AKADEMISCHES
FORUM FÜR
AUSSEN-
POLITIK

UNION
ACADEMIQUE
DES AFFAIRES
ETRANGERES

ACADEMIC FORUM FOR FOREIGN AFFAIRS

UNITED NATIONS YOUTH AND STUDENT ASSOCIATION OF AUSTRIA

EISENSTADT - GRAZ - INNSBRUCK - KLAGENFURT - LINZ - SALZBURG - VIENNA

VIMUN

VIENNA INTERNATIONAL MODEL UNITED NATIONS
04 - 08 August 2019

Preparation Paper/Study Guide:

United Nations Office on Drugs and Crime (UNODC)

Simulation of a Meeting of the
Commission on Crime Prevention and Criminal Justice (CCPCJ)

"Finding Measures to Prevent Cybercrime"

Table of Content:

1. Introduction:

The United Nations Office on Drugs and Crime (UNODC) is responsible for the abatement of illegal drugs and international crime. The corps was established in 1997 as a result of the merge of the United Nations Drug Control Programme and the Centre for International Crime Prevention. The UNODC works in various regions of the world with an enormous network of field offices. The main part of the budget comes from voluntary contributions (~90%). (*see*: UNODC)

The headquarter is located in Vienna, Austria. Around 500 staff members are working in the office in Vienna. The field of work of the United Nations Office on Drugs and Crime is many-faceted – for example: Human Trafficking. It stretches from drug abuse prevention and drug dependence treatment and criminal justice reform to tackling organized crime and terrorism or corruption and economic crime. (*see*: UNODC Annual Funding Appeal)

The United Nations Office on Drugs and Crime assists Member States in their efforts against illicit drugs, crime and terrorism. There are three main aspects of the work programme:

> Field-based technical cooperation projects to enhance the capacity of Member States to counteract illicit drugs, crime and terrorism;
>
> Research and analytical work to increase knowledge and understanding of drugs and crime issues and expand the evidence base for policy and operational decisions;
>
> Normative work to assist States in the ratification and implementation of the relevant international treaties, the development of domestic legislation on drugs, crime and terrorism, and the provision of secretariat and substantive services to the treaty-based and governing bodies.

(*see*: UNODC)

The education of people concerning the dangers of drugs and drug abuse and the strength of international actions against illicit drug production and trafficking is one of the main goals of the United Nations Office on Drugs and Crime. To reach this goal, the office started many initiatives, including alternatives in the area of illegal drug crop cultivation and the implementation of projects against money laundering. (*see*: UNODC) Another very important part of their work is the improvement of crime prevention and assist with criminal justice reform. In 2002, the General Assembly approved an expanded program of activities for the Terrorism Prevention Branch of the United Nations Office on Drugs and Crime. These activities focus on providing assistance to states, on request, in the ratification and implementation of the 18 universal legal instruments against terrorism. (*see*: UNODC)

As already mentioned, the United Nations Office on Drugs and Crime has around 20 field offices in over 150 countries. The staff is collaborating directly with governments and non-governmental organizations. The staff members develop and implement drug control and crime prevention programs, which were made to the countries' particular needs. (*see*: UNODC) This collaboration should lead to reach the target of fulfilling the work on the Sustainable Development Goals. The United Nations Office on Drugs and Crime work especially on these SDG's: Good Health and Well-Being (3), Gender Equality (5), Clean Water and Sanitation (6), Decent Work and Economic Growth (8), Reduced Inequalities (10), Sustainable Cities and Communities (11), Life below Water (14), Life on Land (15), Peace, Justice and Strong Institutions (16) and Partnerships for the Goals (17). (*see*: UNODC – The Sustainable Development Goals)

2. Background information about the topic:

Cyber Crime if the greatest threat to every company in the world

Ginni Rometty (CEO of IBM)

2.1. What is Cybercrime?

2.1.1. Definition:

Firstly, we need to understand what cybercrime is. Therefore, the following definition is added: "Cybercrime is any criminal activity that involves a computer, networked device or a network." (*see*: SearchSecurity) Mostly, the financial aspects play an important role and there are various types of profit-driven criminal activities. The United States Department of Justice created three different categories:

- crimes in which the computing device is the target;
- crimes in which the computer is used as a weapon;
- crimes in which the computer is used as an accessory to a crime.

The Council of Europe Convention on Cybercrime has established an own definition of this issue, saying: "[…], defines cybercrimes as a wide range of malicious activities, including the illegal interception of data, system interferences that compromise network integrity and availability, and copyright infringements." (*see*: SearchSecurity) It is also mentioned that other forms can include the sale of illegally bought items (e.g. weapons, drugs,…) or the solicitation, production, possession of distribution of child pornography. (*see*: SearchSecurity)

2.1.2. How does Cybercrime work?

Criminals use a wide range of methods to achieve their goals. Those methods change constantly. The common types are:

- Distributed DoS attacks (DDoS) – this method is used to shut down a system or network. Therefore, the network's communication protocol is used against itself by overwhelming the capabilities for responding to connection requests.
- Malware – here we talk about an infection of systems of networks. Malware is used to damage a system of harm users by demanding the system or data saved in the system.
- Phishing – this infiltration of networks includes sending fraudulent mails to users in an organization tempting them to download added files or simply click on links. The result is that the system or network is going to be infiltrated with a virus of malware.
- Credential attacks – this method is used to steal IDs or passwords for accounts. A key sniffer can be installed to expose the victim's credentials.
- Hijack – criminals may attack a website to change or delete some content or to access or modify databases without authorization. Therefore, a SQL injection (is a type of security exploit in which the attackers add Structured Query Language [SQL] code to a web form input box to gain access to resources or make changes to data) is used to insert malicious code into a website. The second step is that it can be used to exploit vulnerabilities in the website's database, enabling a hacker to access data, such as passwords, credit card numbers or trade secrets.

(*see*: SearchSecurity)

2.2. History of Cybercrime:

The development of new technologies has led the peoples into the 21st century. Computers and networks are an indispensable part of our all daily lives, but also the sort of crime has changed. Criminals utilize other methods to get what they want: data!

In the beginning of the new era, the technological era, the crimes were simple hacks to get access to stored data. The first big wave of cybercrime came together with the emails in the late 1980ies. Malware (see 2.1.2.) were sent to various hosts to infect the target computer. Together with technological progress in the 1990ies and the advanced web browsers the second wave of cybercrime appeared. Via internet connections it was quite easy to install a virus on someones computer, because due to the multitude of different forms, the vulnerability was very high. The third wave came around the turn of the millennium. Social media became more and more popular and people provided information about their selves voluntarily. For criminals it was therefore very easy to get and use that information.

Currently we talk about the latest wave. The establishment of a global criminal industry created a way for criminals to work together ("gangs") and use sophisticated methods. These methods allow them to target nearly each and every one who provides data on the web. (*see*: LeVPN)

Estimates from the United Nations cyber security experts say that about 80% of all cyber-based crimes are committed by gangs of criminals. Those gangs seem to be organized as a legitimate business having regular work hours with a hierarchy in their staff and operate and maintain whatever deception it is, they currently focus on. LeVPN identifies three aspects why criminals work like that:

> "First, the criminals can easily hide behind their terminals far from regulators, operating with impunity by using the latest high-tech software and networking techniques to mask their locations and misdirect any prying eyes. Second, the Internet provides easy access to just about everyone on the planet and when it comes down to brass tacks anyone with money of information to steal is

> probably connected and not hard to find. Third, if you want to run a scam you don't have to be a programmer, all you have to do is know where to buy one."
>
> (*see*: LeVPN)

Another opportunity for criminal activities is the Deep Web or Deep Dark Web. Illegal activities are on the daily schedule there. Here we talk about websites a normal person does not care about, but in the end you can find a wide range of different things: "These sites include everything imaginable ranging from innocent chat rooms where the members want to remain completely anonymous to sites where you can buy your very own malware." (*see*: LeVPN)

The cyberspace has also created new possibilities to attack infrastructure of states. Therefore, we can say that cybercrimes illustrate a threat to international peace and security. Stein Schjølberg writes: "A global framework on cybersecurity and cybercrime is necessary for harmonizing measures against risks and threats in cyberspace, and may reduce the cybersecurity digital divide for developing countries." (*see*: Stein Schjølberg, 2017: 1.)

In 2005 the United Nations Office on Drugs and Crime made a proposal for an International Court for Cyberspace. This suggestion came up during the Congress in Bangkok: "Recommends that the Review Conference pursuant to Article 123 of the Rome Statute of the International Criminal Court consider the crimes of cyberterrorism and cybercrimes with a view to arriving at an acceptable definition, and their inclusion in the list of crimes within the jurisdiction of the Court." (*see*: Stein Schjølberg, 2017: 6.)

Hence an open-ended intergovernmental expert group was established. The target was to supervise a comprehensive study on the problem cybercrime and the response to it. The first meeting took place in Vienna in January 2011 (17th to 21st). In February 2012 the United Nations sent a questionnaire and dissemination to the member States, the private sector, IGOs and academia. In April 2012 regional workshops were organized and information from 69 member States and 67 NGOs was received. (*see*: Stein Schjølberg, 2017: 6.)

The last meeting took again place in Vienna (February 2013) and it agreed on recommendations for technical assistance and capacity building, while proposals for new national and international responses to cybercrime could not reach any possibility for a consensus. (*see*: Stein Schjølberg, 2017: 6.)

2.3. Actions to combat Cybercrime:

As already mentioned, there were attempts to do something against cybercrime, but in this section the main focus should be on diverse regions/countries in the world. It must be clear that the chosen regions/countries do not represent to whole world, but it covers a wide field.

2.3.1. United States of America

Due to the high interconnectivity the risks of theft, fraud and abuse have increased significantly. Together with the development of technical devices the vulnerability of people gets higher and higher. The United States of America is regularly a victim of cyber activities committed by criminals. Federal law enforcement works to apprehend and prosecute offenders, disable criminal infrastructure and prevent cyber criminals and their state sponsors from profiting from illegal activities. (*see*: Homeland Security & Whitehouse.org, 2018: 10.)

The United States of America created a model concerning priority actions. A mechanism for reporting and response to incidents is the first aspect. Here the link between action and reaction is most important: “The prompt reporting of cyber incidents to the Federal Government is essential to an effective response, […].” (*see*: Whitehouse.org, 2018: 10.) Keeping electronic surveillance and computer crime law up to date is the second aspect. Here a close collaboration between the administration and the congress is eligible. Besides the reduction of threats from transnational criminal organization in cyberspace and the improvement of apprehension of criminals located abroad the strength of collaboration with partner nations is the main target of the United States of America. The report says: “The United States will strive to improve international cooperation in investigating malicious cyber activity, including developing solutions to potential barriers to gathering and sharing evidence.” (*see*: Whitehouse.org, 2018: 11.)

A cybersecurity workforce is seen as a tool for an advantage regarding strategic national security. The United States Government will continue with investments in programs to build a domestic talent pipeline: “The Administration will leverage the President’s proposed merit-based immigration reforms to ensure that the United States has the most competitive technology sector.” (*see*: Whitehouse.org, 2018: 17.) The expansion of re-skilling and educational opportunities is an important part as well. Education and trainings are essential when a successful development will be achieved: “[…] to promote and reinvigorate educational and training opportunities to develop a robust cybersecurity workforce.” (*see*: Whitehouse.org, 2018: 17.) The usage of executive authority to highlight and reward talent is also added. In the report you can find: “The United States Government will promote and magnify excellence by highlighting cybersecurity educators and cybersecurity professionals.” (*see*: Whitehouse.org, 2018: 17.) Here we can see that the whole project was designed for a long-term periode.

2.3.2. European Union

The member States of the European Union have to deal with daily attacks in the cyber field. Personal information, spam or child pornography are widespread. The European Commission has a strong cooperation with the French Presidency regarding an elaboration of different practical methods to combat those attacks. A strong partnership, including knowledge-sharing is the key element to success. The strategy should also include an alert platform in the short term. Around 300.000€ are earmarked by the European Commission for Europol to implement the platform. (*see*: Europa.eu, 2018)

The Commission has also adopted a proposal concerning a regulation of the European Parliament and the Council. The establishment of the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres should be promoted. This would lead to a greater support for development of the technological and industrial capabilities. (*see*: European Commission, 2019: 82.)

As already mentioned in 2.3.1., a strong collaboration between countries is favoured. A working group of experts from the EU and the US collected various efforts. The summit between those representatives took place in November 2010. The efforts worked out during the summit include:

- expanding incident management response capabilities jointly and globally, through a cooperation programme culminating in a joint EU-US cyber-incident exercise by the end of 2011;
- a broad commitment to engage the private sector, sharing of good practices on collaboration with industry, and pursuing specific engagement on key issue areas such as fighting botnets, securing industrial control systems (such as water treatment and power generation), and enhancing the resilience and stability of the Internet;
- a programme of immediate joint awareness raising activities, sharing messages and models across the Atlantic, as well as a roadmap towards synchronised annual awareness efforts and a conference on child protection online in Silicon Valley by end 2011;
- continuing EU/US cooperation to remove child pornography from the Internet, including through work with domain-name registrars and registries;
- advancing the Council of Europe Convention on Cybercrime, including a programme to expand accession by all EU Member States, and collaboration to assist states outside the region in meeting its standards and become parties.

(*see*: Europa.eu (2))

This working group was a model for other countries or organizations with similar cyber issues. Information sharing was mentioned as most important aspect. (*see*: Europa.eu (2))

As addendum please keep the General Data Protection Regulation (GDPR) in mind. You can find information about it here: https://gdpr-info.eu/ (last access on 19th of July 2019)

2.3.3. China

According to InfoSec Institute the highest numbers of cybercrime victims are located in China, Russia and South Africa.

Contrary to other Asia-Pacific countries, China's cybersecurity law imposes strict data localisation requirements and cross-border transfer restrictions. China also dies not allow the collection, storage, transmission and use of personal information, but with the provisions allowed in the constitution, Chinese cybersecurity law, telecommunications law, tort law and consumer rights law, takes a piecemeal approach to data protection. (*see*: Lexology.com)

However, it is important to note that to this day China still has not sighned any treaties with the European Union or other nations in the world on data protection and is not a member of the Cross-border Privacy Enforcement Arrangement or the Asia-Pacific Privacy Authorities. (*see*: Lexology.com)

For instance, the cybersecurity law was passed in November 2016 and came into effect on June 1st, 2017 during which time regulatory measures were being periodically issued to supplement its provisions. On May 9th, 2017 the Supreme People's Court and the Supreme People's Procuratorate of China issued the interpretation on several issues concerning the application of law in the handling of criminal cases involving infringement of citizens' personal information. (*see*: Lexology.com)

It is also important to note that a draft privacy law was prepared and circulated in 2003. The draft law was added to the five-year legislative plan in 2009. However, there are no indications that the draft law will be enacted in the immediate future. The various law, regulations and guidelines that address the protection of personal information include:

- the cybersecurity law;
- security assessment measures for cross-border data transfer of personal information and important data;
- the decision on strengthening protection of network information;
- the law on the protection of consumer rights and interests;
- the measures for the administration of online transactions;
- the information security technology guidelines in personal information protection within public and commercial services information systems – these are voluntary, non-binding standards jointly issued by the

General Administration of quality supervision, inspection and quarantine and the standardization administration in 2012 to provide guidance on enforcement actions and litigation for the protection of personal information;

- the provisions on protecting the personal information of telecommunication and internet users;
- several provisions on regulating the market order of internet information;
- the medical records administration measures of medical institutions;
- the measures for administration of population health information
- the measures for the administration of internet email services;
- the standards for the assessment of internet enterprises' protection of personal information, which are not binding and
- the administrative provisions on short message services.

(*see*: Lexology.com)

2.3.4. Russian Federation

Being one of the major victims of cybercrime in the world, the largest contributor of the market for cybercrime in Russia is stolen credit and debit cards, which constitutes over $680 million, according to IB, which is a leading company in fraud prevention, cybercrime and high-tech investigations. Threats to mobile banking were also on a trend, wo which Group IB pinpointed five criminal gangs that were using Trojan horses to infect android phones and steal banking information using SMS banking and phishing websites. IB also pointed out that one group was able to steal $1.2. million. (*see*: Cybersecurityintelligence.com / Globalriskinsights.com / Trendmicro.com)

At the same time, online banking fraud was essentially decreased from $615 million to $425 million, which is the lowest in a very long time. The number of Russian speaking groups was reduced from 8 to 5 within only one year. However, during this time spam fraud has grown more worrisome, to which the Group IB reported over 10,000 new online stores selling pharmaceuticals (which was the majority of the spam shops), fake products and software. (*see*: Cybersecurityintelligence.com / Globalriskinsights.com / Trendmicro.com)

These spam stores were found to be colluding with legitimate and licensed sellers to deceive international payments rules, which forbid the payment of unlicensed medical supplies. The spam fraud was found to be worth approximately $841 million. (*see*: Cybersecurityintelligence.com / Globalriskinsights.com / Trendmicro.com)

The Group IB report found out that cybercrime in Russia has an annual turnover of more than approximately $2 billion. Other reports identify Russia as the source of at least a third of the world's most deadly malwares, such as the Trojan and Malicious malwares. "In terms of sophisticated types of malware, Russia leads the way", says Kyle Wilhoit, an American cybersecurity expert. (*see*: Cybersecurityintelligence.com / Globalriskinsights.com / Trendmicro.com)

According to the 2012 study "Russian Underground 101", the Russian cybercriminal world also offers goods and services in hidden markets, which include exploit kits, bulletproof web hosting, VPN services, custom-created malware, and pay-per install (PPI) services. Over the years, it evolved to become more cosmopolitan and professional in the following aspects:

- automated processes to accelerate trades and lower prices;
- more seamless and standardized transactions via new marketplaces;
- newly optimized and segmented translations and antispam-proofing offerings;
- unique platform-registration processes that ensure anonymity and
- an easier access to bulletproof hosting services (BPHS) that form the base of undetected proceedings.

(*see*: Cybersecurityintelligence.com / Globalriskinsights.com / Trendmicro.com)

The company Ernst & Young conducted a research where they surveyed workers of Russian corporations and the assumption that many of these corporations were covering up for being a victim was put forward, in order to not lose the trust of their customers, who have doubts about cybersecurity. It was found out that 98% of the participants claim that the organizations they work for do not completely address their own weaknesses regarding cybersecurity and 71% of the participants think that the resources are lacing. (*see*: Cybersecurityintelligence.com / Globalriskinsights.com / Trendmicro.com)

In the recent years Russia found themselves to being detached from confronting cyber threats. Many sources think that is because of their "aggressive" actions in Ukraine and other allegations being made about "interference in Western elections", such as in the United States and Austria through cyber methods. (*see*: Cybersecurityintelligence.com / Globalriskinsights.com / Trendmicro.com)

2.3.5. African Union

The African continent displays one of the most rapid growth rates in internet users worldwide, having a digital connectivity that keeps growing every day and that has almost tripled in the past five years. Oyumone, which is a British consulting company, states that by 2022 a billion people in Africa will have internet access, which proves that Africa is catching up to the other continents in the aspect of cyberspace, as it has now become an essential tool for communication, innovation, social development and economic progress. Along with that both the governments and corporations have become an increasing target in cyberattacks. (*see*: AU.int / AU.int (2))

Extensive research states that 10-15% internet penetration as the threshold level for the generation of significant hacking activities. Bülent Teksöz, from the company Symantec Middle East set forth that "cybercrime is shifting towards the emerging economies. This is where the cyber criminals believe the low-hanging fruit is". Which is why many of the African economies are the important sources and also the victims of cyber-threat. (*see*: AU.int / AU.int (2)) According to Serianu, which is a Kenya based IT and business advisory firm, in the year 2017 cybercrimes have costed the African economies $3.5 billion. The same year, annual losses to cybercrimes were estimated to be at $649 million for Nigeria and $210 million for Kenya. Similarly, according to SABRIC, the South African Banking Risk Information Centre, South Africa loses $157 million annually to cyberattacks. (*see*: AU.int / AU.int (2))

In the year 2016 alone, Symantec observed 24 million malware incidents that targeted the African continent. Financial institutions of Ghana declared having experienced more than 400,000 incidents related to malware, 44 million related to spam emails and 280,000 related to botnets. (*see*: AU.int / AU.int (2))

Business Software Alliance said that the two countries with the world's highest software piracy rates in 2017 were from Africa: Libya and Zimbabwe, the proportions of which the unlicensed software in the two countries were 90% and 89% respectively. (*see*: AU.int / AU.int (2))

In October 2018, the African Union Commission partnered with several organizations and held the first ever forum on cybercrime in Addis Ababa, Ethiopia, to which more than 250 delegates across the continent, criminal justice authorities of 50 African countries, national governments and international institutions attended to. The focus of the forum was on three main streams:

- cybercrime policies and legislation, international standards and good practices;
- international cooperation against cybercrime and
- capacity building to empower criminal justice authorities to deal with cybercrime cases.

(*see*: AU.int / AU.int (2))

During this forum the UNODC "mandated to assist member states to prevent and prosecute transnational organized crime and other serious crimes, including cybercrime, through capacity building and technical assistance". This can be done through its Global Programme on Cybercrime and respective regional programmes for Africa, yet also through cooperation and partnership with other international organizations as well as NGOs and the private sector, which is a vital part of UNODC's capacity building strategy. (*see*: AU.int / AU.int (2))

The main objectives of UNIDC's programme is to increase efficiency in the investigation and prosecution of cybercrime, chiefly in respect to "online child sexual exploitation and abuse", "strengthened intergovernmental cooperation" and also to create strong connections between the private sector and the law enforcement. (*see*: AU.int / AU.int (2))

3. **Q**[uestions] [a] **R**[esolution] **M**[ust] **A**[nswer]:

- ➢ Which measures could be implemented on an international level to prevent cybercrime?
- ➢ How should single member States deal with cybercrime?
- ➢ How could developed countries support underdeveloped countries to reduce the threat of cybercrimes?

4. Additional Material:

4.1. Videos:

https://www.youtube.com/watch?v=FqrLUtIFVjs&feature=youtu.be&fbclid=IwAR20B8bXVFU0rWsFbPkJqmKlDSHttPqGNPybQab4EvAR9Lh2nundj71uXR8 (18th of July 2019)

4.2. Readings:

4.2.1. Newspapers (various languages):

English:

https://www.aljazeera.com/indepth/features/cyber-scams-multi-million-dollar-business-180918054043911.html (18th of July 2019)

https://www.aljazeera.com/news/2015/04/chief-crime-terrorism-feed-150412163101879.html (18th of July 2019) **!!!**

https://www.bbc.com/news/uk-scotland-scotland-politics-34858626 (18th of July 2019)

https://www.bbc.com/news/uk-northern-ireland-48703072 (18th of July 2019)

https://au.int/en/pressreleases/20180412/african-union-commission-and-council-europe-join-forces-cybersecurity (18th of July 2019) !!!

French:

http://www.lefigaro.fr/vox/societe/2017/05/19/31003-20170519ARTFIG00272-cybercriminalite-l-insuffisante-prise-de-conscience-des-pouvoirs-publics.php (18th of July 2019)

http://www.lefigaro.fr/flash-actu/2017/05/13/97001-20170513FILWWW00153-cyberattaque-plus-de-75000-victimes-dans-le-monde.php (18th of July 2019)

http://www.lefigaro.fr/secteur/high-tech/2017/05/30/32001-20170530ARTFIG00140-l-etat-lance-une-plateforme-pour-aider-les-victimes-de-cyberattaques.php (18th of July 2019)

Spanish:

https://elpais.com/tecnologia/2018/05/10/actualidad/1525962120_169031.html (18th of July 2019)

https://elpais.com/elpais/2013/02/19/eps/1361281322_025092.html (18th of July 2019)

4.2.2. PDF Files:

ASEAN (2013): ASEAN Declaration to prevent and combat cybercrime. [pdf available: https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf] (19th of July 2019)

Li, Xingan (2015): Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime. [pdf available: https://www.cybercrimejournal.com/Li2015vol9issue2.pdf] (22nd of July 2019)

UN-ESCWA (2013): The ESCWA Cyber Legislation Digest. Development Account Project – Regional Harmonization of Cyber Legislation to Promote Knowledge Society in the Arab Region. [pdf available: https://www.unescwa.org/sites/www.unescwa.org/files/page_attachments/escwa_cyberlegislationdigest_v7-1.pdf] (19th of July 2019)

UNODC (2013): Comprehensive Study on Cybercrime. [pdf available: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf] (19th of July 2019) !!!

Youm, Heung Youl (2011): Technical measures to fight cybercrime. [pdf available: https://www.unodc.org/documents/southeastasiaandpacific/2011/09/cybercrime-workshop/ppt/cybersecurity_apec_workshop_hyyoum_final.pdf] (19th of July 2019) !!!

4.2.3. Links:

Cybercrimedata AS (2019): The Shanghai Cooperation Organisation (SCO). [https://www.cybercrimelaw.net/SCO.html] (19th of July 2019)

RSIS (2012): The Shanghai Cooperation Organisation: Challenges in Cyberspace – Analysis. [https://www.eurasiareview.com/27022012-the-shanghai-cooperation-organisation-challenges-in-cyberspace-analysis/] (19th of July 2019)

Shaohui, Tian (2017): Text: International Strategy of Cooperation on Cyberspace. [http://www.xinhuanet.com//english/china/2017-03/01/c_136094371_4.htm] (19th of July 2019) !!!

5. About the Chairs:

5.1. Kemal Sarsu

After having completed the IB Diploma Programme at the Vienna International School, Kemal began his studies in law at the University of Vienna last semester. He is interested in football, music, movies, politics and global events. He says that he has “very much respect for everyone who joins this conference, because”, he personally knows that “it is not an easy thing to put yourself out there and make arguments in front of other people that you have never met before”. He is very much “looking forward to getting to know new people who are full of life and learning new things from them during the 25th anniversary of VIMUN”.

5.2. Kevin Lechner

Kevin is currently working on his first master thesis in the field of African Studies with focus on linguistics. He did a bachelor’s degree in African Studies with focus on linguistics before. Besides that, he studies International Development (MA) as well – both masters at the University of Vienna. Upcoming October he starts a third master’s programme (M.E.S. – Master of European Studies) at the Postgraduate Centre of the University of Vienna. He is very interested in languages and linguistics, politics and history. “Model United Nations Conferences are always a great opportunity to meet new people from all over the world and exchange experiences with many interesting young leaders”, he says.

6. Used Literature:

6.1. Internet Links:

AU.int: https://au.int/en/ie/survey/cybersecurity (22nd of July 2019)

AU.int (2): https://au.int/en/pressreleases/20181017/auc-set-hold-first-african-forum-cybercrime-african-union-headquarters-addis (22nd of July 2019)

Cybersecurityintelligence.com: https://www.cybersecurityintelligence.com/blog/the-shocking-state-of-cybercrime-in-russia-648.html (22nd of July 2019)

Europa.eu: http://europa.eu/rapid/press-release_IP-08-1827_en.htm?locale=en (19th of July 2019)

Europa.eu (2): http://europa.eu/rapid/press-release_MEMO-11-246_en.htm (19th of July 2019)

Globalriskinsights.com: https://globalriskinsights.com/2019/03/russia-cyber-attacks-blindspot/?fbclid=IwAR0JX3cflAgDLopXdNx2mPkXvYiCjKUSwq3kJS9GcfMBwNYxjq5gww-2OB0 (22nd of July 2019)

Homeland Security: https://www.dhs.gov/cisa/combating-cyber-crime (19th of July 2019)

LeVPN: https://www.le-vpn.com/history-cyber-crime-origin-evolution/ (19th of July 2019)

Lexology.com: https://www.lexology.com/library/detail.aspx?g=6a51305a-eccd-4f3f-a3a4-0b9e21843c19https%3A%2F%2Fwww.cybercrimejournal.com%2FLi2015vol9issue2.pdf&fbclid=IwAR0SQwlBhFlrWA8_WbPP8t22cWXPWMIvdJCAZ-qATmS3iYIkT0psFl4JhC4 (22nd of July 2019)

SearchSecurity: https://searchsecurity.techtarget.com/definition/cybercrime (18th of July 2019)

Trendmicro.com: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/russian-underground-automized-infrastructure-services-sophisticated-tools?fbclid=IwAR1efeEfIcM5TAsOmXOAxFUwxBO2mWgfClEc-5dZmKPkC4ZclNzc09fn1kA (22nd of July 2019)

UNODC: https://www.unov.org/unov/en/unodc.html (18th of July 2019)

UNODC Annual Funding Appeal: https://www.unodc.org/unodc/en/about-unodc/annual-appeal.html (18th of July 2019)

UNODC – The Sustainable Development Goals: http://www.unodc.org/unodc/en/about-unodc/sustainable-development-goals/sdgs-index.html (18th of July 2019)

6.2. PDF Files:

European Commission (2019): Horizon 2020. Work Programme 2018-2020. [pdf available: http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security_en.pdf] (19th of July 2019)

Stein Schjølberg (2017): The History of Cybercrime. [pdf available: https://www.researchgate.net/publication/313662110_The_History_of_Cybercrime_1976-2016] (19th of July 2019)

Whitehouse.org (2018): National Cyber Strategy. [pdf available: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf] (19th of July 2019)