TED ISTANBUL MODEL UNITED NATIONS 2020

“Protecting Future Generations”

The issue of crimes committed in cyberspace

Duru Yünek

Deputy Chair

Committee: NATO

Issue: The issue of crimes committed in cyberspace

Student Officer: Duru Yünek Deputy Chair

Introduction:

The interconnected nature of information and communication technologies (ICTs) in the 21st century, has caused an unprecedented erosion in the online borders, making cyber security a transnational issue, which is to be dealt via a global approach. Cybercrime and cyber warfare are becoming more and more organized, costing more than a trillion dollars per year in practices that include inter alia, identity theft, online fraud and loss of intellectual property, targeting millions of people worldwide, as well as businesses and national governments. In the spirit of combating the emerging threat of cybercrime, the United Nations Economic and Social Council (ECOSOC), launched a special event on the 9th of December 2011, in New York, raising the issue of "Cybersecurity and Development"2. The discussions were concentrated in three specific pillars: (1) Awareness building concerning the ongoing situation, the emerging challenges of cybersecurity and its ties to development, (2) The identification of the best practices and policies in the direction of forming a solid background of cybersecurity globally, (3) The further research for options and strategies in the purpose of shaping a holistic approach towards the rising threat of cyber warfare. The question of whether a cybercriminal activity is perpetrated by a state or a Non-State Actor (NSA) is challenging and in many cases, remains unanswered. That's exactly the reason why tackling this issue demands the cooperation not only among states but between the states and the private sector, as well. Furthermore, mobilizing the civil society is of utmost importance, while maintain close cooperation with law enforcement agencies. A useful metaphor to further understand the interconnectivity of cyber security is to think of it as the financial and banking interconnectivity of the states. As it has been proven by the economic crisis of 2008, taking a step back in a national economy can create a domino effect with tremendously extended repercussions. The nature and the proceedings of cybersecurity and by extend of cyberwarfare, is in most cases not available to the public. Of course, one should not overlook the socio-economic factor of the topic under discussion; the division between the developed and developing states. The developing world often may not have the demanded economic and technological resources to combat cybercrime and effectively contribute to the safeguarding of cyber peace. This situation creates the ideal

circumstances for a “safe haven” for cybercrime perpetrators as it creates a window of opportunity for them, full of legal loopholes and technical deficiency. High risks are also being faced by underage users. Communities as well as families have to provide young people, entering the cyber world for the first time with the appropriate instructions, and of course, cautionary remarks. More specifically, media literacy guidelines provided online by International Telecommunications Union (ITU)3 are of imperative importance for the above purpose. The legal cornerstone concerning the combating of cybercrime is the Budapest Convention. In brief, this international treaty holds as its primordial goal the harmonization of national criminal legislative measures for the prosecution of cybercrimes including but not limited to; copyright infringement, fraud, child pornography, hate crimes and breaches of network security. In this regard, efforts are being made in building upon the Budapest Convention (2001, Convention on Cybercrime) 4 through enhancing it with the introduction of a global strategy. Taking into consideration all of the abovementioned factors, it can be concluded that the global aspect of the problem is consistently underlined by the states and points to the direction of global partnership as its solution. The United Nations are committed to employ their full strategic and analytic capabilities to their full extent in order to efficiently and effectively combat this burning issue for the international community.

Definition of Key Terms

International security: Generally refers to the synthesis of measures adopted by governmental and intergovernmental authorities for the purpose of ensuring survival and safety. These measures vary and can escalate from diplomatic agreements to military action. Undoubtedly, international and national security are directly linked and some might say that one works are a prerequisite for the other.

Cybercrime: Cybercrime is a criminal act and can be defined as "an offence that is committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)"7 As underlined by the Budapest Convention (2001) some terms related to the technical nature of a cybercrime have to be further explained, and explicitly defined; a. "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c. "service provider" means: i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service. d. "traffic data" means any computer data

relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Cyberwarfare:Defined as any virtual act of aggression with a political motivation aiming to affect the enemy's computer and information systems. The ultimate goal is to paralyze the financial and organizational systems via means of alternation or theft of top secret information, thus undermining and rendering useless networks, important websites and essential services. There are 2 possible acts of virtual aggression:

i. Sabotage the end goal is to disrupt the flow of operations and equipment necessary for the military and financial computer systems to function properly such as but not limited to; communications, fuel, power and transportation infrastructures.

ii. Espionage and/or security breaches the theft and unlawful acquisition of classified information from the enemy's institutions for purposes of military, political or financial nature. The method used is the disabling of the rival's networks, software, computers or the Internet.

Cybersecurity: Cybersecurity is the safeguarding of an online system's security, an online database's intactness and overall, the maintenance of one's virtual "sovereignty". To safeguard the above methods of prevention are of utmost importance. One to protect themselves has to have a comprehensive and in depth understanding of the enemy's "arsenal" as well as possible strategies. This translates to having a knowledge upon the potential information threats, such as an advanced virtual "virus" or other malicious programs. Cybersecurity defense strategies are largely based upon;

i. Identity management,

ii. Risk management

iii. Incident management

General Overview :

First and foremost, there is a need to keep an equilibrium between the privacy of citizens (and states) and public safety (and consequently, cybersecurity). Privacy is a primordial human right. "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence..." (Art. XII, Universal Declaration of Human Rights). Respect for privacy is the cornerstone of democracy, because it is directly linked to free thought and expression. However, privacy of computer networks is just as important as it includes many times sensitive personal data. Thus, the need for investigation of such crimes arises now more than ever. Moreover, cross border coordination is essential to the modern globalized nature of cybercrime, and the international legal framework needs to correspond to this circumstance. When a threat is global (e.g. "wannacry" malware that hit at the same time 150 states), the procedure of investigating the perpetrators needs to be global to be efficient. Thus, a complex international investigation is required. However, as it has been already stated, legal framework for cooperation on the matter is rather lacking and mainly focuses upon regional cooperation, while it gives no one single investigative governance authority. As a result, the investigation process is rendered tremendously complicated and eventually, ineffective. 17 Even in cases where the perpetrator of such acts of aggression is found, there is the possibility

that they have fled to a “safe haven”, where cybercrime laws are largely ineffective (or non-existent) and implementing an extradition request is essentially unachievable. What is more, jurisdictional limitations are definitely a deterrent to the speed with which a global evidence gathering process moves. With cross-border investigations, a law enforcement agency is required to go through a multitude of bureaucratic procedures that can take up more than valuable time. Electronic evidence is even more difficult to detect and even easier to hide. Of course, to this regard, the private sector can surpass some of these jurisdictional procedures and provide access to evidence held by private industry. Nevertheless, this does not mean that a need for an international effective understanding brought by a global cooperation framework is not still imperative. All in all, it should be underlined that the Budapest Convention of 2001, which is currently the most prevalent international convention on the matter, is highly effective given the circumstances and the fact that it was signed 16 years ago. The harmonization of domestic laws by its state parties is largely achieved and non-state parties have been using it as a model for their cybercrime legislation, as well. Thus, the question that comes forward is that the international community should not waste this stable ground put forward by this treaty and should instead build upon it by discussing with the non-members their hesitations. After all, is it the Budapest Convention really an international one if such a large amount of countries are not included

Major Parties Involved

European Union: Cybercrime is a priority for the mandate of the European Commission in the field of security. Given the constant increase in reliance on online services, the cost of cyber-attacks to European Union’s economy has grown in an unprecedented rate. This new challenge has brought about the need for an extensive harmonization of domestic legal framework, hence the issue of the Directive on Attacks against Information Systems, enhancing the cooperation between public authorities on the one hand, and the private sector and civil society on the other. EUROPOL meets the burden of investigation on cyberattacks, conducting thorough analyses and reports on cyber crimes in cooperation with the European Union Agency for Network and Information Security (ENISA). Overall, European strategy towards cyber security aims to increase cyber security and cooperation, also concentrates on making the EU a stronger player in the field of cybersecurity and mainstreaming cybersecurity in EU policies, supporting new initiatives with regard to new technologies, hence the support to the Budapest convention and its further development.

U.S.A.: The main missions towards the achievement of the US strategic goals for cyber security are taken on by the Department of Defence (DoD) with a view to build and maintain ready forces and capabilities to conduct cyberspace operations, to defend and secure the DoD information network and data, as well as to mitigate risks to DoD missions. The US strategy is focused on maintaining and defending the US homeland and US vital interests from destructive or disruptive cyberattacks of significant consequence. What is more, building and maintaining viable cyber options in the direction of controlling conflict escalation and shaping the conflict environment at all stages, is a primordial goal for the US cybersecurity strategy. Lastly, the United States support the Budapest convention and its further development in the spirit of creating robust international alliances and partnerships for the deterrence of shared threats and the increase of international security and stability

The Russian Federation Russia was the first country to take action addressing cyber security, submitting a resolution to the First Committee in 1998. In 2010, along with the USA and China, Russian delegates considered the issue of cyber-attacks the most serious of challenges in the 21stcentury, and followed up in 2011 by publishing a convention on International Information Security.

On the other hand, Russia has been accused of conducting several cyber-attacks, such as the ones between 2007 and 2008 on several eastern European countries. More recently, the incident sparked by Edward Snowden has brought the Russian stance into the limelight regarding the formulation of cyber warfare policies.

Organisation for Security and Cooperation in Europe (OSCE)

In December 2013 the OSCE participating states in the Permanent Council (decision No.1039, 26 April 2012), decided to step up individual and collective efforts to address the security of and in the use of Information and Communication Technologies (ICTs). They further decided to elaborate a set of draft Confidence Building Measures (CBMs) to enhance interstate cooperation, transparency, predictability, stability, and to reduce the risk of misperception, escalation, and conflict that may stem from the use of ICTs. The OSCE role as a regional arrangement under chapter 8 of the UN Charter confirms that the CBMs complement UN efforts to promote CBMs in the field of security of and in the use of ICTs.

People's Republic of China

There is a lot of controversy around the People's Republic of China concerning cyber security and cyber warfare. China was one of the first countries to support Russia with respect to cyber security, supporting the resolutions and suggested conventions. On the other hand, China has allegedly been accused of conducting cyber warfare on countries including Australia, India, Canada and the USA. Most recently, China has suspended the Cybersecurity Cooperation with the USA after being charged with cybercrime.

International Telecommunications Union (ITU)

The ITU is the only UN organization working on issues related to cybercrime. It is a treaty organization that joined the UN under article 57 of the UN Charter. This union is run by large and specialized technical staff with the role of setting technology standards. The main role of the ITU, following the World Summit on Internet Security (WSIS), and the 2010 ITU Plenipotentiary Conference, is to improve security and safety, as well as build confidence in the use of Information and Communication Technologies (ICTs). The Global Cybersecurity Index (GCI) is an ITU-ABI research joint project which ranks the cybersecurity capabilities of member states.

Timeline of Key Events

When	Event
1988	The Morris Worm was created and spread around computers in the US.
1995	Kevin Poulsen made sure that he would win the Porsche that KIIS FM was offering as he took control of the phone network and effectively

	blocked incoming calls to the radio station's number.
1999	Teen hacks NASA and US Defense Department. At the same time, the Melissa virus spreads through the Internet.
2007	Estonian government networks were harassed by a denial of service attack by unknown foreign intruders, following the country's spat with Russia over the removal of a war memorial
2008	The US Secretary of Defense's unclassified email account was hacked by unknown foreign intruders as part of a larger series of attacks to access and exploit the Pentagon's networks.
2009	U.S. and South Korean government, financial and media websites are attacked, apparently by North Korea. Attacks targeting Twitter and Facebook succeed in taking both sites offline for several hours. Gonzales also manages steal tens of millions of credit card and debit card numbers from over 250 financial institutions by hacking the payment card network of various companies.
January 2010	A group named the "Iranian Cyber Army" disrupted the service of the popular Chinese search engine Baidu. Users were redirected to a page showing an Iranian political message
January 2011	The Canadian government reported a major cyber attack against its agencies, including Defense Research and Development Canada, a research agency for Canada's Department of National Defense.
June 2013	In their first-ever meeting dedicated to cyber defense on Tuesday (June 4), NATO Defense Ministers agreed that the Alliance's cyberdefense capability should be fully operational by the autumn, extending protection to all the networks owned and operated by the Alliance
October 2013	The NATO Computer Incident Response Capability (NCIRC) upgrade project, a 58 Million

	euro enhancement of NATO cyber defenses, is on track for completion by the end of October 2013.

Previous attempts to resolve the issue

Governance of cyberspace is developing, and is moving towards the establishment of feasible norms. Since the debates have been present in the General Assembly‘s first committee for more than a decade, at least half a dozen UN organizations have become involved in the issue most notably in the last five years, and in the latest proposals for a code of conduct. There was a lot of debate about cybercrime in the UN between 1998 up until 2004, when the Budapest Convention on Cybercrime came into force. There have been several standards or norms on cyber warfare emerging at the UN and related forums in the past decades. The speed with which the strategies are being proposed, discussed and adopted about cyber space has increased since the year 2006. With reference to appendices I and II, the graphs illustrate the norm emergence and sponsorship of resolutions in the first committee respectively. From the trend line it can be concluded that the norm emergence and sponsorship of resolutions increased significantly in 2006 when there was support from China, and eventually the US in 2008.

Russia submitted a resolution in the First Committee in 1998 to resolve international issues concerning Internet security. Initially, the United States of America never supported the attempts of the Russian Federation to attain cyber security. However, later in 2009 the U.S. changed their earlier stance by co-sponsoring the draft resolution on cyber security that had been introduced by the Russian Federation in 1998.

In 2010, a Group of Governmental Experts (GGE), consisting of diplomats from several powerful member states, stated that “Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century”. This was followed by Russia proposing an "International Code of Conduct for Information Security" in September 2011 (together with China, Tajikistan and Uzbekistan). In October 2013 the UN approved a Russian proposal titled: “Development in the field of information and telecommunications in the context of international security”, a draft intended to keep the internet and mobile communications secure. The approval of the draft is dependent on the US’s stance on the issue concerning Edward Snowden, who leaked confidential information from the US’s national security agency. The UN General Assembly will debate this resolution this year.

Possible Solutions

Active targeting of underground fora to disrupt the

circulation of powerful and easy to use cyber criminaltools, such as malware kits and botnets.

Disrupt the infrastructure of malicious code writers and specialist web hosts through the active identification of developer groups and a joint action of law enforcement,governments and the Information & Communication

Technology industry to dismantle so-called “bullet proof” hosting companies.

Active targeting of the proceeds of cyber crime in collaboration with the financial sector. For e.g. money mule (is a person who transfers money acquired illegally (e.g., stolen) in person, through a courier service, or electronically, on behalf of others).

Continue to develop insight into the behavior of the contemporary cyber criminal by means of intelligence analysis, criminological research and profiling techniques, and based on the combined law enforcement, IT security industry and academic sources, in order to deploy existing resources more effectively

Appendix/Appendices

United Nations, General Assembly, Sixty-fourth session. (2010). *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures (A/RES/64/211)* [Resolution]. Adopted on the report of the Second Committee (A/64/422/Add. 3). Retrieved 20 July 2017 from:http://undocs.org/A/RES/64/211

United Nations, General Assembly, Sixty-fifth session. (2010). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201)*. Retrieved 1 September 2017 from: http://www.undocs.org/A/65/201

United Nations, General Assembly, Seventieth session. (2015). *Developments in the field of information and telecommunications in the context of international security (A/RES/70/237)* [Resolution]. Adopted on the report of the First Committee (A/58/457). Retrieved 20 July 2017 from: http://undocs.org/A/RES/70/237

United Nations, General Assembly, Seventy-first session. (2016). *Confidence-building measures in the regional and subregional context (A/RES/71/39)* [Resolution]. Adopted on the report of the First Committee (A/71/450). Retrieved 1 September 2017 from: http://undocs.org/A/RES/71/39

United Nations, General Assembly, Seventy-first session. (2016). *Developments in the field of information and telecommunications in the context of international security (A/RES/71/28)* [Resolution]. Adopted on the report of the First Committee (A/71/445). Retrieved 29 August 2017 from: http://undocs.org/A/RES/71/28

United Nations, General Assembly, Seventy-first session. (2016). *Developments in the field of information and telecommunications in the context of international security – Report of the Secretary-General (A/71/172)*. Retrieved 20 July 2017 from: http://undocs.org/A/71/172

United Nations Institute for Disarmament Research. (2016). *Report of the International Security Cyber Issues Workshop Series*. Retrieved 20 July 2017 from: http://unidir.org/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf

United Nations Institute for Disarmament Research. (2017). *Cyber* [Website]. Retrieved 31 August 2017 from:http://www.unidir.org/est-cyber

United Nations, International Telecommunication Union. (2007). *Global Cybersecurity Agenda (GCA)*. Retrieved 31 August 2017 from: https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

United Nations, International Telecommunication Union. (2014). *Understanding cybercrime: Phenomena, Challenges and Legal Response* [Report]. Retrieved 30 August 2017 from: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf

United Nations, International Telecommunication Union. (2017). *Global Cybersecurity Index (GCI) 2017* [Report]. Retrieved 20 July 2017 from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

United Nations, International Telecommunication Union. (2017). *ITU Cybersecurity Activities* [Website]. Retrieved 31 August 2017 from: https://www.itu.int/en/action/cybersecurity/Pages/default.aspx

United Nations, International Telecommunication Union. (2017). *ITU-EC-ACP Project* [Website]. Retrieved 1 September 2017 from: https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/Pages/default.aspx

Bibliography

1 “Cyber Warfare”. UN News Center. http://www.un.org/press/en/2014/gadis3512.doc.htm2 Marc Goodman, Future Crimes (Doubleday 2015), 32

3 “US Considering Retaliation to Chinese Hacks” The New York Times.

http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html

4 “U.S. decides against publicly blaming China for data hack” Washington Post. http://wapo.st/1RP2gYb

5 “China’s Xinhua says U.S. OPM hack was not state-sponsored”. Reuters. http://reut.rs/1P9X4Ka

6 “Chinese government has arrested hackers over OPM breach” Washington Post http://wapo.st/1PwmNiO

7 “10 Reasons To Worry About The Syrian Electronic Army”. Business Insider.http://www.businessinsider.com/syrian-electronic-army-2013-5?op=1

8 P.W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What Everybody Needs to Know. Oxford University Press

Post, Ashley. "Five Hackers Charged in Biggest Cyber Crime Case in U.S. History." Five Hackers Charged in Biggest Cyber Crime Case in U.S. History. Inside Counsel, 26 July 2013. Web. 17 June 2014. <http://www.insidecounsel.com/2013/07/26/five-hackers-charged-in-biggest-cyber-crime-case-i>.

Cybercrime." *DGs*. N.p., n.d. Web. 17 June 2014. <http://ec.europa.eu/dgs/home- affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm>.

United Nations Office for Disarmament Affairs. (2017). *Developments in the field of information and telecommunications in the context of international security* [Website]. Retrieved 20 July 2017 from:https://www.un.org/disarmament/topics/informationsecurity/

United Nations Office for Disarmament Affairs. (2017). *Military Confidence-building* [Website]. Retrieved 30 August 2017 from: https://www.un.org/disarmament/cbms/

World Summit on the Information Society. (2017). *WSIS Forum 2017: Information and Knowledge Societies for SDGs – Outcome Document.* Retrieved 30 August 2017 from: https://www.itu.int/en/itu- wsis/Documents/wf17/WSISForum2017_ForumTrackOutcomes.pdf