Karlsruhe Model United Nations

23 - 25th November 2018

Luis Cuadrado

Marc Kerstan

Economic and Social Council

Study Guide

Table of Contents

Overview of the Committee

"The ECOSOC is one of the six main organs of the United Nations established by the UN Charter in 1946. It is the principal body for coordination, policy review, policy dialogue and recommendations on economic, social and environmental issues, as well as for implementation of the internationally agreed development goals[1]."

The ECOSOC's composition and its powers are laid down in chapter 10 of the Charta. The council consists of 45 members that are elected by the United Nations General Assembly (UNGA).

The ECOSOC's resolutions, like the ones drafted by the UNGA are legally non-binding. However, its decisions which are passed by simple majority can build up political pressure and thus influence the policy-making of member states of the UN. Concrete powers of the ECOSOC allowing this are e.g. its right to set up commissions, its right to initiate studies and reports and its right to make recommendations based on these studies to other UN bodies.

[1] http://www.un.org/en/ecosoc/about/

Topic A: Fighting Income Inequality With Modern Technology

1.Introduction

We are in the middle of an economic revolution. New technology, especially digital technology changes the way economic processes and transactions are conducted. New skills are required in today's labor market and occupations which have been considered vital are becoming insignificant.

This fundamental change does not only affect high-tech industries like communication or internet technology but also has a significant impact on industries like banking and finance or even agriculture. Therefore the digital revolution is geographically not limited to the developed world but reaches developing countries as well. While the speed of technology adaption and the level of incorporated technology differs, every country can benefit from the technological revolution.

"But technological innovation will not automatically lead to prosperity and sustainability in every country and every society. The digital revolution requires new and inclusive policy responses if it is to benefit everyone", warns Achim Steiner, Head of the United Nations Development Programme (UNDP, 2018).

Consequently, it is crucial to look at policy areas where the digital revolution can unfold its potential the most and improve human well-being. Economically speaking, this means to search for areas with the biggest opportunity for growth. This growth centered view, however, neglects the social dimension of sustainable development. Therefore it is necessary to analyze and asses the possible effect of the digital revolution on income inequality.

2. Dimensions of Income Inequality

There are many measures to capture income inequality empirically. Each has advantages and disadvantages and no measure alone provides a conclusive result. The most common tool used is the Gini-Coefficient, which measures income inequality, by comparing the actual distribution of income with the case of an equal distribution. The coefficient then scales the result on a value between 0 and 1, where 0 means that everybody receives the same income and 1 means that one person alone receives all of the income generated in the respective data sample.

Figure 1 depicts the Global Gini-Coefficient for the time between 1820 and 2010. It shows that starting in 1820 and following the industrial revolution, global income inequality has risen from a Gini

coefficient of 0.50 to reach its maximum at .065 in the 1990s. The observed decline afterward is mainly attributed to the enormous economic growth in China and India, which account for a large proportion of the available data.

Figure 1

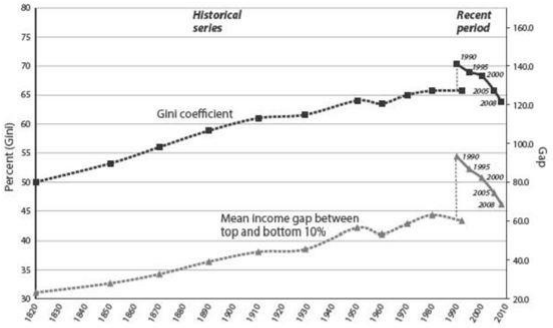
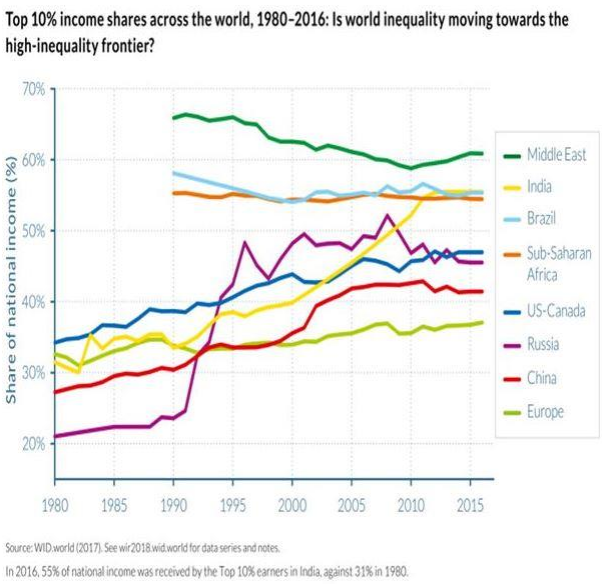


Figure 1. Evolution of World Inequality, 1820–2008.
Sources: The historical data come from François Bourguignon and Christian Morrisson, "Inequality Among World Citizens: 1820–1992," *American Economic Review* 92, no. 4 (2002): 727–44. It uses estimates of GDP per person provided by Angus Maddison (in *Monitoring the World Economy*, Paris: OECD Development Centre, 1995). The recent data represent an update of the article by François Bourguignon, "A Turning Point in Global Inequality . . . and Beyond," in *Research on Responsibility. Reflections on Our Common Future*, ed. Wilhem Krull (Leipzig: CEP Europaische Verlagsanstalp, 2011). The indexes of purchasing power parity that Angus Maddison used for the historical data referenced the year 1990. The data for the recent period use purchasing power parity data based on price statistics that were collected in 2005, which sometimes resulted in significant revisions to the parity indexes. This explains much of the discontinuity between the two series in 1990.

Source: Bourguignin (2015)

Figure 2



Source: Alvaredo et al. (2018)

Following the World Inequality Report by Alvaredo, et al. (2018) it is useful to emphasize one crucial shortcoming of the Gini coefficient. Its greatest strength, to compare inequality between countries, using only one metric, is also its greatest weakness. Boling down the problem of income inequality to one artificially created index makes it very hard to interpret the coefficient from a within-country perspective. This impedes the work of policymaker, who cannot infer if the level of the Gini coefficient can be considered too high, sustainable or socially desirable.

Another popular measure which is commonly used is the proportion of income earned by a certain percentage of individuals at the top of the income distribution. This approach has the that it is fairly easy to interpret. However, the most obvious disadvantage of this measure is that it does not inform on the income distribution of the rest of the population. Therefore it is necessary to have a look at other segments of the income distribution and look at the respective share of total income. Furthermore, the question of a socially desirable outcome remains unclear.

Figure 2 indicates that the share of income received by the top 10 of individuals, has constantly increased over many parts of the world or has remained at a high level. The difference in the result

between figure 1 & 2 emphasizes the importance of using several metrics to analyze income inequality. While the Gini index suggests lower income inequality on a global scale, income inequality within certain areas or countries has increased.

It is important to note that the above-mentioned measures and their respective values are the results of a process within society and economy. The discussion on inequality gains a lot more depth when we start to ask, how we ended up with these numbers and what variables should be the primary policy target in order to combat income inequality.

According to Afonso, LaFleur, and Alacrón (2015) especially two different views have been predominant in this discussion. The first one is called inequality of outcomes. It takes an ex-post view on the creation of income inequality, meaning that it is concerned with the actual statistical values of the income distribution. In this context, material variables such as income are considered the main indicator for human well-being. Consequently, how this distribution of income is obtained, is less relevant for this approach.

The other view, which was proposed by Sen (1999), suggest that the discussion should not focus on income inequality alone. Instead, it is crucial to create equal opportunities for as many people as possible, so they can better pursue their own economic goals.
This view does not take the income of an individual as given but sees it as a consequence of several factors. The individual can be considered responsible for some of these factors, but not all of them. This view claims that there are factors which are beyond one's control. These factors are for example parental wealth, geographical origin, gender or ethnicity. Consequently, these variables, are among other things like personal talent or effort, key components in explaining the present levels of income. It is now the challenge for the policymaker to address factors which are beyond individual control and create fair initial conditions.

This concept of inequality also gives an answer to the question what a “desired” level of income inequality is. If people are compensated for the initial disadvantages which are beyond one's control, and income is fully the result of individual choices and skills, then the result can be considered socially desirable.

3. The Sustainable Development Goals (SDG)

On the 25th of October 2015, the General Assembly of the United Nations adopted the Resolution “Transforming our world: the 2030 Agenda for Sustainable Development”. This agenda of “unprecedented scope and significance” (p.3) lays out 17 Goals for Sustainable Development (SDGs).

These goals are the successors of the Millennium Development Goals (MDG) of the United Nations and try to improve the process of human development by incorporating the experiencing and lessons learned from the MDGs. These goals comprehensively tackle issues which affect the quality of human development. Thereby each goal has a set of specified targets, which should be reached by 2030.

For the purpose of fighting income inequality, Goal 10 aims to “reduce inequality within and among countries” (p.14). One of the specified targets for this goal is to “progressively achieve and sustain income growth of the bottom 40 percent of the population at a rate higher than the national average”(p.21).

Additionally the goal tackles the different concepts of inequality discussed in chapter 2 as it is incremental to “ensure equal opportunity and reduce inequalities of outcome including by eliminating discriminatory laws, policies, and practices” (p.21) and “empower and promote the social, economic and political inclusion of all, irrespective of age, sex, disability, race, ethnicity, origin, religion or economic or other status” ”(p.21).

There is a scheduled process where the progress on each SDG is reviewed. The review will be conducted by the United Nations High-level Political Forum on Sustainable Development (HLPF). The HLPF gives countries a platform to share their experiences, especially their successes and challenges. Additionally, the HLPF enables better policy coordination as not only state representatives are present, but also participants from the private sector and civil society.

For the meeting of the HLPF in 2019 among others the progress of SDG 10 is reviewed. For this purpose 51 countries provide a Voluntary National Review (VNR) of their progress in terms of fighting (income) inequality. Among those countries are many developing countries and even some developed countries. They will meet under the theme “Empowering people and ensuring inclusiveness and equality”.

4. Modern Technology in Development

The exact scale and impact of the current (digital) technological revolution have yet to be determined, but the potential among and within all branches of the economy are enormous. Consequently, there are a lot of different (social & economic) policy areas which are of interested in the debate on income inequality. The following policy areas should therefore not be considered final, but rather be seen as a starting point for your country-specific research.

Banking and Finance

The smartphone is the most commonly used tool for communication. This new form of connectivity also changes the financial world. The smartphone has become a pillar of financial infrastructure, as it promotes financial inclusion all over the world. People, especially in rural areas, are now able to access financial services such as bank and saving deposits, money transfers and payments via their smartphone. A prime example of this development is the communication firm M-Pesa located in Kenya. M-Pesa provides a digital wallet for users, which then can be used for cash conversion, payments or money transfers. Using a model by Dabla-Norris and others (2015) Ndung'u, Morales and Ndirangu (2016) conclude that the resulting increased efficiency of financial services in Kenya has lowered transactions costs and creates additional funds for existing entrepreneurs and people who try to start a business

While providing a great opportunity for sustainable development, success depends also on the respective policies, which minimize the potential risks. Since mobile-based banking technology promotes financial inclusion, it is also crucial to acknowledge that inexperienced segments of the population are now for the first time introduced to financial services. Consequently, it is imperative to foster financial literacy and provide measures of consumer protection.

Another concern addressed in the World Development Report 2016: Digital Dividends (2016) is the market entry of nontraditional providers of financial services. Concerning in this context is that those firms might not be covered by traditional financial oversight. One example of this trend is the Chinese online shopping service Alibaba. Alibaba provides small loans to its vendors but is not considered a classical financial institution. This raises concerns which compare to the shadow banking sector before the great recession, a sector who is under no regulatory framework.

Agriculture

In 2016 32 % of employment in low- and middle-income countries, was in agriculture. Taking only a look at low-income countries, this number rises to 67.7 % (World Bank, 2016). Consequently, agriculture and its respective policies are of major concern for sustainable development and the fight against income inequality. Although agriculture is considered to be the world's oldest industry, this does not impede the impact of modern technology on this economic sector, as the improved sharing of information also benefits farmers. New information concerning weather, improved seeds, or best practice in planting and harvesting seeds can greatly improve productivity. Additionally, the mobile phone can improve market integration of farmers on a global and local scale. Jensen (2007) found

that the introduction of the mobile phone significantly decreased the variance in prices and reduced waste in local fishing markets in India. This led to improved efficiency and increased welfare in the respective area.

However, there are still concerns about the impact of the digital revolution on agriculture. Goyal (2016) argues technology itself is not enough to improve agricultural outcome, but must "be backed by complementary investments in physical infrastructure, including electricity and literacy" (p. 92). She further argues that it is crucial to develop sustainable business models to attract private investors.

Education

Maybe no other field of policies is linked as much to the concept of equalizing opportunities like education. In this field, technology can have a significant impact on the quality of education.

In developing countries, where poor infrastructure, long travel distances to schools, insufficiently supported and qualified teachers, and ill-equipped schools prevail, modern internet communication technology can improve the quality and availability of education. However, field experiments suggest that the provision of the technology itself is not sufficient to increase the quality of education. One striking case was made in Peru where a program provided laptops to pupils in rural areas. However, despite the provision of technology, Ortiz and Cristia (2012) did not find any significant improvement in learning math or English. Trucano (2016) explains this result with the Matthew effect. He argues that the likelihood to benefit from new technology in education depends on an already existing private use of this kind of technology. Consequently, those who are introduced to new technology are likely to profit less from this technology. Trucano further argues that an alternative approach should be considered in which already available technology is innovated for the purpose of education.

The Impact of Automation

While there are many promising opportunities of the digital revolution, with every economic revolution, there are disruptive changes in the predominant economic structures, especially within labor markets. In accordance with the extreme progress in computer science and artificial intelligence, one of the most pressing issues at the horizon is the phenomena of automation, the process of substituting labor with capital. A report by the McKinsey Global Institute (2017) finds that "50% of the time spent on work activities in the global economy could theoretically be automated by

adapting currently demonstrated technologies“ (p.25). While this does not imply that those activities vanish within the next couple of years, as the cost for this substitution is still high, the potential long-term effects of automation will change labor markets and skill requirements.

In light of this development, the World Economic and Social Survey (2018) calls for "complementary investments in skills, education and social protection” (p.8) in developed countries in order to cope with the replacement of jobs by machines. Especially, as automation changes the required skill sets for successful labor market participation, schooling and education plans have to keep up with this development.

5. Topics of Debate

Generally, the debate should be focused on how all nations can reach the formulated SDG targets regarding income inequality and entangled issues, with the help of modern technology. For this purpose, it is useful for each country to present some of their domestic policies which have been addressed in chapter 4, to the committee. If the domestic policy has been successful, the discussion should focus on how other countries can replicate this result. If it has not proven useful, the reasons for its failure should be investigated.

6. Questions for your preparation

• Do you represent a developed or developing country?

• How did income inequality evolve over the past 20 years in your country?

• What is school enrollment among different levels of education in your country? Is there a significant gap between regions, ethnicity or gender?

• How accessible is the internet in your country?

• If your country would submit a Voluntary National Review at the High-level Political Forum on Sustainable Development, what would it look like? What have been your countries greatest successes and challenges in the context of fighting income inequality?

• At which areas can your country profit most from (digital) technological advancement?

• Is your country in a leading/special role in any technology area, for example, i.e Artificial Intelligence, Internet technology or communication?

• How are knowledge and technology distributed in your country? Does your country have a National Innovation System?

7. References

Alvaredo, F., Chancel, L., Piketty, T., Saez,E., Zucman, G. *World Inequality Report 2018*. The Belknap Press of Harvard University Press, 2018.

Bourguignon, F. (2015): *The Globalization of Inequality* , Princeton University Press 2015.

Dabla-Norris, E., Ji,Y., Townsend, R., D. Filiz Unsal. (2015) *Identifying Constraints to Financial Inclusion and Their Impact on GDP and Inequality: A Structural Framework for Policy,* IMF Working Paper 15/22 (Washington: International Monetary Fund).

Goyal, A. (2016): Sector Focus 1 Agriculture, in World Bank. 2016. World Development Report 2016: Digital Dividend, 90-92.

Jensen, R. (2007). "The Digital Provide: Information (Technology), Market Performance, and Welfare in the South Indian Fisheries Sector." Quarterly Journal of Economics 122 (3): 879–924.

McKinsey Global Institute. (2017). *JOBS LOST, JOBS GAINED: WORKFORCE TRANSITIONS IN A TIME OF AUTOMATION*. Retrieved from https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Future%20of%20Organizations/What%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/MGI-Jobs-Lost-Jobs-Gained-Report-December-6-2017.ashx.

Ndung'u, N., Ndirangu, L., Morales, A. (2016): *Cashing In on the Digital Revolution*, in: Finance & Development,53 (2), 14-17.

Ortiz, E. and Cristia, J. (2014): *The IDB and Technology in Education: How to Promote Effective Programs?* Washington, DC: Inter-American Development Bank.

Sen, A. K. (1999), *Development as freedom*, Anchor Books.

Trucano, M. (2016): Sector Focus 2 Education, in World Bank. 2016. World Development Report 2016: Digital Dividend, 146 -147.

United Nations Development Programme (September 25, 2018). *UNDP: Digital revolution can unlock prosperity with right policy mix* [Press Release]. Retrieved from

http://www.undp.org/content/undp/en/home/news-centre/news/2018/UNDP_Digital_revolution_can_unlock_prosperity_with_right_policy_mix.html.

United Nations, Economic and Social Council, World Economic and Social Survey 2018: Frontier technologies for sustainable development Overview, E/2018/50 (29 April 2018), retrieved from http://www.un.org/ga/search/view_doc.asp?symbol=E/2018/50.

United Nations General Assembly resolution 67/97, *Transforming our world: the 2030 Agenda for Sustainable Development*, A/RES/70/1 (25 September 2015), available from undocs.org/A/RES/70/1.

Afonso,H., LaFleur,M., and Alacrón,D. (2015): *Development Issues No. 1: Concepts of Inequality*, United Nations Department of Economic and Social Affairs.New York. Retrieved from https://www.un.org/development/desa/dpad/publication/no-1-concepts-of-inequality/.

World Bank, World Development Indicators. (2016). *Employment in agriculture (% of total employment) (modeled ILO estimate) (SL.AGR.EMPL.ZS)*. Retrieved from http://databank.worldbank.org/data/reports.aspx?source=2&series=SL.AGR.EMPL.ZS&country=#advancedDownloadOptions.

World Bank. 2016. *World Development Report 2016: Digital Dividends.* Washington, DC: World Bank. doi:10.1596/978-1-4648-0671-1. License: Creative Commons Attribution CC BY 3.0 IGO.

Topic B: 17 years of Budapest Convention on Cybercrime – Towards a new international framework against cyber criminality

1. Topic Area

The developments in information technology over the last decades have not only lead to significant economic growth and to the rise of whole new economic branches – Silicon Valley being the best example for this - but have also substantially changed the way firms and public authorities operate and ultimately found their way into our everyday life.

The average adult spends 5.9 hours a day with digital media[2] which does not only demonstrate the transition from analogous to digital work. It also shows how we spend our free time nowadays. Average usage of tablets and mobile phones reached an all time high in 2017 with 3.3, trend going upwards.

This increasing dependency of our societies on information technology in general and the internet in particular has its downsides. Cyber-attacks against critical infrastructure paralyze entire regions, child pornography is distributed via the darknet and hackers steal personal data from millions of internet users. Those attacks against states, violations of children's rights and of individual privacy cannot be solved unilaterally. A joint, multilateral effort is needed in order to address them.

2. Definition of Key Terms

Cybercrime

Cybercrime itself is defined as "criminal activity […] committed using a computer especially to illegally access, transmit, or manipulate data"[3].

This very broad definition includes activities ranging from simple computer fraud[4] to outright cyberterrorism and cyberwarfare. This committee will primarily focus on financial computer fraud (i.e. cyber-attacks committed in order to profit financially), data theft and attacks against critical infrastructure.

[2] This includes internet-connected devices such as smartphones, desktops and laptops.
[3] Merriam-webster.org.
[4]

Two very common ways hackers use to illegally access data and ultimately extract money out of their victims' pockets are Ransomware and Phishing.

Ransomware

Ransomware is a type of malware (malicious software) that locks or infects system and demands a ransom to unlock it. The first known ransomware attack happened as early as 1989. A malware distributed via floppy disks to AIDS researches held their computers hostage, demanding its victims to make a payment between $189 and $378. Until today, the health industry remains the one most exposed to ransomware attacks.

Phishing

Phishing is a form of social engineering which means that the performer of a phishing attack uses human interaction to deceive its victims. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Devices through which hackers can gain access to personal information are not limited to computers, desktops or cellphones. The rise of the so-called Internet of Things (IoT) continues to open new access possibilities for hackers.

Internet of Things

The term Internet of Things (IoT) refers to the network built out of single computing devices that can be interconnected via the Internet. One example for an application are smart home systems that allow you to start your dishwasher, switch off the lights or turn on your tv with your smartphone via a wireless LAN or Bluetooth connection. In case of poorly designed security mechanisms, hackers could install ransomware which forces you to transfer money to them before you can open the door to your own home.

Another way for hackers to interrupt the functioning of a computing system or network are Distributed Denial of Service (DDoS) attacks.

Distributed Denial of Service (DDoS)

DDoS attacks are attacks that send a large number of requests to a computing system in order to overload it. Although, in some cases this can be done via a single computing device, they are more commonly performed by a large number of network sources, so-called botnets.

DDOS is not always the result of ill intent. It can also be the result of unexpectedly large traffic. An example for this is the crash of the CNN website on 9/11.

As the internet of things' rise continues, the number of potential "recruits" for hackers' botnets increases, making DDoS attacks more likely in the future.

One potential target of DDoS attacks is critical infrastructure.

Critical Infrastructure

A nation's critical infrastructure provides essential services to the public that are critical to the functioning of a state. Examples for critical infrastructure are power grids and health services.

3. Historic Background

When talking about cybercrime or cyber attacks one must distinguish between the origin of the attacker. The motivation for state actors to perform a cyber-attack is a different one than the financial motivation of a hacker performing a ransomware attack in order to gain money.

Thus, the following overview of cyber-attacks is primarily sorted by performer then by chronology.

However, it is to bear in mind that for most of the following cyber-attacks no culprit could be unequivocally identified which is due to the nature of cyber-attacks.

3.1. Cybercrimes committed by State Actors

Stuxnet (2005)

One of the earliest cyber incidents was the attack on Iranian nuclear centrifuges known as Stuxnet. The Stuxnet code has allegedly been built by the American and Israeli government to sabotage Iranian nuclear plans in a way that made it look like an accident.

Its complexity and the possibilities to build on its code in order to design cyber weapons revolutionized cybercrime and made the world aware of the destructive power of such weapons.

WannaCry (2017)

In 2017, more than 200,000 computers in about 150 countries were hit by a ransomware cyberattack called WannaCry. WannaCry locked its victims' access to their computers and demanded a ransom. Critical infrastructure such as hospitals were hit hard. Some hospitals, those adhering to the British National Health Service in particular, had to divert patients and shut down operations.

WannaCry's origin was never determined with certainty. While some experts suspect the People's Republic of North Korea behind the attack, others believe that the attack was not carried out by a state due to a bug in early versions of WannaCry that prevented its victims from paying the demanded ransom. States are simply not known to make such mistakes when performing cyber-attacks. One reason why WannaCry was financially rather unsuccessful for its performers – it made only $50000 worth of ransom – is that it only succeeded on computers running on Windows XP that had not upgraded a patch upgrade. This example proves that periodic upgrading of software is a helpful defense against cyber-attacks.

3.2. Cybercrimes committed by Non-State Actors

Cyber-attacks by non-state actors are either committed to profit financially e.g. by using phishing attacks or in order to make a political statement (hacktivism).

3.2.1. Russian Business Network (RBN) (2006)

The "Baddest of the Bad" of the Internet as described by VeriSign[5] offered its users a veritable market for cybercrime. By providing its users with the possibility to interact with each other and exchange their knowledge and nefarious code lines RBN offered the tools to e.g. commit phishing attacks or access child pornography.

3.2.2. Hacktivism: Dyn (2016)

Dyn is a company that controls the internet's domain name system (DNS) infrastructure. On 21 October 2016, Dyn's servers were hit by an unprecedented DDoS attack performed via a huge botnet, called the Mirai botnet. As a result, high-end internet sites like Twitter, CNN and Netflix were brought down. The circumstance that makes this case especially interesting is that the Mirai botnet was not composed out of desktops or laptops but of about 100.000 IoT devices like e.g. digital cams hence exposed the low security of IoT devices.

[5] US firm operating the .com and .net domains and offering services for the secure functioning of websites.

Hacktivist groups such as SpainSquad, Anonymous and New World Hackers claimed responsibility for the attack and called it a response to Ecuador limiting Julian Assange's access to Internet at their embassy in London where Assange resided at that time.

3.2.3. Election Hacking (DNC Hack 2015)

One cyber-attack that arguably tormented American politics was the hack of the server of the US Democratic National Convention (DNC) in 2015. It became clear that the hackers were in the system for over a year and stole thousands of emails including opposition research and campaign correspondence which WikiLeaks published in the following months. The security company CrowdStrike accused the Russian government of the attack, in particular the two groups named Fancy Bear and Cozy Bear, behind which many experts suspect the Russian military agency GRU and the Russian Foreign Intelligence Service SVR. GRU is also suspected to be responsible for the hack during the French presidential elections and the cyber-attack against the Bundestag.

3.2.4. Cyberterrorism (ISIS cyber-attacks)

In recent years, ISIS has led several successful cyber-attacks against Western institutions. In 2015, the terrorists hacked the Twitter account of the US Central Command[6] and posted the message "I love you ISIS".

Two years later, IS affiliates attacked the British National Health Service (NHS) and displayed images of their militias torturing their victims in Syria. This incident sparked a discussion in the House of Commons on the cyber security of government agencies.

4. Previous Resolutions

The first resolution passed concerning cybercrime was ECOSOC resolution 55/63 which has been adopted in January 2001. Among others, it recognizes that the technological advancement in the digital sector created new possibilities for criminal activity. It states furthermore, that international cooperation is needed to tackle the downsides of this development but recognizes at the same time that different development states between nations when it comes to information technology hinder effective cooperation.

One document which serves as a model for international cooperation in the fight against cybercrime is the Convention on Cybercrime signed on 23 November 2001 in Budapest, Hungary.

It is the first international treaty that intends to fight computer and Internet related crime by harmonizing national laws.

[6] The US Central Command is a Unified Combatant Command of the US Department of Defense.

Except from this agreement to harmonize national laws, the main achievements of the Budapest Convention on Cybercrime as it is also called are the clear definitions of computer-related crimes like e.g. computer-related crimes including child pornography, copyright infringement and system interference. Even though the ECOSOC does not dispose of the power to force Un members to take certain steps and albeit the strong wording of the Convention on Cybercrime which the ECOSOC cannot match, it has the power to recommend and encourage every endeavor it regards as necessary to fight cybercrime.

Another important UN resolution is UNGA resolution 64/ 211 which recognizes the deep need to protect critical infrastructure and provides a voluntary self-assessment tool for national efforts to protect critical information infrastructure. Even though it clearly stresses that states should primarily focus on national measure, it points to the positive impact that international collaboration in the field has on governments that struggle with IT challenges.

A third resolution which should be consulted for references in ECOSOC resolution 2013/39 which aims at fostering international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.

These documents give an overview on achievements in the fight against cyber criminality and can serve as an inspiration for your very own resolution as well as priorities that you may want to set during your discussion.

5. Key Conflicts

The key question of the discussion on international cooperation in the fight against cybercrime is, has been and will continue to be: “How far can we go?”. Delegates will have to consider the field of tension between international cooperation and national sovereignty since information sharing on cybersecurity measures has its costs in times that countries like the US and military alliances like NATO have defined cyberspace as a field of operation. The challenge is to find areas where the benefits outweigh the cost by finding common ground. Setting international standards for the persecution of copyright infringers and distributers of child pornography is likely to be easier than agreeing on a way to hold hackers accountable who attack critical infrastructure or meddle in elections (as those hacks are most likely orchestrated by states).

6. Proposed Solutions

Responses to cybercrime come in a range as diverse as cybercrime itself. Every facet of cybercrime - be it cyber terrorism or protection against simple phishing attacks – has to be tackled in a different manner. While the most efficient approach is always a form of international cooperation, its practical implementation can be tricky.

As for identity-related crimes and attacks against critical infrastructure, the private sector must be held accountable in some way in order to incentivize the firms operating websites that process confidential personal information or build and administer critical infrastructure to take adequate measures to protect their customers or the infrastructure.

Finding ways to strengthen government security systems might prove more difficult. Here - for obvious sovereignty reasons – states seldomly rely on the international community. However, the chair is looking forward to see a debate on how to support developing countries in strengthening their defensive cyber capacities to be able to defend attacks from the outside directed at meddling in their elections.

Cyberterrorism poses a special challenge: How to find common ground if some states are secretly supporting of cyber-attacks as a means to cause political, economic or social turbulences in countries they regard as enemies or competitors. While a recommendation to build an international cyber taskforce to meet ISIS on the battleground of cyberspace might find international support, cyber giants like e.g. Russia will most likely oppose any solution proposal that involves international technical support for countries hit by cyber attacks which cannot unequivocally by attributed to terror organizations.

Also, one problem to overcome is the distrust between countries when it comes to sharing technical expertise or intelligence. The risk of supplying a potentially hostile country with means to protect itself against cyber-attacks is one that no country will take.

All in all, a well-thought through compromise that considers the benefits and risks of intelligence and expertise sharing is what this committee should be looking for in order to draft a resolution that is acceptable for the members of the committee.

7. Chair's Expectations

Each delegate is expected to write a study guide on both proposed topics. For topic B, the delegates are expected to deliver a wholistic overview on its countries position concerning the willingness to collaborate to fight cybercrime. Special consideration should be given to the trade-off between the benefits of this cooperation - i.e. the detention of criminals and the protection of citizens' rights – and the loss of national sovereignty regarding the handling of cybercriminals.

The goal of the discussion in the committee is to pass a resolution which addresses the main threats of cybercrime. It is up to the delegates to decide where they want to set the focus. However, the resolution should cover the following problems:

- Identity related crime
- Computer-related fraud

Other challenges that an improved version of the Budapest Convention on Cybercrime could address are:

- Attacks against critical infrastructure
- Hacktivism
- Cyber Terrorism

Ideally, the final resolution will foster international cooperation in the fight against cybercrime. The diplomatic key challenge is to draft a resolution behind which as many key stakeholders as possible can gather but whose wording is not softened by countries traditionally pointing to national sovereignty when it comes to fighting cybercrime.

8. Proposals for further Research

The final product of your discussion on this topic is supposed to be an improved version of the Budapest Convention on Cybercrime published in 2001. Thus, we strongly recommend you to have at look at the document itself as well as all sorts of news articles evaluating its usefulness. Another motivation to do this is to get an idea of the format in which international resolutions are drafted. This will prove useful when you will be drafting your own resolution here at KAMUN or other conferences.

As cybersecurity is a very technical topic which can only be understood if one is aware of the technical details, www.zdnet.com can be a very helpful source. It provides its readers with information on technology as well as with the latest cyber news.

9. References

https://uk.pcmag.com/netflix/95287/feature/tech-addiction-by-the-numbers-how-much-time-we-spend-online

https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

https://www.us-cert.gov/

https://www.dhs.gov/

https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

https://www.bsi.bund.de/EN/Topics/Criticalinfrastructures/criticalinfrastructures_node.html

http://www.un.org/en/sections/un-charter/chapter-x/index.html

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

https://www.heise.de/security/artikel/Strukturen-des-Russian-Business-Network-270928.html

https://www.forbes.com/sites/kateoflahertyuk/2018/08/23/midterm-election-hacking-who-is-fancy-bear/#22a3abe22325

https://www.washingtonpost.com/opinions/global-opinions/working-with-russia-on-cyber-regulation-is-like-paying-a-bully-for-protection/2018/09/04/b16787ea-b08e-11e8-9a6a-565d92a3585d_story.html?noredirect=on&utm_term=.9cb56ca862f6

https://www.cybersecurity-review.com/news-april-2017/russia-prepares-new-un-anti-cybercrime-convention-report/