely be on this committee. The delegates in this committee will not only talk about the presented topic but also will have to interact with the other delegates of their country delegation to establish a consistent country policy throughout the conference. As the head of your country delegation, you can issue instructions to the country's delegates in the other committees including the Security Council. The decisions and instructions are solely up to the delegates and will shape the direction of the MainMUN 2022. Therefore, the head delegates have a significant impact and influence on the work done in the other committees.

As an international crisis committee besides the regular structure of the United Nations, the world leaders are going to address the most pressing issues. However, the committee will follow the regular MainMUN Rules of Procedure for committees. In addition to those, the crisis committee will also adhere to the second set of Rules of Procedure which are crisis specific and will be provided to delegates separately. These will explain how the system of directives works and how the members of the crisis committee can use them to perform specific actions during the conference.

The topic of the MainMUN 2022 Crisis committee will be **Cyber Security as a Sitting Duck - Fighting Cyber Terrorism in the Digital Age?**

The Crisis committee will be monothematic but news of other important matters which will need to be debated during the conference can arise at any time. Meaning, delegates should prepare for their country's policies broadly and not just topic specific. Because just like the "real world", you never know what is going to happen tomorrow.

We hope that you are as excited as we are to discuss cyber security and we can have a very fruitful discussion altogether!

3. Cyber Security and Cyberterrorism

Data breaches of social media platforms and email providers, the selling of personal data, hacking of personal and business networks – these are just a few examples of cyber-attacks. Over the last years, the chance that you might be a personal victim of cybercrimes at least once in your life has increased significantly. Additionally, our digitalised world offers a valuable target for cyber terrorists and cyber warfare. State and non-state actors may influence you indirectly via election meddling, leaking of national security data, attacks on national infrastructure and many more.

Asymmetric warfare is not a new concept, but our digitalised world opens new possibilities here. It is often much easier, and much cheaper, for countries and non-state terrorist groups to fight their wars not physically but make use of cyberspace. Nations can employ non-state actors to meddle with the national security of other nations and might be successful to the point, that the origin of the attack may never be revealed. Thus, cyber terrorism is gaining ground.

The Crisis committee will have to deal with the question of how nations can prevent possible attacks on their infrastructure and economy. Sharing information between nations can have significant advantages for all interacting states but imposes security issues as well. The delegates need to find the right way to address the issues at hand to protect citizens not only via protecting their governments from possible cyber-terrorism but also the citizens in their use of the cyberspace as well.

3.1. Terms and Definition

To understand the issue at hand, the next chapter will give some insight and define the major concepts.

Cyberattack

Cyberattacks are also known as Computer Network Attacks (CNA) and exploit computer systems, technology-dependent enterprises, and networks. They change computer codes, logic or data via malicious code and can compromise data. Additionally, these CNAs can lead to cybercrimes like identity and information theft (Techopedia.com 2019a).

Cyberattacks can include but are not limited to, offences such as system infiltration, viruses, password sniffing, identity theft, fraud, spyware, instant messaging abuse and Denial of Service (DoS) on the digital side, but also the theft of hardware, such as mobile devices or laptops.

Denial of Service attacks in which an abundance of requests and messages are sent to servers, using up their resources and therefore locking out users are probably one of the more famous ones, especially in targeting citizens rather than governments (Technopedia.com 2019b).

Cybercrime

Online banking information theft, identity theft, online predatory crimes and unauthorized computer access are all cybercriminal activities. Those activities can typically be divided into two categories: crimes that target computer networks or devices and crimes that use computer networks to advance other criminal activities (Technopedia.com 2019c). Additionally, cyberterrorism is also part of cybercrime.

Cyberterrorism

As mentioned earlier, cyberterrorism is a subdivision of cybercrime. Cyberterrorism thereby digitalizes the logic of asymmetric warfare. A small entity attacks a bigger player. The process inherits an imbalance of power between the opponents. Cyberterrorist attacks target weaknesses in computer systems, computer data or programs (Technopedia.com 2019d). Unlike cybercrimes on private actors with the intention of personal enrichment, cyberterrorism targets foremost public actors by causing harm and destruction. Due to a definition of the European Union Agency for Law Enforcement Training (CEPOL), cyberterrorist attacks intend "to coerce a civilian population and influence policy of target government or otherwise affect its conduct." (CEPOL n.d.) A preferred target of cyberterrorism is critical infrastructure (definition see below). However, cyberterrorism must be differentiated from hacktivism and cyber warfare. A small entity attacks a bigger player

Cyberwarfare

Cyberwarfare translates the logic of war, states attacking states, into the cyber space. Therefore, cyberwarfare is the use of cyberspace of a state actor to harm the state security of a country by attacking its computer and information systems. This differentiates cyberwarfare from cyberterrorism. In contrast to cyberterrorism, it is only instigated from one nation to attack another nation and does not follow the logic of asymmetric warfare of a non-state actor attacking a state actor. It can involve third party actors, but only acting on behalf of a state. It usually involves either sabotage or espionage (Technopedia.com 2019e). All cyberwarfare is cybercrime but not all cybercrime is cyberwarfare.

Critical Infrastructure

The U.S. Department of Homeland Security defines critical infrastructure as follows: "Overall, there are 16 critical infrastructure sectors that compose the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. The National Protection and Programs Directorate's Office of Infrastructure Protection (IP) leads the coordinated national effort to manage risks to the nation's critical infrastructure and enhance the security and resilience of America's physical and cyberinfrastructure." (www.cisa.gov n.d.)

The definition of the European Commission does not differ too much from the U.S. definition: "Critical infrastructure is an asset or system which is essential for the maintenance of vital societal functions. The damage to critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the EU and the well-being of its citizens." (BRIEFING Implementation Appraisal, n.d.).

It is apparent, that critical infrastructure is an important sector for society and therefore protection of it must be a priority for governments. This sector includes, for example, the emergency services sector, the government facilities sector, the financial services sector, and many more which are essential to the way a country is running, meaning attacks on critical infrastructure could have devastating effects on the citizens and their life.

3.2. Framework

The international legal framework regarding cybercrime and cyberterrorism is highly fragmented. There are no internationally binding rules and regulations in place. This background guide presents some regulations with the utmost importance in the next segment.

3.2.1. Convention on Cybercrime (Budapest Convention)

The discourse regarding cybercrime often refers to the Convention on Cybercrime, also called Budapest Convention. This document was negotiated by the Council of Europe in 2001 and came into action in 2004.[1] Since 2001 66 nations have joined the treaty including states outside the Council of Europe like Japan, the USA, the Philippines or Ghana. The BRIC states reject to accede to the treaty thus far. However, the invitation of the Council to India has validity until December 2024 (Council of Europe n.d. a). There is no open invitation to the other mentioned states.

What did the convention codify? Art. 15 calls upon the member states to implement domestic legislation "which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention

[1] See the full list here

for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality." The convention itself does not set a legally binding framework but calls for the implementation of national legislation for the first time. These laws must specifically include the following crimes: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, offences related to infringements of copyright and related rights. The Council of Europe and its international partners did not specifically address the issue of international cyberterrorism. However, it addresses the means of financing said terrorism (see chapter 4.4).

The convention includes two additional protocols. The first one is open for signatures since 2003 and criminalizes acts of racist and xenophobic nature in cyberspace. The second one is still pending. The Council expects the opening for signatures in March 2022. The second protocol intensifies the cooperation and disclosure of digital evidence.

The treaty lays thereby the internationally binding foundation for the prosecution of cybercrime on a national level. In this regard, the Budapest Convention is highly influential. According to the Council of Europe, 158 states used the convention as a guideline or source for their domestic legislation.

3.2.2. Salvador Declaration

The Salvador Declaration or Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World was passed as a result of the 12th UN Congress on Crime Prevention and Criminal Justice from the 12th-19th of April 2010 in Salvador, Brazil. The goal was to "take more effective concerted action, in a spirit of cooperation, to prevent, prosecute and punish crime and seek justice" (Declaration Preamble). According to the Council of Europe, the states discussed ideas based on the Budapest Convention but also other ideas for a treaty (Council of Europe 2010). Even though the declaration was specifically mentioned in the draft, it was not included in the final document (Council of Europe 2010). Cybercrime is specifically mentioned in §§ 41 and 42. § 41 instructs the United Nations Office on Drugs and Crime to assist UN member states via technical assistance and training "to improve national legislation and build the capacity of national authorities, in order to deal with cybercrime". Specifically, the Declaration mentions "the prevention, detection, investigation and prosecution of such crime in all its forms, and to enhance the security of computer networks" as a national task. § 42 invites all interested parties to set up an "intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by the Member States, the international community and the private sector. "

In conclusion, the declaration defines cyber security as a national task.

3.2.3. Madrid Guiding Principles

The Madrid Guiding Principles are 35 guidelines for UN member states presented by the counter-terrorism committee of the Security Council "to stem the flow of foreign terrorist fighters". It is consistent with the Security Council Resolution S/2015/939. The guiding principle focuses mainly on physical terrorism, less on cyber-terrorism. However, it is a concise set of guidelines for member states to encounter and to rise preparedness for an external terrorist attack. Like the Budapest Convention, the Madrid Guiding Principles are not legally binding international law in itself but call upon the member states to implement national legislation and encourage international cooperation.

The Madrid Guiding Principles address cyberterrorism briefly in Principles 25 and 26. Guiding principle 25 encourages the UN member states to review their national legislation. The goal is "that evidence collected through special investigative techniques or from countries of destination or evidence collected through ICT and social media, including through electronic surveillance, can be admitted as evidence in cases related to foreign terrorist fighters […]" (Madrid Guiding Principles 2015). The process to do so shall thereby never infringe international Human Rights Law and especially the freedom of expression. Guiding Principle 26 asks the UN members to "build ICT and forensic capacities and expertise within national law-enforcement agencies and [to] strengthen the capacity of law-enforcement agencies to monitor social media content related to terrorism in order to prevent the flow of foreign terrorist fighters." (Madrid Guiding Principles 2015) Again, international Human Rights law should be held in high regard.

3.3. Relevant UN Resolutions on Cybercrime, Cyber Security, and Cyberterrorism

Cyber security is a relatively new concern when compared with other problems the United Nations deals with. However, the member states were able to come to a common ground on certain aspects and to pass several relevant resolutions.

3.3.1. A/RES/73/27 and A/RES/73/266

In December 2018 the UN General Assembly adopted resolution A/RES/73/27 on "Developments in the Field of Information and Telecommunications in The Context of International Security". Focussing on the peaceful use of Information and Communication Technologies (ICTs) this resolution promotes state and non-state actors to work together, as well as different nations, in information sharing and upkeeping human rights in cyberspace. This resolution also set up an Open End Working Group (OEWG) to "to further develop the rules, norms, and principles of responsible behaviour of States […], and the ways for their implementation" (A/RES/73/27) consisting of all UN member states and working on a consensus basis. The Working Group handed its Final Substantive Report in on March 10th, 2021. As expected, the report contains suggestions instead of substantive regulations. However, it calls for Rules, Norms and Principles for Responsible State Behaviour. These measures should be discussed and drafted by the Open-ended Working Group on the security of and in the use of information and communications technologies 2021-2025 established by A/RES/75/240 established. Furthermore, called the working group on strengthening the international law.

Also, in December 2018 the General Assembly adopted a second resolution on "Advancing Responsible State Behaviour in Cyber-space in the Context of International Security" (A/RES/73/266). A/RES/73/266 sets up another Group of Governmental Experts (GGE) on cyberspace consisting of 25 members to study the question of norms and behaviours in cyber-space. This group will work closely together with different regional organizations such as the AU, EU, and ASEAN. Working in a smaller group of experts can have the advantage of finding solutions quicker, however, it also involves a selection process of the members, omitting opinions of the UN members who are not part of that GGE.

Both resolutions do not mention cyber security but focus instead on ICTs. They were both sponsored and supported by different groups in the United Nations as they overlap in some points but have varying points of concern depending on the member state. Both draw inside information from the Group of Experts on ICTs which has been established following a 1998 resolution. Since then, this group has set up rules, norms, and principles of responsible behaviour of States which are included in A/RES/73/27 voted upon in 2018. "Developments in the Field of Information and Telecommunications in The Context of International Security" was also the title of resolutions of the General Assembly in the past such as A/RES/71/28 of 2016, A/RES/69/28 of 2014 and A/RES/68/243 of 2013. This shows that the international stage has realized the high importance of cyber security and continues to take steps towards guidelines, information sharing, safety measures and other necessary measures to provide cyber security not just for citizens directly but also by ensuring state security and therefore important infrastructure.

3.3.2. A/RES/64/211

Lastly, the resolution A/RES/64/211 "Creation of a global culture of cyber security and taking stock of national efforts to protect critical information infrastructures" was adopted in 2010 (A/RES/64/211). It strengthens the results of the resolutions above and invites again all member states to work together. The resolution contains just two operative clauses, yet a lot of preambular clauses. However, there is an annex to the resolution. It contains a voluntary self-assessment tool for national efforts to protect critical information infrastructures which gives practical advice and general guidelines on how to establish and implement cyber security on the state level. This resolution is based on a previous resolution, A/RES/58/199 "Creation of a global culture of cyber security and the protection of critical information infrastructures".

3.3.3. A/RES/55/63 and A/RES/56/121

Other important resolutions regarding cyber security are older. The resolutions A/RES/55/63 and A/RES/56/121 – both named "Combating the criminal misuse of information technologies" (A/RES/55/63 and A/RES/56/121) – were adopted in 2001 and 2002 respectively and deal with the important issue of misuse of information technologies. In these resolutions, the UN member states note the work done by the European Union (see Budapest Convention), the G8 and others and call for international standards.

3.4. Problems and Risks

3.4.1. Recent Cyber Attacks

State and non-state actors can interfere with the sovereignty of an independent state. A vivid example is election meddling, most prominently the Russian interference in the 2016 presidential elections. First clues for an alleged hacking appeared back in 2014, attempting to influence the previous election (Ferguson 2019). The voting machines commonly used in the US elections served as a weak spot. With being electronic and connected to the internet these machines offered the perfect entry point. While there is no certain evidence of Russia changing the outcome of the votes, it also remains unclear why they interfered in the first place.

Another example of a severe attack with an unknown source was a DoS attack on the critical infrastructure of Tallin, Estonia in 2007. Following the removal of a Soviet monument the Russian minority in Estonia and subsequent violently protested leaving 150 people injured. To make things worse, the incidents were paired with false Russian news agency reports. On April 27, 2007, hackers hit Tallin's critical infrastructure with a severe DoS attack targeting the president, the parliament, banks and media outlets. As a result, the internet was inaccessible for weeks, disrupting online banking and the workflow of the highly digitalised administration (Ferguson 2019). As one of the first cyberattacks of this scale, it raised awareness of the international community on network security and led to the creation of the Cooperative Cyber Defense Center (CCDC) in 2008. This NATO based centre has been followed by the launch of the European Union Agency for Network and Information Security (ENISA) by the European Union to help the members with questions of cybersecurity (Herzog 2011).

The Ukraine was victim of the first known successful cyberattack on a power grid in December 2015, which left more than 230,000 citizens without power. While the nations grid is protected via different control centers and firewalls, it was not enough to stop the attack. In this case individual employee accounts were hacked to access internal databases and destroy the IT systems from within (Zetter 2016).

Probably the most famous so-called “computer worm” is the, in 2010 discovered, computer worm “Stuxnet”. With just 500kb of data needed to implement it, it was transferred via a USB drive to attack multiple Iranian facilities (Holloway 2015). It was observed that a “strange number of uranium enriching centrifuges were breaking” (Holloway 2015) in the Natanz nuclear facility in Iran by the International Atomic Energy Agency in 2010. While suspicious, the direct cause of this was unknown at the time. When Iranian technicians hired a Belarusian security firm later in the year to check their computer systems, it was discovered that malicious files of the Stuxnet worm were the cause for the damages (Holloway 2015). Stuxnet became famous because it not only destroyed the computer systems but also critical equipment, taking it out of the digital realm into the real world (Zetter 2014). While never officially acknowledged, it is widely recognized to have been created by both intelligence agencies of the United States of America and Israel (Frulinger 2017) in an attempt to influence the Iranian development of nuclear weapons.

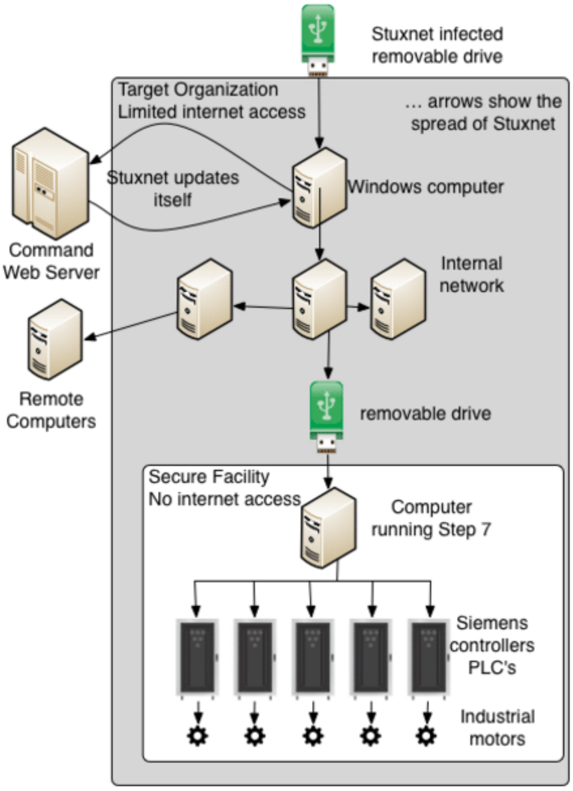

Figure 1: How Stuxnet Spreads (Connell, Anne & Palko, Tim & Yasar, Hasan. (2013).

In 2016 about $81 million US Dollar were stolen from the central bank in Bangladesh by the notorious hacking group „Lazarus“ (Businesswire 2017). This has been the largest cyber heist since the invention of the internet. Further attacks on other national banks were planned by interrupted by cybersecurity firms (Businesswire 2017). Lazarus is suspected to be behind the attacks on the Polish financial sector in 2017 due to findings of Lazarus wiper tools in some Polish bank computers (GReAT 2017).

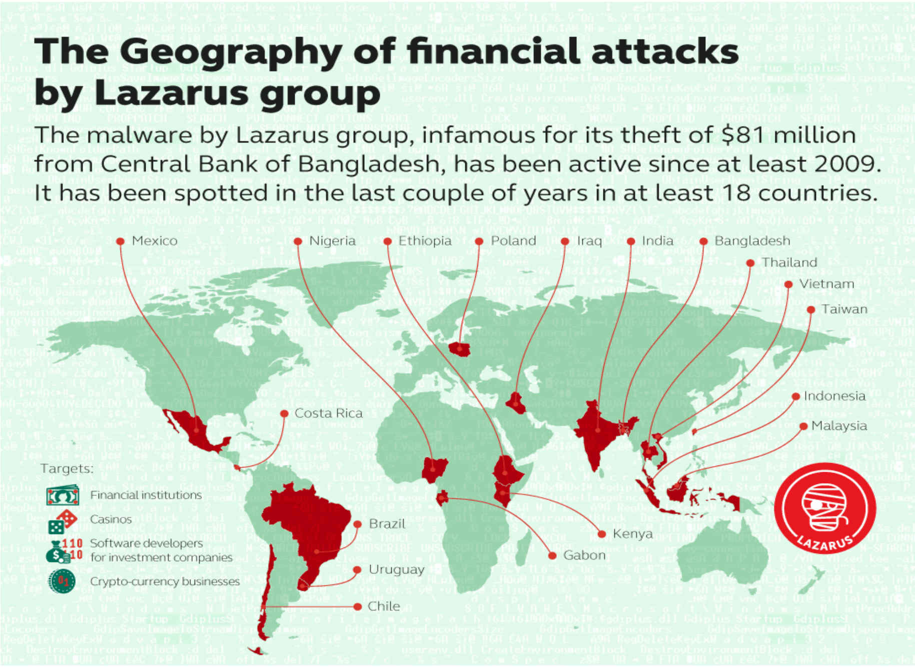
The Geography of financial attacks by Lazarus group
The malware by Lazarus group, infamous for its theft of $81 million from Central Bank of Bangladesh, has been active since at least 2009. It has been spotted in the last couple of years in at least 18 countries.
Mexico
Nigeria
Ethiopia
Poland
Iraq
India
Bangladesh
Thailand
Vietnam
Taiwan
Indonesia
Malaysia
Costa Rica
Brazil
Kenya
Gabon
Uruguay
Chile
Targets:
Financial institutions
Casinos
Software developers for investment companies
Crypto-currency businesses
LAZARUS

Figure 2 The Geography of financial attacks by Lazarus group (GReAT 2017)

The Lazarus group first emerged in 2009 and has since attacked cyber systems in at least 18 countries around the globe (GReAT 2017). Before the group started attacking banks, it was notorious for conducting

„cyberespionage and cybersabotage activities“ like leaking loads of internal data from Sony Pictures Entertainment (GReAT 2017).

While their motives seemed only malicious towards companies in the beginning of the group, the heist on the Bangladeshi bank kicked off their interest in financial gains via cyber terrorism. Furthermore, they have executed multiple so-called „Bluenoroff watering hole attacks“ in Mexico, Australia, Uruguay, Russia, Norway, India, Nigeria, Peru and Poland (GReAT 2017). In addition, the tracking of IP addresses has led to North Korea where cybersecurity experts suspect the origins of the Lazarus group.

3.4.2. The Role of Social Media

We have attacks that are conducted via the internet and crimes conduced with the internet as a tool. The first category features typically crimes like fishing for private data e.g. credit card numbers etc., fraud or application of viruses like a trojan. The second category is classified as crimes that are using the internet as a platform for their crimes, such as spreading child pornography or recruiting new members for a terroristic group e.g. via social media (United Nations: United Nations Office on Drugs and Crime, 2013).

Algorithms of social media platforms can make it easy to recruit members which have already been part of a specific social media “bubble” because they are more susceptive to blindly believe those that fall into the same believe systems as them. To curb indoctrination via social media, the nations must work together with the private companies owning the platforms, to find solutions on the spread of false information and propaganda.

In contrast to the malicious use of social media, Interpol uses social media channels and their contents to find suspects and witnesses of terrorist attacks (Interpol, n.d.). Interpol states, that they have used platforms to “identify potential witnesses, as was the case following the London Bridge attack in the UK in 2017, and the attack at a hotel complex in Nairobi, Kenya, in January 2019“ and that they are also using facial recognition tools on content uploaded to those platforms, to “support member countries in their investigations”.

3.4.3. Lack of International Cooperation

Besides the beforementioned Budapest Convention, just a few other international partnerships are challenging cybercrime on an international level. Especially the European Union fights cybercrime with a cross-border approach. The European Union Agency for Cyber Security or ENISA was founded in 2004 and has been fighting cybercrime since. Interpol combats cybercrime on an international level cooperatively and universally. Other organizations like NATO fight these crimes with a political purpose and a clear opponent. Additional attempts are geographically closed. The OECD started to set a common set of rules to protect the privacy and the flow of personal data in the 1980s. The *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD

Guidelines 2013) were a great milestone for the framework that protects the privacy and private data. The guidelines were updated in 2013 and contain a more modern approach (OECD Privacy Framework 2013). The only international organization fighting cybercrime is the United Nations Office on Drugs and Crime (UNODC). However, the fight against cybercrime is just a subtask in the greater goal to fight organized crime. A specialized organization did not come into action yet.

Protection against and prosecution of cybercrimes are still primarily a national issue. For instance, the US wrote a special strategy to prevent the theft of US trade secrets in the light of increasing cyber-attacks in 2013.[2] This leads to another problem, the national jurisdiction. States can limit access to the internet or set up laws that economic companies must follow, but this does not apply universally.[3] Bernard H Oxman even argues that there is a national right to prosecute foreign crimes on national territory, e.g., cybercrimes against national security architecture. Yet, there is still no national right to persecute national crimes on foreign territory, meaning there is a conflict of jurisdiction.[4]

To put it briefly, cybercrime is fought in several but not connected actions. An international task force that coordinates the international war against cybercrimes is still not in action. Measures are still primarily executed by national states.

3.4.4. Financing of Cyberterrorism

Modern times require modern resolutions. The same goes for funding cyberterrorism. Today a lot of non-traceable funding is done via the cyberspace. The implementation of online currencies, such as bitcoins, which work via block- chain provides almost endless options for financing. Especially block-chains are hard to impossible to trace, so the source of money may never be discovered. Further, money laundering in the digital age is an also much easier for criminals than using offline methods.

One way to finance cyber terrorism, besides the obvious country financing to attack opponents, is cybercrime. This can take many different forms such as simple payment fraud, schemes to steal from the normal internet, sexual abuse material is usually sold via the dark net. The dark net is also used to sell illegal substances and armoury, all either to finance individuals or groups, with often malicious intent. Europol (2019) claims, that over 90% of identified money mule transactions are linked to cybercrime. This includes, but is not limited to, "Phishing, malware attacks, online fraud, e-commerce fraud, business e-mail compromise and CEO fraud, romance scams, holiday fraud and many others" (Europol 2019). The gains from these types of cybercrimes can be solely to the financial

[2] E.g.: Executive Office of the President of the United States, Administration Strategy on Mitigating the Theft of U.S. Trade Secrets, Washington, D.C., February 2013, https://www.justice.gov/criminal-ccips/file/938321/download

[3] Bernard H. Oxman, »Jurisdiction of States«, in: Rüdiger Wolfrum (Hg.), Max Planck Encyclopedia of Public International Law, Online Edition, Oxford. 2014,

[4] Further reading: Benedikt Pirker, »Territorial Sovereignty and Integrity and the Challenges of Cyberspace«, in Katharina Ziolkowski (Hg.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, Tallinn: NATO CCDCOE, 2013, S. 189–216.

benefit of individuals but more often they are used to fund lager cyberattack groups partaking in cyberterrorism.

The next level of cybercrime can be the hacking of banks and financial institutions which can both be seen as cybercrime as well as cyber terrorism. See 4.1 for examples.

While international organizations have been cracking down on terrorist financing, most of the transactions have been moved to the cyberspace, making it impossible to track the flow of funds in most cases. Cryptocurrencies are a lot harder to track (sometimes not at all) than regular monetary funds. Darknet websites such as “Fund the Islamic Struggle without Leaving a Trace” are used to transfer bitcoins to jihadis (Wang and Zhu 2021). As Islamic law allows the use of cryptocurrencies, most of the terrorist groups funding is done via bitcoin today (Wang and Zhu 2021).

As some of their financing comes from private and institutional donors, the terrorists also accrue large sums by trading bitcoins in exchange for private data that has been hacked before (Hampton and Baig 2015). “In January 2016, criminals used ransomware to control the computers of the Lincoln Group, demanding a ransom of 500 USD worth of Bitcoin, but they ultimately failed. In November 2015, three Greek banks received blackmail threats, demanding payment of hundreds of thousands of euros in Bitcoin” states Brown (2016). As the general population becomes more and more involved in cryptocurrencies, terrorist groups also increase their use of the cyberspace for malicious activities. The “anonymity, decentralization and globalization” (Feng and Ding 2019) as well as “the irreversibility of cryptocurrency transactions and low transaction costs” (Brill and Keene 2014) are the reasons why it is so attractive for terrorist financing.

To prevent the financing of terrorists, anti-money laundering/anti-terrorist financing (AML/ATF) measures must be strengthened. He et al. (2016) argue that counter-terrorism financing has a good pre-prevention mechanism that can effectively prevent terrorist financing. In the case of funding via cybercrime, states must implement stronger observation of the cyberspace, increase security in critical infrastructure as well as in the financial and governmental sectors and educate their citizens on the safe use of the internet. In addition, they must cooperate to establish regulatory systems for cryptocurrencies. There are many aspects delegates must consider in their fight against cyberterrorism and its funding. individuals as well as the selling of sexual material. The latter often goes hand in hand with other crimes such as the exploitation of minors or adults.

3.5. Guiding Questions

- What position does my country have on the issue cybercrime and cyberterrorism?
- Is there a need for a consolidation of national legal frameworks on an international level?
- The number of cyberattacks rise. Is the current legal framework sufficient? If no, what measures can be done to strengthen it?
- How can the financial means of cyberterrorist be dried out properly?

- Should be there an international regulation for social media to prevent recruiting and hate speech?

3.6. Further Reading

1) Budapest Convention
2) The OECD Privacy Framework
3) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98)
4) You can find a long list of significant cyberattacks here: CSIS
5) Read up on specific cyber-attacks in the country you are representing.
6) A/RES/55/63, A/RES/56/121, A/RES/57/239, A/RES/64/211, A/RES/68/243, A/RES/69/28, A/RES/71/28, A/RES/73/266, A/RES/73/27, A/RES/73/27 (To find out your countries position on this topic)

3.7. Sources

Briefing Implementation Appraisal. (n.d.). [online] Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf.

CEPOL. (n.d.). cyberterrorism. [online] Available at: https://www.cepol.europa.eu/tags/cyberterrorism.

Council of Europe (n.d. a): Non-members States of the Council of Europe. Five years validity of an invitation to sign and ratify or to accede to the Council of Europe's treaties [online] Available at: https://rm.coe.int/16806cac22.

Council of Europe (n.d. b): 20th anniversary Budapest Convention. [online] Available at: https://www.coe.int/en/web/cybercrime/key-facts#{%22105028002%22:[2]}.

Council of Europe (2010): 12th UN Congress on Crime Prevention and Criminal Justice (Salvador, Brazil, 12-19 April 2010). Summary of outcome regarding cybercrime. [online] Available at: https://rm.coe.int/16802fa42d.

Brown S. D. (2016). 'Cryptocurrency and Criminality. The Bitcoin Opportunity.' The Police Journal 89(4): 327–339.

Connell, Anne & Palko, Tim & Yasar, Hasan. (2013). Cerebro: A platform for collaborative incident response and investigation. 2013 IEEE International Conference on Technologies for Homeland Security, HST 2013. 241-245. 10.1109/THS.2013.6699007.

Europol. (2019). Money Muling. [online] Available at: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/money-muling.

Feng S., Ding J. (2019). 'Money Laundering Risk in Digital Cryptocurrency Transactions: Evidence and Enlightenment.' International Financial Research 7: 25–35.

Ferguson, Scott. (2019) Russia Targeted All 50 States During 2016 Election: Report. [online] www.govinfosecurity.com. Available at: https://www.govinfosecurity.com/russia-targeted-all-50-states-during-2016-election-report-a-12838.

Fruhlinger, J. (2017). What is Stuxnet, who created it and how does it work? [online] CSO Online. Available at: https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.

GReAT (2017). Lazarus Under The Hood. [online] Securelist.com. Available at: https://securelist.com/lazarus-under-the-hood/77908/.

Hampton N., Baig Z. A. (2015). Ransomware: Emergence of the Cyber-Extortion Menace. Perth: SRI Security Research Institute, Edith Cowan University.

He D., Haksaret V., Almeida Y. et al. (2016). 'Virtual Currency and Its Expansion: Preliminary Thinking.' Research on Financial Supervision 4: 46–71.

Herzog, Steven. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security, 4(2), pp.49–60.

Holloway, M. (2015). Stuxnet Worm Attack on Iranian Nuclear Facilities. [online] Stanford.edu. Available at: http://large.stanford.edu/courses/2015/ph241/holloway1/.

www.interpol.int. (n.d.). Analysing social media. [online] Available at: https://www.interpol.int/Crimes/Terrorism/Analysing-social-media.

Oecd.org. (2013). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD. [online] Available at: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

OECD (2013). THE OECD PRIVACY FRAMEWORK. [online] Available at: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Techopedia.com. (2019a). What is a Cyberattack? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/24748/cyberattack.

Techopedia.com. (2019b). What is a Denial-of-Service Attack (DoS)? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/24841/denial-of-service-attack-dos.

Techopedia.com. (2019c). What is Cybercrime? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/2387/cybercrime.

Techopedia.com. (2019d). What is Cyberterrorism? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/6712/cyberterrorism.

Techopedia.com. (2019e). What is Cyberwarfare (Cyber War)? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/13600/cyberwarfare.

United Nations: United Nations Office on Drugs and Crime (2013). COMPREHENSIVE STUDY ON CYBERCRIME - Draft February 2013. [online] Available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

Wang, S. and Zhu, X. (2021). Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing. Policing: A Journal of Policy and Practice.

www.businesswire.com. (2017). Chasing Lazarus: A Hunt for the Infamous Hackers to Prevent Large Bank Robberies. [online] Available at: https://www.businesswire.com/news/home/20170403006303/en/Chasing-Lazarus-A-Hunt-for-the-Infamous-Hackers-to-Prevent-Large-Bank-Robberies.

www.cisa.gov. (n.d.). Supporting Policy and Doctrine | CISA. [online] Available at: https://www.dhs.gov/what-critical-infrastructure.

Zetter, Kim (2014). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. [online] WIRED. Available at: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

Zetter, Kim (2016): Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Retrieved from: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/#.