The European International Model United Nations 2016

Security Council

Photo source: Georgetown Security Studies Review, March 2016.

Cyber-warfare

Welcome Letter

Distinguished delegates,

On behalf of The European International Model United Nations (TEIMUN), we would like to welcome you the United Nations Security Council. Participating as a delegate at the oldest collegiate MUN in Europe, especially in the Security Council, will be a challenging, yet extremely rewarding experience for you. In and out of session, you will be pushed to consider innovative solutions to modern issues of security. Outside of the committee room, you will have the opportunity to take part in cultural excursions, break a move on the dance floor, play football on the beach, all while making friends from around the world.

Through this background guide we hope to provide you with the necessary information needed to find a solution for the ongoing disputes of the Arctic territory. As chairs, we expect the delegates of the Security Council to give their best effort while respecting the rules of procedure and their fellow delegates. Ultimately, we hope that TEIMUN will be an amazing experience for all of you, and that besides the challenging debates and having a blast, you will make connections and friends that will last for a lifetime. We hope to meet you all in person very soon, and welcome to TEIMUN!

Your chairs,

Arijan Pranjić & Oliver Unverdorben
SC@teimun.org

Introduction

The ways of warfare have evolved through the centuries from the most primitive technologies and techniques, to the most advanced arsenals and tactics we possess currently. Today, in the 21st century, technology is advancing at an extremely rapid pace. This has resulted in new forms of waging wars, one of the most dangerous and notable ones being cyber warfare. Since the invention of the internet and its spread, new possibilities for "incursions" into either individuals, or nations, have opened up. Today the world is connected more than ever before. Smartphones, computers, "smart cars", even smart houses, are all being integrated into the world network for easier access to information. However it is not only the individuals that are being more and more connected. Governments as well as secret services around the world are also being increasingly connected via the virtual space, and even though the information is being secured with top level security and encryption, this does not prevent subterfuge.

The term "cyberwarfare" which is generally accepted by the United Nations and international customary law, refers to warfare conducted in cyberspace through cyber means and methods[1]. While "warfare" is commonly understood as referring to the conduct of military hostilities in situations of armed conflict. "Cyberspace" can be described as a globally interconnected network of digital information and communications infrastructures, including the Internet, telecommunications networks, computer systems and the information resident therein.[2] To be more precise international customary law separates the usage of cyberwarfare into three categories: under the law governing the resort to force between states (jus ad bellum), under the law of neutrality, and under the law of armed conflict (jus in bello).[3] Cyberwarfare attacks usually disable official websites and networks, disrupt or disable essential services, cripple financial systems, and amongst many other possibilities, steal or alter classified data.[4] Such attacks may cause severe harm, not only to individuals or groups, but entire countries.

One of the main issues when it comes to cyber-attacks is that the requirement to initiate a cyber-attack is a computer and an internet connection. This can make anyone with the required skills and an internet connection a potential "cyber terrorist", and even more importantly the cyber-attack could originate from anywhere on the planet. One of the best examples of how easy it is to initiate a cyber attack, is the recent cyber attack on TalkTalk in November 2015, by a 15 year old boy from Northern Ireland.[5] In this attack the teenager managed to collect personal information of circa 157,000 TalkTalk customers, and steal more than 15,600 bank account numbers.[6] It is due to this fact and

[1] http://searchsecurity.techtarget.com/definition/cyberwarfare

[2] https://ccdcoe.org/multimedia/cyberspace-definition-and-implications.html

[3] http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

[4] http://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare/

[5] https://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave

[6] https://www.theguardian.com/business/2015/nov/06/nearly-157000-had-data-breached-in-talktalk-cyber-attack

the potential damage that can be done by cyber-attacks that make it such a burning security issue in today's world, and even more so in the world of the future.

With the level of connectivity increasing day by day, and computers being integrated into an increasing number of everyday items and locations, we are getting ever more dependent on technology and connectivity. This increase of connectivity only makes cyber-attacks increasingly dangerous. Furthermore the damage to that the economy a cyber-attack could cause is tremendous. The FBI had to notify over 3,000 U.S. companies that they were victims of cyber security breaches in 2013, and 7% of the companies reported a loss of up to one million dollars, in 2013, due to cyber-attacks[7]. It is estimated that a worldwide figure of damage caused by cyber-attacks sums up to 445 billion dollars, which is 1% of the world's total income.

Besides the attacks on the cybernetic infrastructure[8] of the country, civilians, economy and governments, the dangers of cyber-attacks increase in the most dramatic way when it comes to the militaries of the world. Modern military intelligence includes the integration of state-of-the-art computers and electronics, leaving militaries around the globe susceptible to cyber-attacks. Going a step further, the development of UAVs, or drones, has experienced a boom in the last decade. These vehicles were first used for recon missions, however today they are equipped with both air to air and air to ground weaponry, which is capable of inflicting massive damage on its targets. The United States military has been using military drones in Pakistan since 2004, to target high ranking Al Qaeda and Taliban leaders, as well as to target their soldiers[9]. Since 2004, 64 high level insurgent leaders and several thousand Al Qaeda and Taliban warriors have been eliminated using drones. These attacks have also became very controversial due to a series of drone strikes resulting in civilian casualties[10]. According to different sources, ranging from The New York Times, to the Islamabad-based Conflict Monitoring Center (CMC), the total number of civilian deaths, since the beginning of the drone strikes in 2004, range from 200 to 2000 people[11]. Drones are being controlled remotely, and there have been recent advances in artificial intelligence which would allow them to be completely autonomous. This in itself presents a huge risk as even with all the security measures the possibility that a cyber-attack might be used to disable, or even take control over military drones still exists. The consequences of such an attack would be catastrophic, especially if a rogue or terrorist organization managed to take control of a military drone. Even though more

[7] http://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare/

[8] Cybernetic infrastructure is defined as environments that support advanced data acquisition, data storage, data management, data integration, data mining, data visualization and other computing and information processing services distributed over the internet beyond the scope of a single institution.

[9] http://atwar.blogs.nytimes.com/2013/06/17/how-cyberwarfare-and-drones-have-revolutionized-warfare/?_r=0

[10] http://securitydata.newamerica.net/drones/pakistan-analysis.html

[11] http://atwar.blogs.nytimes.com/2013/06/17/how-cyberwarfare-and-drones-have-revolutionized-warfare/?_r=0

complex military installations and branches have extremely high security measures, they are still susceptible to cyber-attacks, and the consequences could be even more catastrophic.

It is due to all these reasons that cyberwarfare and cyber-attacks present a huge threat in today's world. Many organizations and governments have set up defense programs over the past decades, however this is a constantly evolving battlefield. The US department for Homeland Security has been cooperating with the US Customs and Immigration Enforcement as well as the Secret Service, to coordinate its efforts in tracking down potential cyber attacks[12]. Furthermore, several governments including the ones of the Russian Federation and the People's Republic of China, have set up similar programs[13]. On top of that the United States, along with several other countries which have set up similar programmes, have started a campaign aimed at public awareness of cyber threats and cybersecurity. The program set up by US Homeland Security department named "Stop.Think.Connect" aims at not only increasing public awareness of cyber threats, but also focuses on how the general population can help combat cyber threats and attacks[14]. The attack and defense measures evolve almost on a daily basis, and with the world getting more and more connected combatting cyber warfare is becoming increasingly crucial. This is a global issue of great importance, one which if left unchecked could have disastrous consequences. That is why it is up to the UNSC to tackle this issue and provide a safer world, not only today, but also for the future.

Implications of Cyber Warfare

The vast majority of conducted cyberattacks are of criminal nature, designed to steal information and create economic harm. States, however, may possess the capabilities and resources to potentially inflict physical harm by bringing down critical infrastructure, amongst others. Within this context, the lack of a universal definition agreed upon by the international community of which actions may be classified as cyber war becomes a serious issue[15]. The significance of shedding light onto this grey zone becomes evident when taking into account the consequences of an act of war. This section shall give an insight into possibilities to define acts of cyberwar and its implications.

Following a decision of the Estonian government in 2007 to remove a war memorial dating back to the Soviet-era, a set of cyber attacks, aiming at overloading and consequently bringing down Estonian government servers, took place[16]. Due to Estonia's extensive use of internet facilities, these actions, which later became known as "Web War 1", resulted in some short interruptions of government operations. In 2008, a similar kind of cyberattacks was experienced

[12] https://www.dhs.gov/topic/cybersecurity
[13] https://ccdcoe.org/cyber-security-strategy-documents.html
[14] https://www.stopthinkconnect.org/about
[15] http://www.forbes.com/sites/lisabrownlee/2015/07/16/why-cyberwar-is-so-hard-to-define/#18f42cce5850
[16] http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia

by the Georgian government[17]. Parallel to the onset of the physical Russian military advance into Georgia, also the online battlefield in the cyberspace opened up. Several websites appeared, effectively providing everyone with an internet connection with very simple tools to flood Georgian servers with bogus requests in order to overwhelm and consequently disable those servers. This form of attack is known as DoS hacking, and is commonly used amongst hackers and groups aiming at disabling certain websites. Even though the websites could be traced back to Russian hackers, a direct connection to the Russian government could not be proved.

Opinions on whether these attacks should be classified as acts of cyber-war vary widely. According to some members of the international community, cyberattacks should only be viewed as amounting to acts of war, if actual military operations are conducted alongside[18]. The potentially wide-reaching consequences caused by cyber attacks alone, however, challenge this restricted definition of cyberwar[19]. Hence, another possible approach may be to regard the actual *harm* caused by such actions, qualifying acts resulting in severe *harm* rather than mere inconveniences as acts of cyber-war. Consequently, the actions experienced by Georgia would amount to an act of war under the former definition, whereas neither of the above specified attacks would be viewed as cyberwar under the latter.[20]

Theoretical qualifications become significant when taking into account the practical consequences of acts of war. Whereas cybercriminals would, in theory, be treated equally to conventional criminals, a state subject to an armed attack possesses the right to self-defence under the "UN Charter".[21] In the case of Estonia, the attack may well fall under the mutual defence clause of the North Atlantic Treaty Organization (NATO) and trigger its collective self-defense measures.[22] Hence, the response to an act in the cyberspace would not be limited to the online sphere, but could also prompt an actual physical response.

The attacks on the government servers of Estonia and Georgia brought the debate about a universal definition of cyberwar to the use of force. As a country subject to an armed attack possesses the right to individual or collective self-defence, an agreement by the international community on this topic is essential in order create legal certainty in the cyberspace. Once this is established the most important issue needs to be tackled and that is the possible solutions to ending the conflicts entirely. This needs to be done through international cooperation and understanding in hopes of eliminating the need for a physical confrontation completely.

[17] http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/08winter/korns.pdf
[18] https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm
[19] http://www.forbes.com/sites/lisabrownlee/2015/07/16/why-cyberwar-is-so-hard-to-define/#18f42cce5850
[20] http://www.wsj.com/articles/SB10001424052702304563104576355623135782718
[21] Charter of the United Nations, Chapter VII, Art. 51.
[22] Washington Treaty, Art. 5.

Historical background

The origins of cyberwarfare can be traced back to the 1970s, with the creation of the first so called "worm" viruses[23]. The first computer viruses soon evolved and were designed to do different things, with the primary objectives being either gathering intelligence or disabling a certain computer or a network. In the 80's and 90's, computer viruses and hacking evolved exponentially and new forms of computer viruses such as the "trojans" began to emerge[24]. The "trojans", amongst other viruses, were designed to steal data from a specific computer, be it personal, or corporate[25]. By the beginning of the 21st century illegal hacking groups were formed with one of the more famous ones like the "Russian Business Network" (RBN), starting to proliferate their "reign on the internet".[26]

However perhaps the most well known hacker groups is "Anonymous". "Anonymous" is a hacktivist group founded in 2004 whose first goals concerned mostly entertainment[27]. However over the years "Anonymous" has become the largest international, even global, hacktivist group which became famous for shutting down internet pages using DDoS attacks[28]. According to the group itself, it has no leader, rather it is composed of hackers from all over the globe who share similar ideas and goals. Having previously conducted attacks against certain groups such as the Church of Scientology in the US, the group gained popularity in 2011 with the "Occupy Wall Street" movement. It is at this time that "Anonymous" actually became favoured by the public, and were seen by many as the supporters of "the people", rather than institutions or governments [29]. Since than "Anonymous" continued its operations worldwide targeting specific websites owned by specific groups, one of their most recent attacks concerns the stealing of 276 GB of NASA (National Aeronautical Space Agency) radar logs and videos.[30] "Anonymous" became well known only in 2011 and 2012, however hacker attacks started to boom a long time before that.

It is around 2005 that the cyber-attacks started to boom in quantity, both conducted by states, individuals, and by corporations.[31] These attacks continue today, and have increased in sophistication and quantity, with China currently being the "leader" in the number of cyber-attacks conducted, closely followed by Russia and the USA.[32] However back in the year 2003 something called "botnet farms", began to emerge. Botnet farms were computers infected by "worm" viruses, which were designed to further spread the virus and infect more computers and networks, without the computer owner's awareness of the

[23] http://online.lewisu.edu/msis/resources/the-history-of-cyber-warfare
[24] https://antivirus.comodo.com/blog/computer-safety/short-history-computer-viruses/
[25] https://usa.kaspersky.com/internet-security-center/threats/trojans#.V1DMuZMrKSM
[26] https://www.theguardian.com/technology/2007/nov/15/news.crime
[27] http://abcnews.go.com/US/worldwide-hacker-group-anonymous/story?id=37761302
[28] http://www.digitalattackmap.com/understanding-ddos/
[29] http://www.fastcompany.com/1788397/real-role-anonymous-occupy-wall-street
[30] http://www.mirror.co.uk/tech/anonymous-hackers-attack-nasa-over-7602389
[31] http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm
[32] https://www.bba.org.uk/wp-content/uploads/2015/02/red24+Cybercrime+Top+10+countries+where+attacks+originate+-++2015.pdf

security breach[33]. The spread of botnet farms has led the FBI to commence an operation to track down and destroy the farms (computers where the virus originated from), and to detain the perpetrators. It is the same year that a botnet attack was detected on eBay, one of the world's largest consumer services on the internet. A year later in 2008 cyber-warfare was presented in an even more sophisticated form as a worm virus was detected aboard the International Space Station[34]. Later the same year, a group of hackers suspected to be working for Russia, managed to hack into the Pentagon's computers, and not long after that India's largest bank, State Bank of India, was hacked by a group of hackers from Pakistan[35]. In 2009, Israeli students developed a program that allowed the computers of Israeli citizens to be used by Israeli hackers to target Pro-Hamas websites[36]. Additionally, in the summer of 2009, a group of insurgents managed to compromise US military drones and intercept live video feeds with the use of an old Russian software which cost $26 USD.[37]

As can be seen from prior breaches in cyber-security, the intensity and technique of cyber-attacks has increased dramatically in the last decade[38]. This has resulted in the creation of cyber security divisions by a multitude of countries, as well as personal and corporate measures to protect information and fend off cyber threats. Today these threats pose a bigger threat than ever before. In the last few years, several events have shown us the capabilities and potential for destructive possessed by cyber-warfare methods. It is due to this that many call cyber-warfare the battlefield of the modern world and the future.

Responses to Cyberattacks

Even though there is no uniform approach on how to respond to cyberattacks, states and intergovernmental organizations, such as NATO, have begun to outline strategic concepts for cyber-warfare in order to establish a framework of circumstances under which cyberattacks could be used.[39] These approaches have in common that they focus on enhancing the defence of cyberattacks and on developing offensive capabilities. The following will provide an overview over these aspects of responses to cyberattacks.

On the one hand, the improvement on cybersecurity is an integral part of any strategy for cyberspace. As part of the national strategy of the US, for instance, federal agencies shall aid private-sector businesses responsible with critical infrastructure to prevent cyberattacks on its facilities.[40] Those measures, however, might involve a controversial extent of privacy infringement, as government agencies may be required to monitor a significant flow of data, such

[33] http://www.scientificamerican.com/article/spam-shadow-history-of-internet-excerpt-part-three/
[34] http://jcsl.oxfordjournals.org/content/17/2/187.full
[35] http://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html
[36] https://www.wired.com/2009/01/israel-dns-hack/
[37] https://www.theguardian.com/technology/2009/dec/17/skygrabber-software-drones-hacked
[38] http://online.lewisu.edu/msis/resources/the-history-of-cyber-warfare
[39] https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf
[40] https://epic.org/security/infowar/cip_white_paper.html

as e-mail communication. The European Union has setup several cybersecurity programs as well. The EU program for cybersecurity is focused around the "Cybersecurity Strategy of the European Union".[41] The cybersecurity strategy of the EU includes combating cyber threats and improving cyber resilience by increasing cooperation and information exchange, as well as raising awareness. Furthermore it focuses on the creation of an EU Cyber Defence Policy which would work in the framework of the already established Common Security and Defence Policy (CSDP)[42]. And ultimately it focuses on educating experts in the field to better combat any potential cybersecurity threat.

However important the improvement of defensive capabilities may be, an inherent feature of cyber-warfare remains that the advantage rests with the attacker. Hence, states are trying to come to terms with conditions under which they could employ cyberattacks in an offensive manner. The U.S. strategy for cyber-warfare adopted in 2015, for instance, may allow for pre-emptive cyberattacks by the US, if its interests can thereby be furthered[43]. Such actions could already be observed a few years before in 2007, when the Stuxnet virus, which infected Iranian computers at its Uranium enrichment facilities in Natanz and consequently slowed down Iran's nuclear programme, was traced back to the US and Israeli governments[44]. These programs and proposals pose a large problem to the international community as there are no specific laws in place which would limit the actions of cyber attacks in specific manners. The United Nations itself did have a few attempts to create certain international measures which would limit cyber activities, however a consensus was never reached. It is due to this fact that it is crucial to define exact limitations to cyber warfare, and to strictly define in what sorts of situation might it be used, as well as in which forms. Furthermore any form of military intervention requires the approval of the UN Security Council, should the same rule apply when it comes to the usage of cyber warfare? The Chapter VII, Article 41 of the United Nations Charter, states that the Security Council may decide what measures not involving the use of armed forces are to be employed to give effect to its decisions. However nowhere does it specify does this include cyber attacks, or cyber warfare, and till this point the Security Council hasn't issued a single resolution concerning the approval or use of cyber attacks as one of the possible measures. This is one of the issues that needs to be resolved as quickly as possible as it would open up an entirely new way of measures that the Security Council could employ and hasn't been able to use so far.

However, even though the UNSC hasn't issued a single resolution limiting the use of cyber attacks, on June 7th a group of experts agreed on a substantial report to the UN Secretary-General Ban Ki-moon, under the title of "On the Developments in the Field of Information and Telecommunications in the Context

[41] http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm
[42] http://www.eeas.europa.eu/csdp/
[43] http://www.nytimes.com/2015/04/24/us/politics/pentagon-announces-new-cyberwarfare-strategy.html
[44] https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

of International Security."[45] Upon the release of the report the Secretary-General appointed a group of 15 experts from the five permanent UNSC members with the addition of experts from Argentina, Australia, Belarus, Canada, Egypt, Estonia, Germany, India, Indonesia and Japan to carry out a mandate from the UN General assembly to "study possible cooperative measures in addressing existing and potential threats" in regards to information and communications technology (ICT).[46] Furthermore the members states of the United Nations have contributed to various extents to the requests of the General Assembly when it comes to sending the reports on their views on the international law and cooperation to prevent destabilization of state relations in cyberspace. In the extensive reports risks, threats and vulnerabilities were discussed, alongside a potential universal legal framework and trust and transparency building. What the member states and experts agreed upon is that cyberspace and cyber threats are an ever increasing danger to the international community and a problem that needs to be dealt with as soon as possible. Furthermore what has been proposed is the increase in transparency between states when it comes to the issues of ICT and cyberspace. Ultimately what the reports concluded that the potential creation of a universal legal framework when it comes to cyberspace would be necessary in order to create an ordered hierarchy and classifications of cyber attacks, as well as to distinguish in what cases would the use of cyberwarfare be allowed and would the Security Council have the authorization to call for a cyber attack on a certain actor, and in what situations.

Laying down strategies on when to employ offensive cyber-attacks also has to be viewed in the light of the concept of deterrence. Mostly for technologically advanced countries such as the US or China, which are more vulnerable to cyber-attacks, it is essential to display the capacity of locating the potential aggressor and presenting their cyber warfare capabilities.[47]

The practical translation of this claim, however, is enormously complicated by the fact that attacks can be launched from everywhere and aggressors can adopt the identity of innocent users. This anonymity makes it possible for governments to have attacks conducted by informal groups and hence deny accountability for those actions, so that attribution remains a rather big problem. Furthermore retaliatory cyberattacks on less modern countries may not produce the necessary outcomes to effectively deter those actions.

The outlined potential explosiveness of cyberwar highlights the necessity of effective mechanisms for the control of cyber-weapons and the use of it. In this respect, accords on rules by the international community are crucial. Such possible agreements on the prosecution of criminals or the duty of states to prevent or at least condemn attacks initiated from their territory could heighten

[45] https://www.un.org/disarmament/topics/informationsecurity/
[46] https://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity
[47] https://fcw.com/articles/2016/03/09/cyber-resiliency-chowdhry.aspx

the political costs of such acts of cyber-warfare and hence hinder the employment or escalation of such actions.

QARMAs (Questions a Resolution Must Answer)

1. Given modern breaches in cybersecurity, how should "cyber warfare" and "cyber-attacks" be legally defined? Define, or update, the legal definitions of cyber warfare, cybersecurity and cyber attacks.

2. With the number and sophistication of cyber-attacks increasing, what measures should be taken to prevent, or decrease, future state to state cyber-attacks?

3. Should an international framework be established to increase international cybersecurity?

4. Cyber threats originating from non-state actors, especially rogue and terrorist organizations, are often excluded in conversations regarding international cybersecurity. With increasing accessibility to tools of technological destruction among individuals and non-state actors, what should be done to ensure security from non-state actors, especially terrorist organizations?

5. Issues of personal privacy have become a contentious topic of debate with many civilians untrusting of government surveillance. How can security be increased without violating the privacy of citizens? What measures can be taken to ensure the right to personal privacy?

6. Computer systems and informational technologies are fields of constant change and evolution. What tactics should be employed in order to keep up with advancements in cyber warfare technology?

Authors: Arijan Pranjić, Oliver Unverdorben. TEIMUN 2016.