Study guide Zamun 2019

DISEC

Asymmetric Warfare on the Internet

Table of contents

Letter from the chair 3

Introduction to the topic 4

Introduction to the committee 5

Key terms and phrases 6

History of the topic 7

Notable issues connected to asymmetric warfare on the internet 8

Notable examples of cyber-attacks: 10

Conclusion 11

Useful Links 12

Other used literature 13

Letter from the chair

Dear Delegates

My name is Jozef Mačák and I will be this year's chair of the DISEC Committee. I am currently in my first year of university studies studying Security and Strategic studies + Economic policy on Masaryk University in Brno Czech Republic. I enjoy all sorts of competitions from Business Case competitions to Debates or MUNs. This will be my

Below you will find the study guide. Its aim is to provide you with a basic definition topic as well as to give you some sort of a road map onto which issues you might try to focus on. It aims to introduce you to the topic and establish a basis for your further research. Unless you have worked with a similar topic it is very probable that you need much more research in order to be successful in the committee. If you need help with anything connected to stuff mentioned above or anything to do with this MUN don't hesitate to contact me on my email jozef.macak22@gmail.com .

Introduction to the topic

Internet as we know it was created almost 30 years ago (at the time of the writing of this study guide) and since it's invention it went to change our lives in the most extraordinary manner, in most cases for the better .Many things we wouldn't be able to imagine living without nowadays, such as social media or search engines, would not come into existence were it not for the Internet. In 2017 according to Kleiner Perkins Internet trends, the average amount an adult user spends on the Internet per day was 5.9 hours. This means that almost a quarter of our lives is spent using the Internet in one form or another, and for most people reading this study guide it is probably even more. Logically with that we can come to the conclusion that this might also pose a huge vulnerability to all of us. Discounting phenomena such as internet related addictions or diseases we can focus on the other types of threats arguably more serious ones, the fact that most of infrastructure or transfer of secure data is somehow connected to the Internet.

Taking into account that more or less anyone can access these using the right tools and time, this easily proves that it might be the largest current vulnerability of most states. In most cases the only defense which can be mounted against such attacks is prevention of failure due to the human factor as well as devising some sort of rapid response procedure if an attack is discovered.

In addition to this there is also another form of asymmetric internet warfare in current times is information warfare. Numerous different sources of information have been created and nearly anyone can seem like a legitimate news authority given enough time and effort. This therefore makes it much harder for people to disregard fact from fiction causing people to rather believe news which adhere to their viewpoint and support their political stance. The lack of critical thinking and sheer amount of information that an individual has to process during the day create fertile ground for political manipulation. We can see this in almost any western country with events such as Brexit referendum or rise of the extremist parties across EU.

DISEC

Introduction to the committee

DISEC also known as **United Nations General Assembly First Committee** also known as **Disarmament and International Security Committee** is a committee responsible for mainly disarmament and de-escalation of weaponization.

The topics it discusses usually fall under seven thematic clusters:

1. Nuclear weapons
2. Other weapons of mass destruction
3. Outer space (disarmament aspects)
4. Conventional weapons
5. Regional disarmament and security
6. **Other disarmament measures and international security**
7. Disarmament machinery

This year's topic falls under the 6th cluster. Cyber and information warfare is proving to be used as an actual weapon nowadays. Therefore in the interest of international security we should try to define these terms and try to come up with guidance concerning these forms of warfare. We should define when the use of these forms of warfare is legitimate, how to combat its illegitimate use and what level of capability is acceptable. The main goal of this is to not fall into another arms race just with different weapons.

Key terms and phrases

Asymmetric warfare

With regards to asymmetric warfare, in our committee we will rather use the definition connected to the cyber threats and information warfare instead of the one connected to security and war studies. **Asymmetric warfare** therefore means **focusing an attack on the enemy's weak points and bypassing their strengths**. When connected to cyber warfare this makes more sense due to the fact that unlike in conventional warfare it is much more realistic. Every electronic or computer system has a weakness if the party trying to exploit it has enough patience to find it.

Do not confuse our definition with the traditional one ↓

Asymmetric warfare traditional definition

Asymmetric warfare is war between belligerents whose **relative military power differs significantly, or whose strategy or tactics differ significantly**.[1] This is typically a war between a standing, professional army and an insurgency or resistance movement militias who often have status of unlawful combatants. The belligerents still usually try to bypass their strengths; however compared to our case; cyber warfare and information warfare it is much harder to achieve.

Cyber warfare

Is defined as the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes. It can be used to disrupt concrete electronic systems, steal data from secure databases or hijack equipment of your opponent.

Information warfare

The strategy of attacking enemy news and communication sources in order reduce their ability to communicate. Nowadays used in the form of hoaxes and fake news to reduce differences between fact and fiction in order to achieve reduction of public support or fight capability or hamper their economy.

[1] https://en.wikipedia.org/wiki/Asymmetric_warfare

History of the topic

The point of this chapter will be to act as an intro into the history of our topics. It will contain mainly information about first uses of the forms of warfare such as information and cyber. If applicable some countermeasures to the events will be discussed also.

Cyber Warfare

The first form of cyber-attack happened in 1988 when Robert Morris, a graduate student at Cornell University created a self-replicating program as an “experiment”. Sometime later 10% of the back then Internet network worked only on spreading the “Morris Worm” further. This was also the first time cyber security started to be discussed. Many years later cyber warfare started to take form. Events such as email bombs and denial of service attacks during bombardment of the Balkans in 1999 or Chinese hackers hacking US companies in order to gain technological advantage are real solid examples of cyber warfare.

In 2014 it was first heard in DISEC that cyber warfare might pose a problem, most present delegates agreed with this notion. Until today 5 resolutions passed concerning cyber security in GGE (Group of Governmental Experts) which did not contain more than a promise to work together on these matters as well as basic confidence measures. In 2018 2 competing resolutions were proposed, one by Russia, China and the more authoritarian block proposing concepts of cyber sovereignty and such. The other one was proposed by USA the democratic/western block and is quite vague. Links to both are at the end of the study guide.

In short we can say not much has been done on a UN wide level to resolve real problems concerning cyber security other than idealistic promises of cooperation. The closest we got to a functional interstate body is a NATO Cooperative Cyber Defence Center of Excellence in Tallinn, as obvious from its name it only applies to NATO countries.

It is estimated that as of 2012, at least eleven nations have offensive cyber warfare capabilities and at least another thirty-three possess defensive capabilities.

Notable issues connected to asymmetric warfare on the internet

Undefined use of cyber warfare

When it comes to cyber warfare there is currently little to no standard as to how these weapons can be used. Compared to more traditional weapons such as nuclear, chemical or biological weapons there is almost nothing guiding the use of cyber warfare? There are no conventions of cyber warfare when compared to conventional warfare examples for the latter such as Geneva Convention.

This poses a couple of problems for the whole world

1. Potentially waging inhumane form of warfare
2. Spiraling costs in order to achieve secure status for respective states
3. Increased tension due to increased offensive capabilities by improving a states cyber-defense and cyber-warfare divisions.
4. Trouble with the defining the use of cyber warfare due to easy traceability
5. Trouble with defining the use of cyber warfare due to online hacking culture

1. Having no rules or conventions allows states to wage inhumane forms of warfare through cyber warfare. An example of this could be attacking hospital electronical systems either by attacking them directly or indirectly by causing power shortages in the state.

2. +3. Undefined cyber warfare to the classic security dilemma. Since there is no guidance or agreement as to how and in what extent cyber warfare is used between state actors

4. The fact that it is easily possible to cover tracks for any action constituting under cyber warfare makes it hard to define the legitimate use of cyber warfare. As even a low skilled hacker can be easily untraceable when it comes to his internet actions, or for that matter can easily impersonate someone else it is very hard to hold people accountable for their internet actions. This effect is magnified when suddenly a state sponsored hacking group is behind the actions making it virtually impossible to prove that a state actor was behind the attack.

5. Another problem making cyber warfare hard to hold states behind the attack accountable is that it is hard to know whether an attack on some secured systems is done by a state actor having a concrete goal in mind, or just another group of bored teenagers having a pissing contest in who can hack the more secure database or system. Theoretically it can even be a bit of both.

Lack of common guidelines in catching criminals and terrorists using cyberspace

As mentioned in the above, when it comes to fighting cyber warfare and hackers; especially the ones which are rogue actors or terrorists there is currently no common guideline which would enable cyber centers of various countries to cooperate with in catching these people of interest.

Information warfare

The creation of numerous fake or questionable news sites has many negative effects on the society. Firstly the difference between fact and fiction is getting erased. This effectively creates fertile ground for unrest and rise of radical groups in countries most affected by fake news and hoaxes.

Notable examples of cyber-attacks:

- 1998 Tamil guerillas disrupting to Sri Lankan government officials by sending hundreds of emails to their email addresses daily.
- 2007 cyber-attacks in Estonia in response to disagreement between Estonian and Russian government concerning the relocation of a bronze statue of a Soviet soldier.
- 2010 Stuxnet a worm believed to be created by joint Israeli-American efforts with the aim attack Iranese nuclear facilities in order to decrease Iran’s nuclear capability.
- 2012 Shamoon attack against Saudi Arabian Aramco was a politically aimed attack against Saudi Arabia in order to attack their oil extracting operations. According to the perpetrators they have done the attack because of the oppression of Al-Saud regime.
- 2003 Titan rain attacks. Believed to be one of the first Chinese PLA attacks against USA. Its aim was to get information from American Department of Defense and British Ministry of Defense.

Conclusion

Hopefully you are responsibly preparing for the conference and have all the way up to here. However by reading the study guide your preparation has only started.

Here are few tips in order to be excellently prepared for the conference:

- Read up about your country's foreign policy and public government statements, in order to get the "feeling" of their policy. Wikipedia usually has a page with foreign policy of a state in general also highlighting key issues. This will make it much easier if you get unexpected question during the General assembly.
- Research more about the topic. There should be a few useful links below ↓. You will never have enough knowledge and can always read more. In addition to this you can try to find study guides to similar topics on the internet.
- Statistics and numbers are always helpful and can make it much easier for you to prove a point in the committee session.
- Don't leave your preparation for the last week.

I wish you all best of luck with your preparations
Jozef Macak

Useful Links

Tips for preparing position papers and etc

https://bestdelegate.com/mun-made-easy-how-to-get-started-with-model-united-nations/

Resolutions connected to the topic and their analysis

https://undocs.org/A/C.1/73/L.37

https://undocs.org/A/C.1/73/L.27

https://www.cfr.org/blog/unpacking-competing-russian-and-us-cyberspace-resolutions-united-nations

Some Wikipedia links which speak for themselves

https://en.wikipedia.org/wiki/List_of_cyberattacks

https://en.wikipedia.org/wiki/Cyberterrorism

https://en.wikipedia.org/wiki/Cyberwarfare

Articles about cyber warfare

https://news.usni.org/2012/10/14/asymmetric-nature-cyber-warfare

https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/

Videos about cyber warfare and information warfare

https://www.rand.org/multimedia/video/2019/01/14/accountability-in-cyberspace-the-problem-of-attribution.html

Report about fake news and information warfare

https://datasociety.net/pubs/oh/DataAndSociety_Dead_Reckoning_2018.pdf

Other used literature

http://2013.hackitoergosum.org/presentations/Day3-01.Keynote%20Information%20Warfare%20mistakes%20from%20the%20MoDs%20by%20Raoul%20Nobody%20Chiesa.pdf

http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

https://www.un.org/press/en/2014/gadis3512.doc.htm

https://resources.infosecinstitute.com/cyber-warfare-cyber-weapons-real-growing-threat/

http://www.timesofisrael.com/new-cyber-bug-targeting-middle-east-but-israel-untouched-so-far/

http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

https://www.cfr.org/blog/unpacking-competing-russian-and-us-cyberspace-resolutions-united-nations

https://www.zdnet.com/article/the-day-computer-security-turned-real-the-morris-worm-turns-30/

https://medium.com/@cassiopeiaservicesltd/fact-or-fiction-social-media-as-news-source-increases-spread-of-fake-news-bf747a0821d1

https://online.lewisu.edu/infographic/339/full?cmgfrm=https%3A%2F%2Fwww.google.com%2F

https://news.usni.org/2012/10/14/asymmetric-nature-cyber-warfare

https://www.kleinerperkins.com/perspectives/internet-trends-report-2018/