JAMIA MILLIA ISLAMIA
INTERNATIONAL
MODEL UNITED NATIONS

UNITED NATIONS GENERAL ASSEMBLY

BACKGROUND GUIDE

AGENDA

Assessing and minimizing the risks of cyber-attacks against States

Introduction to the Agenda

Brief Description

In 1945, when the UN charter was signed, the purpose behind several articles within it was to protect the sovereignty of states over their physical assets which were within their legal jurisdiction and/or physical boundaries. One of the fundamental functions of the United Nations in the 20th century was to act as a peacekeeping and conflict resolution organization in situations where nation states that would infringe on the sovereignty of one another would face the threat of international condemnation and in certain situations face uncompromising actions by the Security Council as well as other Intergovernmental Organizations. Arguably such a paradigm, despite its many ideological and evidential flaws, served to protect the rights and assets of many a nation from being compromised with a certain degree of success. One might conclude that for the time, this system of international cooperation and agreement based on principles enshrined in the UN Charter and other International Agreements was a fair set of rules for nations to compete on the world stage without putting the safety of millions of civilians at risk.

However, with the turn of the century it became clear that the decades old model of international intervention as a response to straightforward military aggressions was steadily becoming redundant as more and more non-state actors, operating behind the veils of rogue nations and competing political ideologies. Furthermore, as national assets turned digital in the 21st century, modern economies have become increasingly dependent on the free flow of information in the cyber domain and the integrity of cyber systems critical to infrastructure, defence, political instruments and media. All these new developments, undoubtedly spurred upon by the information revolution, have opened up a completely new domain of competition between nation states and state/non-state actors and in some cases turned into instances of outright aggression as the days of complicated human espionage, surveillance and military supremacy have become ineffective in gaining dominance in this new domain.

Keeping in mind this new view of how security threats to a nation is to be comprehensively handled and how the definition of a nation's sovereignty is no longer limited by physical limits or geopolitical boundaries, the 21st century certainly brings many challenges for the international community to solve with respect to how the United Nations can tackle threats that are no longer well defined by the charter it must operate by. With little precedent to consider while handling such situations, the UN stands at a crossroads where it must define cyber threats and establish some modus operandi to deal with them.

We shall, in the next few pages, explore a few examples of how, according to pundits, this new domain of 'warfare' is shaping modern geopolitical relations and though this background guide may be limited in its scope while defining the problem at hand, we implore all delegates to do their own research and come up with effective, realistic and politically acceptable solutions to the cyber threats that member states face. As representatives in the United Nations General Assembly - Plenary Session, delegates are free to touch upon any aspect they feel pertinent to the agenda be it the legality of cyber warfare, technical definitions/standards for countries or changes required in the international security instruments.

Cyberwarfare in the 21st Century

Cyber warfare refers to a massively coordinated digital assault on a government by another, or by large groups of citizens. It is the action by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption. The term cyber warfare may also be used to describe attacks between corporations, from terrorist organizations, or simply attacks by individuals called hackers, who are perceived as being warlike in their intent[1].

This definition is one that best encompasses the spectrum of activities that analysts have used to describe cyberwarfare however this is one that is still open to interpretation and not officially recognized by member states. As one of the most active 'warzones' ever in the history of mankind it is extremely worrisome that member nations have yet to even formally agree on a common definition and this is a recurring theme in most debates on the matter. Secretary-General Antonio Guterres has voiced his concerns on this issue[2] and has repeatedly asked for international organizations to regulate and minimize such activities but there is still much ground to be covered[3]. In a fight where humans are rarely directly affected, it is difficult to apply humanitarian law, hence leaving nearly the entirety of cyberwar currently unregulated and unrestricted.

As of 2019, the cost of cyberattacks borne by governments and private industry alike has already breached several trillions of dollars annually and has sprouted an entire industry of cyber security companies and products[4]. This figure is expected to grow exponentially as cybersecurity policies and measures mature in all nations. Currently according to the International Telecommunications Union, the UN Specialized agency for ICTs, only 19 countries have a well-developed cyber security framework and roughly half the member states have just started developing one[5].

While there is a definite monetary cost due to cyber-attacks, there are social, political and security challenges to such activities. Not only is public infrastructure such as utilities compromised daily, but defence systems and networks are constantly being attacked to both disrupt activities and steal data[6]. Reports are finding state-sponsored hacking groups have been increasing their activity and targeted both member states as well as the private sector[7].

Besides the attacks on the cybernetic infrastructure 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. 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. These attacks have also become very controversial due to a series of drone strikes resulting in civilian casualties. Drones are being controlled remotely, and there have been recent advances in artificial intelligence which would allow them to be completely autonomous. This presents a huge risk as even with all the security measures the

[1] https://definitions.uslegal.com/c/cyber-warfare/
[2] https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4
[3] https://www.cfr.org/blog/un-secretary-generals-call-regulating-cyberwar-raises-more-questions-answers
[4] https://www.forbes.com/sites/maciejduraj/2019/03/19/u-s-officials-at-recent-rsa-conference-highlights-china-as-biggest-cybersecurity-threat/#2699a0426fb9
[5] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
[6] https://www.daytondailynews.com/news/local/the-war-you-can-see-cyber-warriors-protect-from-daily-attacks/2kYpgKyutTmXvPg1QUhLPP/
[7] https://in.reuters.com/article/cyber-banks/state-sponsored-cyberattacks-on-banks-on-the-rise-report-idINKCN1R32OC

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 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.

On top of cyberattacks using compromised systems to achieve strategic objectives, it is also possible to use the cyber domain legally and use it to cause confusion and spread disinformation online. One of the earliest renditions of this would have its origins in scam call centres around the world but increasingly coordinated efforts of groups of individuals have been successful in 'trolling' social media with fake information. This is a major threat to any member state as it can lead to riots, protests and even affect elections if done with enough efficacy. This was a major concern during the US elections in 2016 and currently investigations are underway to find out the level of Russian involvement in the result of the election[8]. Simultaneously, member states are actively targeting these 'troll farms' in self-defence but obviously without any kind of intergovernmental organization such as the UNSC involving itself into the matter. One of the biggest concerns today is that our current international peacekeeping and intergovernmental cooperation paradigm is insufficiently equipped to address the threats of the fifth domain of warfare.

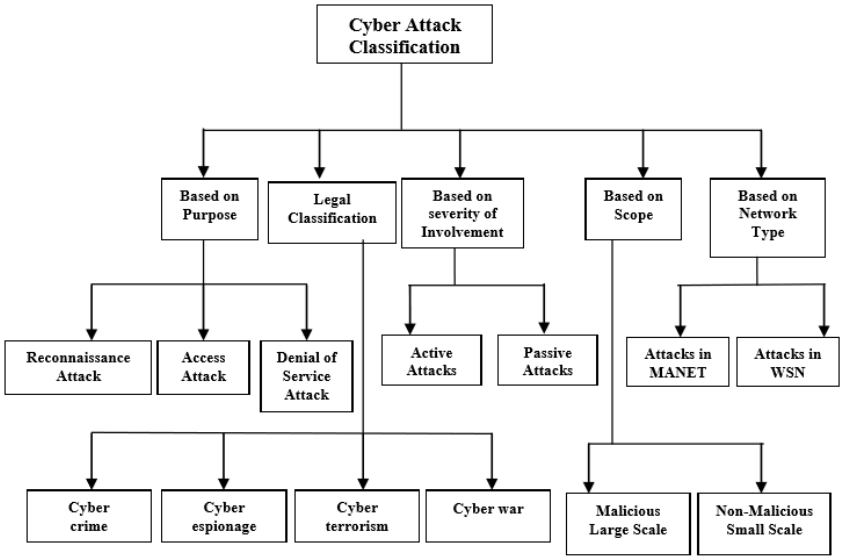

Figure 1 - A Proposed Classification Scheme for Cyber Attacks[9]

For a dramatic visualization of the current situation, it is possible to view live-maps[10] with information on DDoS, Botnets attacks as and when they are detected globally. Even cursorily observing these maps gives a viewer a rough idea on the cyber security trends that are afflicting member states.

[8] https://www.reuters.com/article/us-usa-trump-russia/u-s-disrupted-russian-trolls-on-day-of-november-election-report-idUSKCN1QF26Q

[9] https://pdfs.semanticscholar.org/ba7b/234738e80b027240e9bfd837bfba61c13e17.pdf

[10] https://www.deteque.com/live-threat-map/ https://cybermap.kaspersky.com/

Case Studies

Chinese Cyber Activity

China has been accused of using several methods to obtain U.S. technology (using U.S. law to avoid prosecution), including espionage, exploitation of commercial entities and a network of scientific, academic and business contacts. In addition to traditional espionage, China partners civilian Chinese companies with American businesses to acquire technology and economic data and uses cyber spying to penetrate the computer networks of U.S. businesses and government agencies; an example is the December 2009 Operation Aurora.

Huawei, a Chinese telecom giant with a presence globally, has been accused by several western nations for a variety of cybercrimes which has resulted in its 5G networks being banned in several member states. This has been a major headline for 2019 and has also escalated with arrests and threats from both the Chinese and American authorities.

China also accesses foreign technology through industrial espionage, with U.S. Immigration and Customs Enforcement officials rating China's industrial-espionage and theft operations as the leading threat to U.S. technological security[11]. In 1999, the 'Cox Report' was opened to the public which was a classified report created by experts for the US House of Representatives which highlighted worrying details on China's digital espionage campaign which had resulted in Chinese intelligence gaining top-secret information on USA's thermonuclear capabilities, missile and space program as well as state-of-the-art technologies[12].

Beyond traditional espionage, the Chinese government has also been accused of manipulating digital media such as when the New York Times reported that it was hacked after it published an article on PM Wen Jiabao in 2013. Attacks were claimed to be a part of a broader computer espionage campaign against American news media companies that have reported on Chinese leaders and corporations.

In a bid to contain Chinese activity, member states have taken several actions ranging from countering with their own cyberattacks, revamping their own infrastructure, diplomatic statements, hiring cybersecurity experts etc[13]. USA has repeatedly negotiated with Chinese authorities and reprimanded them for their activities and cyber threats and information theft was a major part of trade negotiations between the two countries. In September 2015, Obama and Xi Jinping vowed that neither the USA nor China "will conduct or knowingly support cyber enabled theft of IP, including trade secrets or other confidential business information," for commercial advantage. China reached similar agreements with Australia, Canada and the UK. Despite all these measures, reports on Chinese activity are still commonplace and this remains a major challenge for member states.

Cyberattacks by Non-State Actors

In recent years, numerous hacks against businesses around the world have also been identified, perpetrated by groups ranging from underground hacking collectives like Anonymous, to cyber-wings of military organizations such as the Syrian Electronic Army or ISIL. The objective of these hacks has been to steal or government secrets, cripple infrastructure, or co-opt communications systems, which

[11] https://www.forbes.com/sites/maciejduraj/2019/03/19/u-s-officials-at-recent-rsa-conference-highlights-china-as-biggest-cybersecurity-threat/#7a8ef4c6fb9f
[12] https://www.govinfo.gov/content/pkg/GPO-CRPT-105hrpt851/pdf/GPO-CRPT-105hrpt851.pdf
[13] https://www.washingtontimes.com/news/2019/mar/6/us-counters-china-cyberattacks/

angers corporations and governments wishing to protect their interests, their information, and their security.

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. 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 by the Georgian government. 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. The potentially wide-reaching consequences caused by cyber-attacks alone, however, challenge this restricted definition of cyberwar. 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.

Everyday new cyberattacks come to light which are caused by groups that are absent from any official records but based on evidence put together by the victims of these attacks, almost always there is a level of cooperation between these groups and an unfriendly member state who wish to do harm to a competing nation, the Centre for Strategic & International Studies keeps a track of all such incidents and releases reports for the public[14].

"You bring me a select group of ten hackers and within 90 days, I'll bring this country to its knees."

- *Jim Settle, former Director of the FBI Computer Crime Squad, 1999*

It can be said that there are primarily two major types of non-state actors that can be held accountable for cyberattacks – hacktivists and cyberterrorists. The boundary between hacktivists and cyber-terrorists is blurred, as they both share the intention of bringing about disruption by using more or less the same tools and techniques. Both these groups use the Internet to advocate their causes (propaganda), and to find supporters, both to aid them financially (fundraising) and to participate in their activities (recruitment)[15]. One of the clearest examples of cyberterrorism activities was back in 1998 when the LTTE attempted to 'disrupt' the communications of Sri Lankan embassies[16]. Groups such as Anonymous and Wikileaks often come to mind when talking about hacktivism but as is usually the case with conventional terrorism, the interpretations of activities depends on who you ask. There is a major grey area when observing the activities of these completely independent groups, may they have stated malicious or benevolent intents and is an important issue to be discussed

[14] https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity
[15] https://baldi.diplomacy.edu/italy/isl/Hacktivism.pdf
[16] https://littlefield.co/cyber-terrorism-understanding-and-preventing-acts-of-terror-within-our-cyber-space-26ae6d53cfbb

for all member states even though they probably have no direct connections with any member states. Cyberterrorists currently operate relatively freely on the dark web with recruitment, black market trade, DDoS and data breaches being part of the modus operandi of many terrorist groups. An example of this is the Pakistani Cyber Army which has in the past not only openly shared guides on how to hack and breach networks but has also actively defaced websites and attacked the digital infrastructure of member states such as India, Israel, China[17]. In response to these activities, there are groups in India and other nations which would retaliate in similar manner to Pakistani websites and digital assets. Such activities put millions of civilians at risk of being denied critical healthcare services, utility services and harms the economy of the target nation.

An Essential Classification of Non-State Actors Operating in Cyberspace

Non-state actors active in cyberspace having the potential to employ digital force or, to various degrees, to be involved in cyber military operations may substantially differ according to size, internal structure, motivational grounds, and relation with the state. Their size may vary from simple (even "unicellular") organisms to large transnational groups. Their organizational structure may be informal, lacking a chain of command, or complex, formal, and stably hierarchical. They may be driven by economic, political, ideological, or religious motivations. Usually, such organisms do not pursue purely military goals, such as power-outcome, typical of state actors or traditional non-state groups that engage in kinetic warfare. Further, they may be directed or stimulated by states or be fiercely opposed to any connection with state political entities.

a) Individual hackers - In cyberspace, the individual represents an important carrier of knowledge and technical skills (which are often located outside official educational structures). Further, new technologies have strongly augmented the capabilities of the individual beyond one's physical potentials, enhancing capacity and role as an autonomous actor in cyberwar. Individual hackers may serve as a valuable asset in the hands of the state, which can benefit from their technical skills. IT experts and hackers may be formally or informally employed in electronic warfare army units, such as the Israeli Defence Forces Unit 8200 or the Chinese People's Liberation Army.

b) Criminal organizations - Due to the lucrative potential of cybercrime, criminal organizations have flourished in cyberspace. Criminal consortia with a presence or ramifications online are among the non-state actors operating in cyberspace that present a higher degree of structural formality and aptitude to interconnect with the state. Their digital manifestations likely reflect the structured, hierarchical organization typical of the crime syndicates. The exclusively financial interest that fuels the organization is the focal point that permits its usability by the state, expressed through an economic relationship. Indeed, such organizations may prove to be ruthless enough and possess the necessary technology, knowledge, and structure to be effective in a cyber scenario. For instance, the Russian Business Network, a criminal organization which administers various illegal activities related to computer crimes—such as

[17] http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/pakistan-cyber-army-pca-hacking-indian-websites-promoting-pakistani-interests-in-cyber-space-and-nurturing-pakistani-hackers/

child pornography, phishing, spam, and malware distribution —appears, according to some commentators, to have contributed (in all likelihood, under state stimulus) to the cyber-attacks conducted in 2008 during the Russia–Georgia war and against Kyrgyzstan in 2009.

c) Cyber mercenaries - Species of the criminal organization genus, cyber "mercenary" groups are composed of highly skilled hackers specialized in sophisticated cyber-attacks. They may sell their skills to the public or private sector, which hires them to conduct precise and specific attacks. Their motivation is exclusively economic and the relationship with the contractor, although not permanent, is expressed in a specific agreement. The Kapersky lab, in collaboration with KISA (Korea Internet Security Agency) and Interpol, recently published an interesting analysis of a cyber mercenary group, active in Japan and South Korea since 2011. According to the research, the group already targeted—inter alia—governmental institutions, military contractors, communication operators and industrial/high-tech companies.

d) Hacktivists - Digital activist (or "hacktivists," a portmanteau of hackers and activists) groups are independent, politically or ideologically driven hacker groups. They may range from local units composed of no more than a dozen persons to large transnational organisms with several satellite sub-groups. Their internal structure, essentially informal, is shaped by the virtual composition and social life of the group. Operations are usually planned and organized on digital platforms, such as fora or IRC channels. The platform represents the (virtual) place where members meet, discuss, and share knowledge.

Problems Faced by Developing Countries

Developing nations are increasingly depending on ICTs to enhance their growth and helping their citizens to access basic services and in the age of active hacking groups capable of compromising such services it becomes immediately apparent that developing economies are the most vulnerable. The UN has in its own reports admitted that there is a need to develop cyber infrastructure in these countries since it is near impossible for them to independently combat experienced and well-funded groups with malicious intents[18].

For business leaders in South Africa, corporate cybercrime is taking centre stage as a major risk to the enterprise. The 'hacking economy' is now thriving globally, and local businesses and organisations have been falling prey to sophisticated attacks for some time now. These attacks often come in the insidious forms of encryption and ransomware.

Worryingly, for businesses that are already being challenged by a fragile socio-political environment, targeted cyber-attacks can prove to be crippling. Often, the reputational damage cannot even be properly quantified. New World Hackers, linked with the same group that attacked government sites, defaced the home page of the University of Limpopo and released a trove of data belonging to students. The hackers later revealed themselves to be operating under the #OpAfrica banner. They published data containing exam and intranet files, the personal data of 16,000 university alumni, as well as the personal information contained in some 1,700 department faculty entries. This is not an isolated incident with almost every developing economy vulnerable to data theft and system disruption[19]

[18] https://news.un.org/en/story/2011/12/397922-developing-countries-most-vulnerable-cyberattacks-un
[19] https://ictframe.com/cybersecurity-challenges-in-developing-countries/

Few experiences undermine a digital financial services (DFS) customer's finances and trust in DFS like becoming the victim of a cybercrime. This is especially true of low-income customers, who are least able to rebound from the losses, and of the newly banked, whose trust in financial services may be fragile. Unfortunately, cybercrime is a growing problem in developing countries, where customers often conduct financial transactions over unsecure mobile phones and transmission lines that are not designed to protect communications.

A report by an American software company, ranked Zimbabwe as the most hackable country out of 183 countries and National Exposure Index released last year reports that several internet protocol (IP) addresses in the country still use outdated protocol, leaving them susceptible to cyber-attacks. With a rapidly digitizing world and billions of internet-connected devices proliferating markets of even low income economies with law and order concerns, it becomes obvious why hackers find developing nations as the easiest targets to strike and since many of these nations also face terrorist threats, there is always the concern of cyberterrorism as well as illegal activities on the dark web and social media which are not strictly classified as a cyber-attack but are definitely a security concern in the digital space[20].

A developing nation faces a multitude of problems daily and can rarely afford to devote resources to cybersecurity but at the same time, a great deal of money is bled out of the economy because of nefarious groups. It becomes a major challenge for the international community to help these nations develop cybersecurity infrastructure without compromising their own state-of-the-art techniques. In the fight against cyberterrorism and cybercrime leaving a few powerful groups operate without retribution will only let them grow in strength and influence and eventually become a major problem for more member states. Also, it is important to remember that many developed states may wish to maintain a technological superiority over other countries to exert their own geopolitical clout globally, leaving developing economies in a precarious situation[21]. Expectedly, all these groups claim to be 'ethical hackers' and 'hacktivists' as well as face little challenge from the nations they operate in, leading to a sort of proxy digital war between opposing member states.

StuxNet Attack on Iran

The Stuxnet Worm first emerged during the summer of 2010. Stuxnet was a 500-kilobyte computer worm that infiltrated numerous computer systems. This virus operated in three steps. First, it analysed and targeted Windows networks and computer systems. The worm, having infiltrated these machines, began to continually replicate itself. Next, the machine infiltrated the Windows-based Siemens Step7 software. This Siemens software system was and continues to be prevalent in industrial computing networks, such as nuclear enrichment facilities. Lastly, by compromising the Step7 software, the worm gained access to the industrial program logic controllers. This final step gave the worm's creators access to crucial industrial information as well as giving them the ability to operate various machinery at the individual industrial sites. The replication process previously discussed is what made the worm so prevalent. It was so invasive that if a USB was plugged into an affected system, the worm would infiltrate the USB device and spread to any subsequent computing systems that the USB was plugged in to.

Over fifteen Iranian facilities were attacked and infiltrated by the Stuxnet worm. It is believed that this attack was initiated by a random worker's USB drive. One of the affected industrial facilities was the Natanz nuclear facility. The first signs that an issue existed in the nuclear facility's computer system in

[20] https://ictframe.com/cybersecurity-challenges-in-developing-countries/
[21] https://mse238blog.stanford.edu/2017/07/imunizr/cyber-security-challenges-in-developing-countries/

2010. Inspectors from the International Atomic Energy Agency visited the Natanz facility and observed that a strange number of uranium enriching centrifuges were breaking. The cause of these failures was unknown at the time. Later in 2010, Iran technicians contracted computer security specialists in Belarus to examine their computer systems. This security firm eventually discovered multiple malicious files on the Iranian computer systems. It has subsequently revealed that these malicious files were the Stuxnet worm. Although Iran has not released specific details regarding the effects of the attack, it is currently estimated that the Stuxnet worm destroyed 984 uranium enriching centrifuges. By current estimations this constituted a 30% decrease in enrichment efficiency.

Many media members have speculated on who designed the Stuxnet worm and who was responsible for using it to essentially attack Iran's nuclear facility. It is currently agreed upon that this worm was designed as a cyber weapon to attack the development of Iran's nuclear development program. However, the designers of the worm are still unknown. Many experts suggest that the Stuxnet worm attack on the Iranian nuclear facilities was a joint operation between the United States and Israel. Edward Snowden, the NSA whistle-blower, said that this was the case in 2013. Despite this speculation, there is still no concrete evidence as to who designed the original cyber weapon.

Significance of Threats

The biggest threat faced by nation states is the escalation of conflict in the event of a catastrophic cyber-attack, or even worse one followed by a conventional attack which pundits have come to describe as a 'cyber pearl harbour'[22]. When considering the practical consequences of acts of war, it becomes very clear that a universal understanding of what a cyberwar is and what protocol is to be followed when dealing with it. 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". 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-defence measures. 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. Such a chain of events is not dissimilar to how conventional conflicts snowball into convoluted international crises hence regulating and minimizing the threat of such a possibility is of the utmost concern for any responsible member state.

Furthermore, it is not just member states that face the risk of cyberattacks, but the digital assets of several intergovernmental organizations may be at risk of being compromised as hackers have in the past attempted to conduct cyber attacks against the OPCW, a major intergovernmental organization overseeing the proliferation of chemical weapons[23]. The international apparatus that has been put in place in the 20th century to maintain peace, stability and human rights now is at risk as many member states and non-state actors could use the cyber domain to disrupt their activities, destabilizing the paradigm of intergovernmental cooperation.

…all cybersecurity experts and the FBI believe that the Sony Pictures hack that year originated in North Korea. A hostile country hit a U.S. civilian target with the intention of destabilizing a major corporation, and it succeeded. Sony's estimated clean-up costs were more than $100 million. The conventional warfare equivalent might look like the physical destruction of a Texas oil field or an Appalachian coal mine. If such a valuable civilian resource had been intentionally destroyed by a foreign adversary, it would be considered an act of war[24].

- *Foreign Policy, September 12, 2018*

Simultaneously, member states must be fully aware of the threats that the private sector faces tremendous risk and has equal strategic importance as many government instruments. In the past few years, it has become evident that the private sector is by far the biggest market for cyber fraud, information leaks and other nefarious activities. While mostly in the realm of criminal and usually without any strategic objective of harming a state, these cyberattacks are difficult to distinguish from cyberwarfare and with non-state actors operating with impunity in several member states, it is not difficult to imagine nations themselves attacking the civilian sector of an adversary for nefarious purposes. In fact, the healthcare services of UK were compromised last year as a result of a worm which could be traced back to hackers in North Korea[25]. However, it is a difficult and arduous process to hold the member state accountable.

Technically speaking, it is very difficult to categorize the various types of cyber attacks that can take place but one of the biggest threats is that of an advanced persistent threat wherein the hackers have complete or partial access to the network of the victim without their knowledge. This can be used to further disrupt operations as

[22] https://www.tandfonline.com/doi/abs/10.1080/02684527.2017.1294379?journalCode=fint20
[23] https://idsa.in/cbwmagazine/russia-foiled-cyber-attack-on-opcw-winter2018
[24] https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/
[25] https://www.forbes.com/sites/kateoflahertyuk/2018/05/03/cyber-warfare-the-threat-from-nation-states/#5b4f207e1c78

well as extract sensitive information. Given below is a simple infographic that can be used to contrast the various impacts an APT can have with those of other types of attacks.

Figure 2 - Comparing Effects of Cyber Threats Faced by Nation States

Corrective Measures

As an issue faced by nearly every major economy and private enterprise, cybersecurity is a constantly evolving fight against those with nefarious intents with solutions lying in both technological improvement and public policy measures. Even though technical solutions are arising every day, one example being that of a regular simulated attack[26] with a red and blue time not unlike those in war games, it is difficult for these solutions to proliferate and truly be effective unless an international instrument for the same is created which is where policy makers come into their own.

… Microsoft announced an important – historic even – call for … a Digital Geneva Convention, which will "commit governments to implement the norms needed to protect civilians on the internet in times of peace." Also proposed is a neutral international organization that would investigate state-sponsored cyberattacks. And he called on private-sector tech companies to pledge to protect their users from all cyberattacks – no matter what their possible origin – and to never assist nation states in carrying out offensive operations in cyberspace.

- *Forbes, Feb 15, 2017*

As the fifth domain of warfare, nations have begun to establish completely new forces capable of projecting power and defending assets in the cyberspace such as the USCYBERCOM[27] which unlike other paramilitary arms, will constantly be conducting activities in real time against threats both domestic and international threats without any UN authorization or transparency in their operations which is a major privacy concern and an even larger security concern because of the very real risk of conflict escalation. Many experts from the field of policy making, science and technology as well as defence have opined on how to contain cyberattacks and how to respond to cyberwarfare. There have been calls for a 'cyber peacekeeping force' inspired by conventional peacekeeping operations of the UN[28] which would not just monitor but help build state capability of preventing such attacks from happening.

[26] https://www.weforum.org/agenda/2018/06/how-organizations-should-prepare-for-cyber-attacks-noam-erez/
[27] https://idsa.in/idsacomments/usa-ups-the-ante-in-cyberspace_msharma_250817
[28] https://arxiv.org/pdf/1710.09616.pdf

While it would seem to be a common-sense measure to impose sanctions on member states partaking in such activities in the absence of a comprehensive system to evaluate cyberattacks, often these sanctions have little to no effect as the cyber capability of a member state is mostly unaffected by outside influences[29] and on the contrary might spur cyberattacks of greater magnitude. It becomes a whole different contention when the security council itself is at odds when holding such member states accountable especially when cyberattacks are an inherently shrouded activity difficult to trace back to the perpetrators.

Previous UN Actions

Criminals and groups with malicious intent are spearheading the attempt, state or state-sponsored actions to disrupt these cyberspace networks are also being identified as a potential danger. At the same time certain nations have felt that the free flow of information, considered to be the primary reason for the Internet's success, could disturb societal peace and harmony. Even though governments have attempted to address these issues by creating national-level mechanisms, the very transnational nature of cyberspace has forced the international community to debate and form norms or rules that should promote good behaviour in cyberspace.

As in the real world, there are varying and sometimes opposing views held by nations when it comes to governing cyberspace. The United Nations (UN) has been working for over a decade to eliminate these differences and create a mechanism to ensure the security and stability of cyberspace. The UN First Committee on Disarmament and International Security which deals with disarmament, global challenges and threats to peace has been discussing the issue of information security since 1998, when the Russian Federation introduced a draft resolution on "Developments in the field of information and telecommunications in the context of international security" in the General Assembly (GA). Since then, member nations have been submitting reports about their thoughts on information security to the UN Secretary General. The initial period was dull without much movement within the UN towards dealing with issues in cyberspace. However, mounting reports of disruptions and the increasing potential of cyberattacks disturbing the peace in the real world led countries to examine these challenges more seriously within the UN. More substantial work began at the UN when it constituted a Group of Governmental Experts (GGE) in 2004 to "examine the existing and potential threats from the cyber-sphere and possible cooperative measures to address them". Since then there have been three GGEs set up by the UN, gaining significant ground. As witnessed during many other efforts by the UN to gain international consensus, the discussion on information security too has suffered due to geopolitical differences between major powers. Largely, the international community is divided into two groups– the West led by the US on one side and Russia and China on the other side. The West has supported the free-flowing nature and functioning of the Internet whereas Russia and China are seeking a role for governments in controlling the information flow on the Internet–multistakeholderism versus multilateralism. Secondly, there is a divide when it comes to the primary challenges that the UN discussions are trying to address. While the US and the West seek to contain economic espionage and criminal activity in cyberspace, Moscow and Beijing are looking at broader rules that would restrict a State's ability to use cyberspace for offensive purposes. Moreover, Russia and China are seeking to formalise an international treaty to govern cyberspace– opposed by the US and other Western countries.

Despite several rounds of negotiations, the GGE ultimately failed to arrive at an agreement over what would constitute a cyberattack and furthermore there was a stronger divide on whether member states would be free to respond to cyberattacks as they would in conventional attacks. Russia, China and Cuba, as part of the GGE, opposed and failed the proposed framework as their own policies were

[29] https://thenewcontext.org/can-the-un-prevent-cyber-attacks/

at stark contrast to those of the US, Europe and their allies[30]. In fact, several nations are in support of making outside interference in the cyber space of another country illegal and that is a major point of contention for all concerned parties[31], while the openness of the internet has been critical in the rapid share of information and rampant globalization we have witnessed but at the same time, there is an argument to be made when disinformation campaigns and social media efforts are made to undermine the sovereignty of another member state. Until consensus is brought on the matter with compromises on both sides, it is unlikely that significant breakthroughs will be achieved.

International Code of Conduct

In 2011 China, Russia, Tajikistan and Uzbekistan submitted a letter to the UN Secretary General requesting him to distribute the International Code of Conduct for Information Security drafted by them as a formal document of the 66th session of GA. The International Code of Conduct (CoC) was a step forward taken by Russia and China to regulate cyber norms and governance. Explaining the CoC, Beijing stated that:

"The International Code of Conduct for Information Security raises a series of basic principles of maintaining information and network security which cover the political, military, economic, social, cultural, technical and other aspects. The principles stipulate that countries shall not use such information and telecom technologies as the network to conduct hostile behaviours and acts of aggression or to threaten international peace and security and stress that countries have the rights and obligations to protect their information and cyberspace as well as key information and network infrastructure from threats, interference and sabotage attacks. CoC reflected the major concerns of these countries regarding the use of information as a weapon and the potential hostile use of cyberspace by a state. The Code restricted its signatories from using "ICTs including networks to carry out hostile activities or acts of aggression and pose threats to international peace and security. Not to proliferate information weapons and related technologies". Going against the western stance on the issue, the Code contained clauses that legitimised state control over the Internet. The Code suggested "that policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities for international Internet-related public policy issues". Additionally, calling for a change in the current Internet governance structures, the Code also suggested creating a multilateral mechanism to manage the Internet. Clauses curbing "dissemination of information which incites terrorism, secessionism, extremism or undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment" were also seen as a way to restrict freedom of expression and speech by many nations in the West. The Code, due to its contesting views with the West on cyberspace, received little support. In response to CoC, Washington issued a statement: the introduction of a draft Code of Conduct for Information Security presented an alternative view

that seeks to establish international justification for government control over Internet resources. At its heart, it calls for multilateral governance of the Internet that would replace the multi-stakeholder approach, where all users have a voice, with top-down control and regulation by states. It would legitimize the view that the right to freedom of expression can be limited by national laws and cultural proclivities, thereby undermining that right as described in the Universal Declaration on Human Rights. The UN General Assembly, Economic and Social Council, and Security Council often stress the importance of cybersecurity and regularly call on member nations to combat cybercrimes. These

[30] https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges
[31] https://www.npr.org/templates/story/story.php?storyId=130052701

organs usually refer responsibilities to the International Telecommunications Union (ITU) which is a UN agency based in Geneva which is responsible for coordinating efforts on these issues. They study cyber activity and set standards to which various governments are supposed to adhere to. The difficulty with such organizations is these standards are often non-binding and there are not enough mechanisms to force countries to play by the rules.

A major difficulty in combating cybercrimes is the sheer amount of data that needs to be monitored in order to catch cybercriminals. Several NGOs have stepped up efforts to monitor cyber activities and on reporting on cybersecurity issues. The International Association of Cybercrime Prevention, "provides information and training about cybercrime prevention. It is also an interdisciplinary research organization bringing together experts, professionals, and individuals involved with the misuse of Information Communications Technology."

The Cyber Peace Foundation is another NGO which is also involved with raising "awareness, counselling, education, training and to reach out to the citizens, the governments, law enforcement agencies (LEAs), private enterprises, NGOs working in cybercrimes and cyber security, universities, cyber security experts and bug bounty hunters; to provide a common platform on a global level."

On top of that, intergovernmental organizations have a key role to play in making sure nations coordinate and share resources to combat the threat of cyberattacks. In 2011, the first simulation of cyberattacks on a nation state was conducted in South East Asia.

Mass web destruction, spam and malware infection were among the scenarios involved during the first cross-border cyber drill organized by the United Nations and an international partnership against online threats in South-east Asia that aims to build cooperation and improve response measures to cyber-attacks.

- *UN News*[32]

There is also hope that bilateral agreements can help solve these issues. In September 2015, Chinese President Xi Jinping and American President Barack Obama met and discussed issues related to cybersecurity and came to a tentative agreement. Prior to President Xi's visit to Washington, Obama administration officials had warned that disagreements over cyberwarfare may lead to sanctions by the US government, and that products might not be able to be sold on international markets. In their meetings, they discussed steps each government should take to curb cyber-spying on both sides, and they agreed to disallow any hackers from committing acts of cyber espionage.

Challenges to Cyber Security Programs

As with any other field of espionage and geopolitical competition, a level of secrecy with regards to capability and sensitive information is often maintained by nations to stay one step ahead of competitors and in the cyber domain, this has profound effects. Day-Zero vulnerabilities, counter-hacking techniques and advanced protective systems are usually not shared and avoidable cyber attacks happen all the time because of the absence of cooperation and trust between member states. This is an understandable phenomenon as it keeps groups with malicious intents guessing about their target's capabilities but at the same time makes cooperation in the cyber domain extremely rare and often ineffective as countries with significant capabilities would wish to maintain a level of supremacy over even their allies.

[32] https://news.un.org/en/story/2011/12/397052-first-un-backed-simulation-cyber-attack-takes-place-south-east-asia

In March 2017, Jullian Assange and the WikiLeaks group published a series of documents revealing the database of day-zero vulnerabilities in several of the world's most popular operating systems[33]. This information was leaked from CIA's own database which begged the question as to why the US government failed to secure these commercially ubiquitous operating systems despite having known of them for nearly a decade. Many analysts believe that this was done by the USA to maintain an offensive edge over competitors even as these vulnerabilities put millions of devices worldwide at a huge risk to being compromised.

A major challenge to addressing cyberwarfare and related threats is still the fact that there is no accepted definition and while there has been much discussion over it with several proposals which have significant claims with justified definitions[34] by using the effect and the intent of the cyberattacks as grounds for qualification, member states need to reach consensus on the matter before international coordinated efforts on this front can even begin. Several studies and papers proposing a scheme for categorizing all types of cyber-attacks and related activities have been published and it is prudent for diplomats to keep them in mind when translating theoretical knowledge into proper policies[35]. Perhaps just as significant is the question of self-defence in response to cyber attacks as even with capabilities to retaliate, member states would have to build a strong case like how conventional retaliation would require significant grounds for action in order to justify a response. In the case of cyberattack, speed is of the essence if an ongoing attack is to be halted and the next biggest challenge is that of holding the perpetrators accountable as currently no international law or treaty would allow for member states to respond directly to hackers or attackers beyond the borders of the victim state however at the same time, there are no restrictions on activity in the cyber domain against such non-state actors as well. This convoluted system of shrouded accountability and the threat of disproportionate retaliation is the biggest debate surrounding the agenda and must be addressed by member states on an international platform.

Questions Any Resolution Must Answer (QARMA)

1. How should we define cyberwarfare and cyberattacks? As a constantly evolving domain based on new and upcoming technology, how can we define something that is inherently dynamic and ever changing?
2. Do the current laws on warfare and provisions in the UN charter apply to acts of aggression in the cyber domain?
3. How can the UN regulate cyberwarfare between member states and bring about peaceful, speedy resolutions to prevent conflict escalation?
4. How should non-state actors be treated and how can member states responsible for them be held accountable?
5. How can all these issues be tackled while keeping in mind the rights of personal privacy of individuals as well as keep healthy international competition in the private sector even after bolstering their cybersecurity infrastructure?

[33] https://www.reuters.com/article/us-usa-cyber-defense-idUSKBN17013U
[34] http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf
[35] https://content.sciendo.com/view/journals/jms/4/1/article-p1.xml