DISCUSSION ON THE POSSIBILITY OF A CYBER WAR AND THE USAGE OF AI IN DEFENCE PROGRAMS

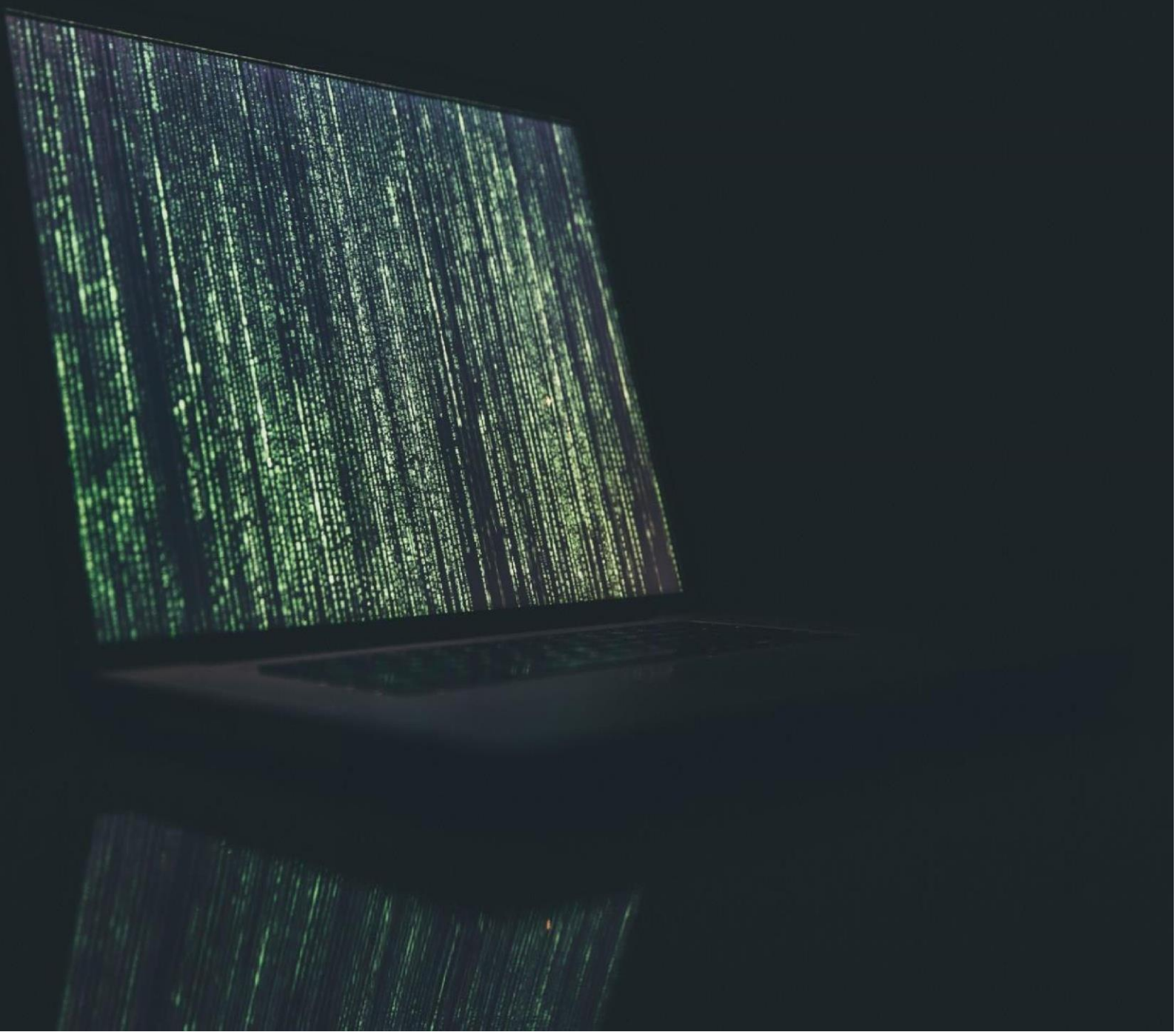

Table of Contents

Letter from The Executive Board

Greetings Delegates!

I appreciate your choice to be a part of the most educational and informational competitions, Model United Nations (MUNs). I am sure a lot of you who are going to do your first MUN would be a bit perplexed yet enthralled to see what's in the house for you but fret not, I am here assigned here to make sure your experience in the SNIS MUN at the UNGA-DISEC committee would definitely be something enlightening and informative. Considering the majority of first timers we are expecting in the committee, I would mostly spend a good portion of the first day discussing and dealing with the intricacies involved in the art of MUNning substantiated with a detail brief of the rules and procedures which would be followed in the committee.

For the smooth running of the committee, I do expect you to have some basic research on the agenda especially reading this study guide before you come for the conference but this study guide is not at all a conclusive package for your research rather it should give you a head start on the vital topics we expect you to bring to the floor during the conference.

Even if you are feeling a speck of anxiety or nervousness, kindly don't worry. We have all been there and we assure you that on the course of 2 days, you will take back some really jovial memories with a brimming pot of knowledge.

All the best!

Domil Antony Johnson

Chairperson

Introduction to the Committee

UNGA – DISEC

The United Nations (UN) Disarmament and International Security Committee
(DISEC) was created as the first of the Main Committees in the General Assembly when the charter of the United Nations was signed in 1945. Thus, DISEC is often referred to as the First Committee. DISEC was formed to respond to the need for an international forum to discuss issues of peace and security among members of the international community. According to the UN Charter, the purpose of DISEC in the General Assembly is to establish “general principles of cooperation in the maintenance of international peace and security, including the principles governing disarmament and the regulation of armaments” and also to give “recommendations with regard to such principles to the Members or to the Security Council.”

Although DISEC cannot directly advise the decision-making process of the Security Council, the fourth chapter of the UN Charter explains that DISEC can suggest specific topics for Security Council consideration. Aside from its role in the General Assembly, DISEC is also an institution of the United Nations Office for Disarmament Affairs (UNODA), formally named in January
1998 after the Secretary-General’s second special session on disarmament in 1982. The UNODA is concerned with disarmament at all levels—nuclear weapons, weapons of mass destruction, and conventional weapons—and assists DISEC through its work conducted in the General Assembly for substantive normsetting support in order to further its disarmament initiatives.

In light of the events in Hiroshima and Nagasaki, the first resolution by DISEC was created in 1946 to address international concerns for the “Establishment of a Commission to Deal with the Problems Raised by the Discovery of Atomic Energy.” DISEC deals with topics that centre around disarmament, global issues, and threats to peace that jeopardize international security. Under Article 11 of Chapter IV of the UN Charter, “The General Assembly may consider the general principles of co-operation in the maintenance of international peace and security, including the principles governing disarmament and the regulation of armament.”

Agenda

Discussion on the possibility of a Cyber War and the usage of AI in defence programs

Introduction

Not so long ago, stories about cyberwar started with scary hypotheticals: What if state-sponsored hackers were to launch widespread attacks that blacked out entire cities? Crippled banks and froze ATMs across a country? Shut down shipping firms, oil refineries, and factories? Paralyzed airports and hospitals? Today, these scenarios are no longer hypotheticals: Every one of those events has now actually occurred. Incident by catastrophic incident, cyberwar has left the pages of overblown science fiction and the tabletops of Pentagon war games to become a reality. More than ever before, it's become clear that the threat of hacking goes beyond nuisance vandalism, criminal profiteering, and even espionage to include the sort of physical-world disruption that was once possible to accomplish only with military attacks and terroristic sabotage.

So far, there's no clearly documented case of a cyberwar attack directly causing loss of life. But a single cyberwar attack has already caused as much as $10 billion dollars in economic damage. Cyberwar has been used to terrorize individual companies and temporarily render entire governments comatose. It's denied civilians of basic services like power and heat—if only briefly, so far— as well as longer-term deprivations of transportation and access to currency. Most disturbingly, cyberwar seems to be evolving in the hands of countries like Iran, North Korea, and Russia as they advance new disruptive and destructive cyberattack techniques. All of which means the threat of cyberwar looms heavily over the future: a new dimension of conflict capable of leapfrogging borders and teleporting the chaos of war to civilians thousands of miles beyond its front. To understand the unique threat cyberwar poses to civilization, it's worth first understanding exactly how the word has come to be defined. The term cyberwar has, after all, gone through decades of evolution— well chronicled in Thomas Rid's history of all things cyber, Rise of the Machines—which has muddied its meaning: It first appeared in a 1987 Omni magazine article that described future wars fought with giant robots, autonomous flying vehicles, and autonomous weapons

systems. But that Terminator-style idea of robotic cyberwar gave way in the 1990s to one that focused more on computers and the internet, which were increasingly transforming human life: A 1993 article by two analysts at the think tank RAND titled “Cyberwar Is Coming!” described how military hackers would soon be used not only for reconnaissance and spying on enemy systems but also attacking and disrupting the computers an enemy used for command-andcontrol.

Glossary

- Advanced Persistent Threat (APT)

  A cyber-attack that uses sophisticated techniques to conduct cyber espionage or other malicious activity on an ongoing basis against targets such as governments and companies. Typically conducted by an adversary with sophisticated levels of expertise and significant resources – frequently associated with nation-state players.

- Attack signature

  A characteristic or distinctive pattern that can help link one attack to another, identifying possible actors and solutions.

- Bot

  A computer connected to the Internet that has been compromised with malicious logic to undertake activities under the command and control of a remote administrator.

- Botnet

  A network of infected devices, connected to the Internet, used to commit coordinated cyber-attacks without their owner's knowledge.

✦ Brute force attack

An attack in which computational power is used to automatically enter a vast quantity of number combinations in order to discover passwords and gain access.

✦

Bug

A relatively minor defect or flaw in an information system or device.

✦ Cipher

An algorithm for encrypting and decrypting data. Sometimes used interchangeably with the word ‘code’.

✦ Computer Incident Response Team (CIRT)

A team of investigators focused on network security breaches. Their role is to analyse how the incident took place and what information has been affected/lost. They then use this insight to provide a response.

✦ Computer Network Defence (CND)

Typically applied to military and government security, CND refers to the measures taken to protect information systems and networks against cyber-attacks and intrusions.

✦ Control Objectives for Information and Related Technologies (COBIT)

A business framework developed and continually updated by ISACA comprising practices, tools and models for management and governance of information technology, including risk management and compliance.

✦ Cross Site Scripting (XSS)

Cross-site scripting (XSS) is a software vulnerability usually found in Web applications that allows online criminals to inject client-side script into pages that other users view.
The cross-site scripting vulnerability can be employed at the same time by attackers to over-write access controls. This issue can

✦

become a significant security risk unless the network administrator or the website owner doesn't take the necessary security means.

Cryptography

The study of encoding. Also, the use of code/cipher/mathematical techniques to secure data and provide authentication of entities and data.

✦ Decryption

The process of deciphering coded text into its original plain form.

✦ Denial of Service (DoS)

This is a type of cyber-attack that prevents the authorised use of information system services or resources, or impairs access, usually by overloading the service with requests.

✦ Dictionary attack

Known dictionary words, phrases or common passwords are used by the attacker to gain access to your information system. This is a type of brute force attack.

✦ Hashing

Using a mathematical algorithm to disguise a piece of data.

✦ Honeypot (honeynet)

A decoy system or network that serves to attract potential attackers, protecting actual systems by detecting attacks or deflecting them. A good tool for learning about attack styles. Multiple honeypots form a honeynet.

✦

✦

IP spoofing

A tactic used by attackers to supply a false IP address in an attempt to trick the user or a cyber security solution into believing it is a legitimate actor.

ISO 27001

The gold standard in information security management systems (ISMS), demonstrating the highest level of accreditation.

✦ Malware

Short for malicious software. Any viruses, Trojans, worms, code or content that could adversely impact organisations or individuals.

✦ Man-in-the-middle Attack (MitM)

Cyber criminals interpose themselves between the victim and the website the victim is trying to reach, either to harvest the information being transmitted or alter it. Sometimes abbreviated as MITM, MIM, MiM or MITMA.

✦ Packet sniffer

Software designed to monitor and record network traffic. It can be used for good or evil – either to run diagnostics and troubleshoot problems, or to snoop in on private data exchanges, such as browsing history, downloads, etc.

✦ Passive attack

Attackers try to gain access to confidential information in order to extract it. Because they’re not trying to change the data, this type of attack is more difficult to detect – hence the name ‘passive’.

✦

✦

Password sniffing

A technique used to harvest passwords by monitoring or snooping on network traffic to retrieve password data.

✦ Patch management

Patches (updates) are provided by developers to fix flaws in software. Patch management is the activity of getting, testing and installing software patches for a network and the systems within it.

Spam

The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

✦ Spear phishing

Spear phishing is a cyber-attack that aims to extract sensitive data from a victim using a very specific and personalised message designed to look like it's from a person the recipient knows and/or trusts.

✦ URL injection

A URL (or link) injection is when a cyber-criminal creates new pages on a website owned by someone else that contain spam words or links. Sometimes, these pages also contain malicious code that redirects your users to other web pages or makes the website's web server contribute to a DDoS attack. URL injection usually happens because of vulnerabilities in server directories or software used to operate the website, such as an outdated WordPress or plugins.

-
-
- Virtual Private Network (VPN)

  An encrypted network often created to allow secure connections for remote users, for example in an organisation with offices in multiple locations.

  Virus

  Programs that can self-replicate and are designed to infect legitimate software programs or systems. A form of malware.

- Zero-day

  Recently discovered vulnerabilities (or bugs), not yet known to vendors or antivirus companies, that hackers can exploit.

  Zombie

  A zombie computer is one connected to the Internet that, in appearance, is performing normally, but can be controlled by a hacker with remote access to it who sends commands through an open port. Zombies are mostly used to perform malicious tasks, such as spreading spam or other infected data to other computers, or launching DoS (Denial of Service) attacks, with the owner being unaware of it.

Scope of Cyber-Warfare

In the spring of 2007, an unprecedented series of so-called distributed denial of service, or DDoS, attacks slammed more than a hundred Estonian websites, taking down the country’s online banking, digital

news media, government sites, and practically anything else that had a web presence. The attacks were a response to the Estonian government's decision to move a Soviet-era statue out of a central location in the capital city of Tallinn, angering the country's Russian-speaking minority and triggering protests on the city's streets and the web.

As the sustained cyberattacks wore on for weeks, however, it became clear that they were no mere cyber-riots: The attacks were coming from botnets— collections of PCs around the world hijacked with malware— that belonged to organized Russian cybercriminal groups. Some of the attacks' sources even overlapped with earlier DDoS attacks that had a clear political focus, including attacks that hit the website of Gary Kasparov, the Russian chess champion and opposition political leader. Today security analysts widely believe that the attacks were condoned by the Kremlin, if not actively coordinated by its leaders.

By the next year, that Russian government link to politically motivated cyberattacks was becoming more apparent. Another, very similar series of DDoS attacks struck dozens of websites in another Russian neighbour, Georgia. This time they accompanied an actual physical invasion—a Russian intervention to "protect" Russia-friendly separatists within Georgia's borders— complete with tanks rolling toward the Georgian capital and a Russian fleet

blockading the country’s coastline on the Black Sea. In some cases, digital attacks would hit web targets associated with specific towns just ahead of military forces’ arrival, another suggestion of coordination.

The 2008 Georgian war was perhaps the first real hybrid war in which conventional military and hacker forces were combined. But given Georgia’s low rate of internet adoption—about 7 percent of Georgians used the internet at the time—and Russia’s relatively simplistic cyberattacks, which merely tore down and defaced websites, it stands as more of a historic harbinger of cyberwar than the real thing.

The world’s conception of cyberwar changed forever in 2010. It started when VirusBlokAda, a security firm in Belarus, found a mysterious piece of malware that crashed the computers running its antivirus software. By September of that year, the security research community had come to the shocking conclusion that the specimen of malware, dubbed Stuxnet, was in fact the most sophisticated piece of code ever engineered for a cyberattack, and that it was specifically designed to destroy the centrifuges used in Iran’s nuclear enrichment facilities. It would be nearly two more years before The New York Times confirmed that Stuxnet was a creation of the NSA and Israeli intelligence, intended to hamstring Iran’s attempts to build a nuclear bomb.

Over the course of 2009 and 2010, Stuxnet had destroyed more than a thousand of the six-and-a-half-foot-tall aluminium centrifuges installed in Iran’s underground nuclear enrichment facility in Natanz, throwing the facility into confusion and chaos. After spreading through the Iranians' network, it had injected commands into the so-called programmable logic controllers, or PLCs, that governed the centrifuges, speeding them up or manipulating the pressure inside them until they tore themselves apart. Stuxnet would come to be recognized as the first cyberattack ever designed to directly damage physical equipment, and an act of cyberwar that has yet to be replicated in its virtuosic destructive effects. It would also serve as the starting pistol shot for the global cyber arms race that followed.

Iran soon entered that arms race, this time as aggressor rather than target. In August of 2012, the Saudi Arabian firm Saudi Aramco, one of the world’s largest oil producers, was hit with a piece of malware known as Shamoon that wiped 35,000 of the company’s computers—about three-quarters of them—leaving its operations essentially paralyzed. On

the screens of the crippled machines, the malware left an image of a burning American flag. A group calling itself “Cutting Sword of Justice” claimed credit for the attack as an activist statement, but cybersecurity analysts quickly suspected that Iran was ultimately responsible, and had used the Saudis as a proxy target in retaliation for Stuxnet.

The next month, Iranian hackers calling themselves Operation Ababil hit every major US bank, knocking their websites offline with sustained volleys of DDoS attacks, a far more focused version of the takedown technique Russians had used against sites in Estonia and Georgia. Again, cybersecurity analysts detected the hand of Iran’s government in the attack’s sophistication despite the “hacktivist” front, perhaps a more direct message from Iran’s statesponsored hackers that any future US cyberattacks wouldn’t go unanswered. A little over a year later, in February 2014, Iranian hackers launched another, more targeted attack on American soil: Following public comments from Zionist billionaire Sheldon Adelson suggesting the US use a nuclear weapon on Iran, sophisticated hackers hit Adelson’s Las Vegas Sands casino, using destructive malware to wipe thousands of computers, just as in the Saudi Aramco case.

By 2014, Iran was no longer the only rogue nation exploiting the potential for cyberattacks to reach across the globe and inflict pain against civilian targets. North Korea, too, was flexing its cyberwar muscles. After years of staging punishing DDoS attacks on its favourite adversary, South Korea, North Korean hackers launched a more daring operation: In December 2014, hackers revealed they had deeply penetrated the network of Sony Pictures ahead of its release of The Interview, a low-brow comedy movie about an assassination plot against North Korean dictator Kim Jong-un. The hackers, calling themselves the Guardians of Peace, stole and leaked reams of emails along with several unreleased films. They capped off their raid by wiping thousands of computers. The hackers left a menacing image on wiped computers of a skeleton, along with an extortion message; they demanded both money and that the release of The Interview be cancelled. Despite that cybercriminal ruse, the FBI publicly named the North Korean government as the perpetrator of the attack, based in part on a slip-up that revealed a Chinese IP address known to be used by North Korean hackers. The roster of global powers entering the fray of cyberwar was growing.

AI-enabled Cyber Defence

The flow of digital information is expanding on a daily basis making it increasingly difficult to manage and structure it or even to separate what is important from what is superfluous.

Faced with this challenge, new promising breakthrough technologies are being developed to bring ‘data analytics’ to the next evolutionary level. Artificial Intelligence (AI), in particular, is expected to become significant in many fields. Some forms of AI enable machine learning like deep learning can be used to perform predictive analytics. Their potential for the defence domain is huge as AI solutions are expected to emerge in critical fields such as cyber defence, decision-support systems, risk management, pattern recognition, cyber situation awareness, projection, malware detection and data correlation to name but a few.

We have already seen tremendous technological progress on self-driving cars where an analysis of the surrounding environment is made in real-time and AI systems steer cars autonomously under specific circumstances. One of the potential applications of AI in cyber defence may be to enable the setting up of self-configuring networks. It would mean that AI systems could detect vulnerabilities (software bugs) and perform response actions like selfpatching. This opens new ways to strengthening communications and information systems security by providing network resilience, prevention and protection against cyber threats. Cyber experts agree that the human system integration is a key element that must be present in an AI cyber security system. If we take into account the high speed required to perform any cyber operation, it’s obvious that only machines are capable of reacting efficiently in the early stages of serious cyber-attacks. AI can thus overcome the shortfalls of traditional cyber security tools. It is also a powerful mechanism able to improve malware detection rates using a baseline of cyber

intelligence data. AI cybersecurity systems can learn from indicators of compromise and may be able to match the characteristics of small clues even if they are scattered throughout the network.

Another aspect relevant in building an AI enabled cyber defence could be the future implications of Quantum computing or high processing computers. This enhancement to support data-processing may increase the efficiency of algorithms. Algorithms are key components of running AI and may be tailored to counter complex cyber threats. An algorithm is a set of step-bystep instructions given to a computer to accomplish a specific task. AI may push this technology to another level, to achieve intelligent autonomous algorithms. To illustrate these research challenges, Facebook recently abandoned an AI experiment after ‘chatbots’ invented their own language which was not understandable by humans. Computer machines had demonstrated better skills than humans in playing chess or poker. This breakthrough technology is likely to be disruptive in many ways nobody can predict today.

Conventions and treaties on Cyber warfare and AI

✦ United Nations Treaties

United Nations Convention Against Transnational Organized Crime (2000)

This treaty, also known as the Palermo Convention, obligates state parties to enact domestic criminal offences that target organized criminal groups and to adopt new frameworks for extradition, mutual legal assistance, and law enforcement cooperation. Although the treaty does not explicitly address cyber-crime, its provisions are highly relevant.

Convention on the Rights of the Child (1989)

Article 34 of the Convention obligates state parties to protect children from all forms of sexual exploitation and abuse, including prostitution and pornography.

Optional Protocol to the Convention on the Rights of the Child (2001)

This protocol to the 1981 Convention addresses the sale of children, child prostitution, and child pornography. Article 3(1)(c) prohibits the production, distribution, dissemination, sale, and possession of child pornography. The Preamble mentions the Internet as a means of distribution. The definition of child pornography, set forth in Article 2(3), is broad enough to encompass virtual images of children.

- ✦ Council of Europe Treaties

The Council of Europe is one of several regional organizations established in the aftermath of World War II. It is separate and distinct from the European Union and has a much larger membership than the EU. The Council's core mission is the protection of human rights, but it also works to promote democracy, the rule of law, and uniform standards.

Much of the Council of Europe's work is accomplished through the drafting of treaties. To date, three treaties drafted under the Council's auspices for the purpose of combatting cybercrime have entered into force. Each of these treaties is open to signature by any country, whether or not it is a member of the Council of Europe.

Convention on Cybercrime (2001)

Also known as the Budapest Convention, this is the first international agreement aimed at reducing computer-related crime by harmonizing national laws, improving investigative techniques, and increasing international cooperation.

Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist or Xenophobic Nature Committed Through
Computer Systems (2003)

State parties which have ratified this protocol to the Budapest Convention are obligated to enact laws to criminalize racist or xenophobic acts that are expressed or otherwise communicated online.

Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007)

This treaty expressly prohibits the use of "information and computer technology (ICT)" to access child pornography (Article 21(1)(f)), to distribute child pornography (Article 30(5)) or to solicit children for sexual purposes (Article 23).

Neither the Geneva Convention nor the international humanitarian law can directly apply to this new type of conflict enabled by vast technological advancements in recent decades. The need for relevant treaties and regulatory framework on cyber warfare and AI has been voiced by many prominent stakeholders at the global level. No straightforward solution to cyber warfare and offensive hacking campaigns by countries exists – and coming up with one is no easy task.

Publicly calling out a country for a cyberattack is still relatively rare as digital tracks are often covered, or non-existent, and naming and shaming also has political ramifications. Yet there's a growing movement for a global agreement on what government-backed hackers can do. United Nations SecretaryGeneral António Guterres wants the world's governments to agree to what would essentially be a Geneva Convention for cyber warfare, regulating what is and isn't allowed in the scope of such of electronic conflicts so as to protect innocent civilians from its direct consequences, much like the 1949 treaty is meant to regulate conventional armed wars.

Microsoft voiced their opinions on the same as “Just as the Fourth Geneva
Convention has long protected civilians in times of war, we now need a Digital Geneva Convention that will commit governments to protecting civilians from nation-state attacks in times of peace. And just as the Fourth Geneva Convention recognized that the protection of civilians required the active involvement of the Red Cross, protection against nation-state cyberattacks requires the active assistance of technology companies. The tech sector plays a unique role as the internet’s first

responders, and we therefore should commit ourselves to collective action that will make the internet a safer place, affirming a role as a neutral Digital Switzerland that assists customers everywhere and retains the world's trust".

Role of Non State Actors

No nation-state thus far has overtly deployed cyber capabilities on the offensive during wartime, though covert operations have taken place during peacetime. NSAs have become substantially involved in the landscape of cyberattacks and even cyber warfare.

Because of the rise of international terrorist organizations, NSAs are now enacting influence on national governments' policy choices both within cyberspace and even more so outside of it. Specifically, within cyberspace, the NSAs have an advantage of an equal playing field with lowered barriers and easier access. Beforehand there existed an inequality between the warfare capabilities of NSAs and nation-state actors for reasons such as monetary resources, land resources, number of soldiers etc. Cyber warfare's lowered barriers to entry severely reduces the gap between NSA and nationstate capabilities within cyberspace. An individual themselves can possess immense amount of technical knowledge capable of creating havoc in the cyber space. Experts also agree that the potential for destruction to critical infrastructure only grows as technology advances and nation-states grow more dependent on network systems for day-to-day key functions. As this prospect of destruction expands, efforts to seek strategies to deal with state or terrorist non state actors engaging in cyber-attacks remain underdeveloped.

NSAs in the cyber realm have enhanced capabilities due to a number of reasons, including easier access to more destructive power, either on their own or through being aided or abetted by a state actor, their organizational structure, and their anonymity. The actors behind cyberattacks tend to hide their own identity to avoid consequences. The degree of connectivity, speed of access, and transmission capabilities challenge the traditional elements of national sovereignty, making it even more difficult to attribute cyberattacks to any actors. These attacks could

include air traffic control, financial markets, energy grids, telecommunications, and more as time goes on. In countries that are increasingly technology-dependent other potential malicious acts, which include tampering with water purification systems, rerouting trains and causing mass collisions, the opening of dams, and the meltdown of nuclear reactors, could cause devastating results similar to traditional warfare.

During the late 1990s, when access to and use of Internet had become commonplace, physical-world conflicts triggered many state-targeted cyber actions, primarily conducted by non-state actors. Hackers with nationalistic tendencies aimed their cyberauctions against foreign countries, commonly in support of their domestic governments, which could be seen at several occasions during the Kosovo conflict.

- ✦ Ordinary citizens

The most common actor in cyberspace is the ordinary citizen, using the Internet for various lawful purposes, such as browsing the web and using online services. When it comes to cyberauctions this actor category is mostly passive, or acts indirectly, e.g. as a “zombified” victim of a botnet (a collection of Internet-connected computers whose security defenses have been breached and control ceded to a malicious party), or as a more conscious actor voluntarily letting own resources be used by others in a cyberauction.

- ✦ Script kiddies

Script kiddies can be said to be the vandals, or perhaps graffiti artists, of the Internet. If access to a web server is obtained, a script kiddie will usually seize every opportunity to deface its web pages, later showing off the achievement in a common Internet Relay Chat (IRC) channel, on Twitter, or a similar social forum. The typical script kiddy searches for existing, frequently well-known and easy to find malware, pre-made scripts, or more advanced security auditing and penetration testing tools that they can use to identify and exploit weaknesses in remote computers, networks or other resources in cyberspace. They can and will do real damage to any network or computer resource they gain access to. The damage is also indiscriminate, often random and with little care, or even understanding, of the potentially

harmful consequences. No difference is made between attacking assets belonging to a large government agency or that of a small business owner.

- ✦ Hacktivists

Hacktivism is the use of cyberspace resources, in legal or illegal ways, as a means of general protest or to promote an expressed ideology or a political agenda. Hacktivism can also, indirectly, be used as a method to reach underlying, hidden political, military or commercial goals. Tools used by hacktivists include web site defacements, internet resource redirects, denialofservice attacks, information theft, web site parodies, virtual sit-ins and various forms of cyber- sabotage. Hacktivists can be seen as a cyberspace equivalent to Greenpeace activists or other groups carrying out acts civil desobediente.

These attacks include the “war” on Scientology, various support actions during the Arab Spring, and attacks on companies such as Louis Vuitton, Sony, Mastercard and U.S. government websites.

- ✦ Hackers

Hackers are people with deep knowledge and thorough understanding of computer technology, and how computer hardware, software and networking interact. They are commonly concerned with subtle details of operating systems, algorithms and system configurations. Depending on their motives, hackers are sub-categorized into black-hat hackers, white-hat hackers, and grey-hat hackers.

Black-hat hackers are the malevolent types of hackers originally dubbed “crackers”. They are people who exploit computer systems and networks for their own benefit. For example, they may hack into an online store’s computer system and steal stored credit card numbers. They may then use the stolen information to purchase merchandise, technical equipment or sell the credit card numbers to a third party.

- ✦ Patriot hackers

Patriot hackers are hackers whose main motives are to aid or support one’s own nation-state in an ongoing real-world conflict or war, by carrying out various disruptive actions in cyberspace directed towards the

enemy of the state. Chinese hackers have traditionally been especially inclined toward patriotic hacking. Several cyberauctions undertaken by these groups have been two-way “hacker wars” between the Chinese-based hackers and their antagonists in other countries.

Russia has also been home to an active patriot hacker collective.

- ✦ Cyber insiders

Cyber insiders are actors who have legitimate access to computer and network resources, including information residing in associated systems, but who are disloyal to their employer, hiring party or constituent, and are willing to betray them for monetary benefits or other reasons. The cyber insider may plant logical bombs or open backdoors in programs they help develop, or steal sensitive data by use of small, portable and easily concealed storage devices.

- ✦ Cyber terrorists

Cyber terrorists are terrorists who use computer and network technologies to carry out their attacks and cause public fear.

- ✦ Cyber espionage

In cyber espionage, agents make use of cyberspace resources for intelligence collection. They intercept information that passes through, or resides in, computer networks or computer systems of special interest, by using cracking and infiltration techniques, software and hardware tools for surveillance, or other similar approaches. The gathered data is analyzed and utilized in the preparation of intelligence reports for the commissioning entity. Cyber espionage may also entail the collection and analysis of open source information, publicly available on Internet web pages or via social media networks such as Facebook, Twitter, blogs, discussion boards and forums.

- ✦ Cyber militias

A cube militia may be defined as a group of volunteers who are willing and able to use cyberattacks in order to achieve a political goal. They utilize a common communications channel, such as an Internet forum or a social media service, and take measures to hide their true identities.

Combatting digital espionage

Cyber espionage is the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage. The lack of established international norms means that many cyber-attacks fall into a gray area below the threshold of total war. By exploiting this uncertainty, nation-state actors, such as Russia, Iran and China continue to pose serious risks. For the sake of efficiency, many infrastructure facilities, like water treatment plants, can now be operated remotely via the internet. As this continues to expand within industrial control sectors, basic cybersecurity protections such as firewalls and detection systems have not been effectively prioritized and integrated in many cases.

1) effective software security- Many systems lack the necessary degree of secure software design and coding practices, resulting in attacks, unvalidated user inputs, and information leakage through vulnerable web services.
2) proper configuration and maintenance of operating systems - When IT security personnel fail to deliver needed patches for operating systems or neglect the correct security options, systems become more vulnerable to malicious actors. The use of weak and default passwords can result in compromised access and intrusion.

3) network security- By leaving network connections open or failing to effectively implement network segmentation within the expanding cyberspace

Denial of Service (DoS)

A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users. DoS attacks can cost an organization both time and money while their resources and services are inaccessible.

There are many different methods for carrying out a DoS attack. The most common method of attack occurs when an attacker floods a network server with traffic. In this type of DoS attack, the attacker sends several requests to the target server, overloading it with traffic. These service requests are illegitimate and have fabricated return addresses, which mislead the server when it tries to authenticate the requestor. As the junk requests are processed constantly, the server is overwhelmed, which causes a DoS condition to legitimate requestors.

A distributed denial-of-service (DDoS) attack occurs when multiple machines are operating together to attack one target. DDoS attackers often leverage the use of a botnet—a group of hijacked internet-connected devices to carry out large scale attacks. Attackers take advantage of security vulnerabilities or device weaknesses to control numerous devices using command and control software. Once in control, an attacker can command their botnet to conduct DDoS on a target. In this case, the infected devices are also victims of the attack.

Botnets—made up of compromised devices—may also be rented out to other potential attackers. Often the botnet is made available to “attack-for-hire” services, which allow unskilled users to launch DDoS attacks.

DDoS allows for exponentially more requests to be sent to the target, therefore increasing the attack power. It also increases the difficulty of attribution, as the true source of the attack is harder to identify.

DDoS attacks have increased in magnitude as more and more devices come online through the Internet of Things (IoT). IoT devices often use default passwords and do not have sound security postures, making them vulnerable to compromise and exploitation. Infection of IoT devices

often goes unnoticed by users, and an attacker could easily compromise hundreds of thousands of these devices to conduct a high-scale attack without the device owners' knowledge.

The magnitude of DDoS attacks is hard to determine and there are no accumulated independent statistics on the number of attacks. However, numbers from a leading provider of DDoS protection solutions indicate that in 2016 more than 18 million DDoS attacks were launched globally. Still, the number is subject to great uncertainty as many DDoS attacks are not registered and as the statistics are based exclusively on analysis of part of the data traffic on the Internet. Nevertheless, it suggests that DDoS attacks are common and pose a real cyber threat.

Unlike many other cyber threats, DDoS attacks are targeted attacks against specific organizations, indicating that some organizations will rarely or never become the targets of DDoS attacks, while others will be regular targets. Still, powerful DDoS attacks have the ability to cause widespread collateral damage, putting everyone using the Internet at risk even though they may not have been targeted directly.

A powerful DDoS attacks against, for instance, a website may cause other users sharing IT infrastructure with the target to lose their internet connection. This may be the case if a client with a hosting company is the target of a DDoS attack that is strong enough to overload the hosting company's network, rendering the website of other clients inaccessible online. Internet providers and providers of cloud solutions that involve several clients sharing the same infrastructure face the same challenges, making the DDoS threat particularly serious for these companies.

Propaganda on the Internet

One of the primary uses of the Internet by terrorists is for the dissemination of propaganda. Propaganda generally takes the form of multimedia communications providing ideological or practical instruction, explanations, justifications or promotion of terrorist activities. These may include virtual messages, presentations, magazines, treatises, audio and

video files and video games developed by terrorist organizations or sympathizers.
Nevertheless, hat constitutes terrorist propaganda, as opposed to legitimate advocacy of a viewpoint, is often a subjective assessment. Further, the dissemination of propaganda is generally not, in and of itself, a prohibited activity.

Social media allows terrorist groups to provide limitless content directly to numerous websites or individuals, without having to go through a third party. Traditionally, the media had a monopoly on covering and interpreting terrorist incidents. Now, terrorists have the ability to instantly convey their messages directly to their target audience. The terrorists can also tailor their recruiting pitch, sending different messages to individuals based on their age, gender, location, or other factors. For example, ISIS sends starkly different messages to Muslims in the West than those closer to the Middle East.

Social media also “lowers the barrier of access” to terrorist propaganda. Social media platforms provide individuals with ways to easily reach terrorist propaganda and terrorist users. Unlike terrorist websites, which typically require individuals to intentionally locate the specific site, individuals may also stumble across terrorist social media accidently. For example, an individual may click on a link posted by a friend and unintentionally land on a jihadist forum. Furthermore, smart phones have made it possible for individuals to constantly have access to the Internet at almost all times and places. Thus, physical location and time are no longer relevant constraints on an individual’s ability to access terrorist information.

The Center for Strategic Counterterrorism Communications (CSCC), located in the U. S. Department of State, was founded in 2010 as the world’s first government-sponsored enterprise – not run by an intelligence agency – to counter online jihadist propaganda.

Recent Developments

Cybercriminals are using more advanced and scalable tools to breach user privacy, and they are getting results. Two billion data records were compromised in 2017, and more than 4.5 billion records were breached in the first half of 2018 alone. Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades. Cyberattacks are the fastest growing crime globally, and they are increasing in size, sophistication and cost.

Four new malware samples are created every second. Phishing remains one of the most successful attack vectors due to its speed, as most phishing sites stay online for just four to five hours. Users only report 17% of phishing attacks, and it is seen as a low-risk type of activity. As a result, today only 65% of all URLs are considered trustworthy. This puts a strain on both the consumer and any enterprise with an online presence.

The consumer Internet of Things (IoT) industry is expected to grow to more than seven billion devices by the end of 2020, according to Gartner. Many consumers do not see IoT devices as a vulnerability, because a significant portion of them do not have a user interface. This could lead to issues understanding what kind of data the device collects or manages.

However, IoT devices are not only collecting valuable user data. They could become an entry point for an attacker or tool to launch a distributed denialofservice (DDoS) attack. IoT devices are not secure by design, because putting a focus on security would significantly increase manufacturing and maintenance expenses.

The majority of AI qualities serve malicious purposes. AI systems are cheap, scalable, automated, anonymous and they provide physical and psychological distance for the attacker, diminishing the immediate morality around cybercrime.

- Twenty-seven countries signed a joint agreement on what is fair and foul play in cyberspace. Countries agree to follow international law and that it’s okay to spy and hack intelligence and military targets but not civilian infrastructure.
- TechCrunch reports that a number of malicious websites used to hack into iPhones over a two-year period were targeting the Uyghur Muslim minority in China’s Xinjiang state. It explains the websites were part of a campaign to target the group by infecting iPhones

with malicious code simply by visiting a booby-trapped web page and gain access to a victim’s messages and passwords, and track their location in near-real time.

- The publicly owned Nuclear Power Corporation of India Ltd (NPCIL) has confirmed that malware associated with state actors has been found on the network of the Kudankulam Nuclear Power Plant. The malware appears to be connected to the Lazarus group, which has been identified by the US Department of Justice as a North Koreanbacked cyber-crime organization. Some organizations have linked the Lazarus group to the WannaCry ransomware attacks which briefly rocked the NHS and other major institutions around the world in May 2017.
- Cyber actors Turla group acquired Iranian tools and infrastructure to conduct attacks on dozens of countries, security officials in the UK and USA have revealed.
  Interestingly, in some instances, it appeared that the implant had first been deployed by an IP address associated with an Iranian APT group, and then was later accessed from infrastructure associated with Turla, a suspected Russia-based group, suggesting Turla effectively took control of victims previously compromised by a different actor.

  Turla, which is also known as Waterbug or VENOMOUS BEAR, regularly collects information by targeting government, military, technology, energy and commercial organizations.
- Ever since they were one of the groups involved in the infamous hack of the Democratic National Committee in 2016, the trail has largely gone cold on the Russian intelligence hackers known as Cozy Bear.
- New research, however, shows Cozy Bear (also known as the Dukes) never went away at all. Although they managed to stay out of the spotlight for over two years, the group has been actively engaged in a sixyear-long spying campaign targeting the ministries of foreign affairs in at least three European countries and a Washington, DC, embassy of a European Union nation, according to new work by the Slovakian cybersecurity company ESET.
  Two other advanced hacking groups from Russia, bearing the code names Fancy Bear and Turla, were found on some of the same breached computers. Russian hacking groups from different arms of the government—in this case the military and the intelligence

agencies—are known to aggressively compete with each other when going after highvalue targets.

- Researchers linked multiple Cyber-espionage campaigns across Asia to the Chinese threat actor group PKPLUG. The group uses its PlugX malware and the number of additional payloads in the campaign. The group primarily targets Southeast Asia regions such as particularly Myanmar, Taiwan, Vietnam, and Indonesia and other parts of Asia such as Tibet, Xinjiang, and Mongolia. The group found active for more than six years, their first attack dated November 2013, against Mongolia, in the attack the malicious payloads launched via digitally signed legitimated applications.
- The United States carried out a secret cyber operation against Iran in the wake of the Sept. 14 attacks on Saudi Arabia’s oil facilities, which Washington and Riyadh blame on Tehran, two U.S. officials have told Reuters. The officials, who spoke on condition of anonymity, said the operation took place in late September and took aim at Tehran’s ability to spread “propaganda.”