United Nations Security Committee

Crime, terrorism and warfare in cyberspace: the dual use of technology

Introduction

As cyber technology improves and advances, so do the capabilities of those who choose to use it for destruction and harm. The world that we know today is already incredibly reliant on cyber technology. An increasing amount of businesses, governments, individuals and their interests depend on cyberspace for day-to-day tasks. As more critical entities essential to the function of our society become immersed in the cyber world, the more vulnerable they are to high risk attacks by a variety of actors. These actors can include rogue individuals, hacking groups, terrorist cells and even government security agencies. According to the United Nations (UN) Global Cyber Security Index (GCI) of 2018 "there will be 70 per cent Internet penetration [percent of world population online] by 2030, increasing the need for a more cyber-secure space".[1] Because cyberspace exists without national borders, and many illicit actors active in this realm operate transnationally, this growing problem demands international attention, cooperation and problem-solving.

The Secretary General of the UN Antonio Guterres said during a speech in 2018, "I am absolutely convinced that, differently from the great battles of the past, which opened with a barrage of artillery or aerial bombardment, the next war will begin with a massive cyber attack to destroy military capacity... and paralyse basic infrastructure such as the electric networks… Episodes of cyber warfare between states already exist. What is worse is that there is no regulatory scheme for that type of warfare, it is not clear how the Geneva Convention or international humanitarian law applies to it[2]" With this mandate from the Secretary General, the UN should continue to expand this role into the cyber domain.

Current Events

The following are recent events that exemplify the importance of cyber security and demonstrate that no entity is immune to the destruction that cybercrime and cyber warfare can cause. In 2017, the Petya cyber-attacks targeted Ukraine and then spread globally to other countries. Within Ukraine, a variety of organizations were attacked like banks, ministries, newspapers and electricity firms. ATMs stopped working and nuclear facilities were forced to be manually monitored causing disruptions in key aspects of the financial and energy sectors. The impact of this attack was great; computers at a variety of companies and governments were shut down leaving them defenseless and unable to use the technology they significantly rely on. The effects of this attack were felt worldwide reaching from the source in Ukraine to countries such as the United States, Russia, France, Germany, the United Kingdom and businesses/corporations that operate in these countries according to the New York Times.[3] The impact of this attack was great. In the United States in 2015 and 2016, Russian computer hackers were able to infiltrate the Democratic National Committee's computer network at access important data and information.[4] In 2013, South Korea was targeted by a cyber attack that affected computer networks of banks and broadcasters, with the attacks originating from North Korea; this is a new development in warfare in the conflict between the two states that has existed for

[1] UN Global Cyber Security Index (2018)

[2] Khalip, Andrei. "U.N. Chief Urges Global Rules for Cyber Warfare." Reuters. Thomson Reuters, February 19, 2018. https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4.

[3] Perlroth, Nicole, Mark Scott, and Sheera Frenkel. "Cyberattack Hits Ukraine Then Spreads Internationally." The New York Times. June 27, 2017. https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html.

[4] Alperovitch, Dmitri. "Bears in the Midst: Intrusion into the Democratic National Committee." CrowdStrike, June 15, 2016. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

over 50 years. [5] The Shamoon attack in 2012 on the Saudi Arabian oil company Aramco is considered to be one of the largest and most expensive cyber attacks in history. It crippled the production, refinement, and outflow of oil in Saudi Arabia for a week. However, the perpetrator(s) of the attack have yet to be identified.[6] This attack demonstrates the power that these non state actors can wield with only a few lines of code, but also to how invisible and hard to trace these groups or individuals can be while committing acts.

We have not yet seen a cyber terrorism attack on a large scale with significant civilian casualties. However, terrorist groups are showing a greater interest in developing cyber capabilities to do harm. In 2015, the "CyberCaliphate" division of Islamic State hacked into the Twitter and YouTube accounts of the U.S. Central Command.[7] They posted propaganda and had access to the accounts for a short period of time. The ability of this group to carry out this attack demonstrates the potential for terrorist groups to expand their capabilities to carry out more damaging and destructive attacks in the future.

These specific cases are just a few of the many cyber attacks that have been committed against state and non state actors. They demonstrate that any entity with a reliance on cyber technology can be at risk. The repercussions from cyber attacks can be anything from a disruption of daily functions, to financial crashes, to political manipulation, and in some cases civilian casualties. As the rate and degree of attacks increases, and their consequences become even more serious, the potential for chaos and destruction rises.

History

Cybercrime, cyber warfare, and cyber terrorism and its regulation has come to the forefront of recent political debates, but the want and need for increased security on networks has existed ever since the invention of computers. In some ways, the beginning of cyber warfare can be traced to the World Wars, when countries on both sides of the conflict worked to intercept and decode enemy transmissions. At the same time, they were attempting to make their own messages unbreakable. Today, as the world becomes increasingly more reliant on digital systems and cyber networks to facilitate everyday business (from bank transactions to maintaining a city's hospitals to public transportation), the potential fallout from a malicious attack becomes increasingly dangerous.

The field of cyber warfare has roots in the field of information warfare as a way to infiltrate the communication systems and networks of other state actors. But whereas information warfare can only obtain information, the access created in cyberwarfare can lead to much greater harm and damage among both military and civilian targets. Historically, the most valuable and highest impact targets of a possible cyberattack were a state's military assets and, if they possessed them, nuclear arsenals and nuclear power plants. More recently, however, higher priority has been placed on conventional electrical grids, public transport systems, and hospitals as civilians are beginning to be seen as possible targets by state militaries, terrorist cells, and other non state actors.[8]

[5] Sang-hun, Choe. "Computer Networks in South Korea Are Paralyzed in Cyberattacks." The New York Times. March 20, 2013. https://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html.

[6] Mackenzie, Heather. "Shamoon Malware and SCADA Security – What Are the Impacts?" Tofino Industrial Security Solution, October 25, 2012. https://www.tofinosecurity.com/blog/shamoon-malware-and-scada-security-—-what-are-impacts.

[7] Cooper, Helene. "ISIS Is Cited in Hacking of Central Command's Twitter and YouTube Accounts." The New York Times. The New York Times, January 12, 2015. https://www.nytimes.com/2015/01/13/us/isis-is-cited-in-hacking-of-central-commands-twitter-feed.html.

[8] Montgomery, Maxwell. 2019. "Proliferation of Cyberwarfare under International Law: Virtual Attacks with Concrete Consequences." *Southern California Interdisciplinary Law Journal* 28 (2): 499–521.

Actions Taken by the International Community

The closest existing international law regarding cyber warfare between independent state actors is Article 2(4) of the United Nations which states that states "shall refrain from the threat or use of source against the territorial integrity or political independence of any state", which can be interpreted to encompass an act of cyber warfare between two states. However, there currently lacks any concrete legal framework for how the international community should proceed following a cyberattack of serious magnitude.[9] While the international community has yet to develop a comprehensive framework on how to classify or respond to cyber attacks, there are some regional frameworks and specific member states that have cyber security policies that have been put in place in recent years. In 2017, The European Union (EU) introduced a number of recommendations related to the creation of a response plan to major cyber security attacks in the EU. These measures included the development of an EU-wide structure that encomasses every level of actor, from local to supranational, as well as the regular practices to test and train cyber defense networks.[10] The North American Treaty Organization (NATO) also has laid out a basic plan regarding training and responding to possible attacks.[11]

Specific member states such as the United States, South Africa, and the UK have introduced their own national set of cyber security policy in addition to regional efforts. The U.S. created the Cyber Security Act of 2015 which was "arguably the most significant piece of federal cyber-related legislation enacted to date" established "a mechanism for cybersecurity information sharing among private-sector and federal government entities".[12] The UK's policy on national cyber defense works in conjunction with that of the EU with the goal of protecting British citizens and businesses. Many African nations have implemented some government led initiatives, but the majority of the services has been given to third party contractors and corporations to save limited resources.[13]As exhibited above, it is evident that many of these frameworks and policies have been recently developed. The field of cyber security is a new frontier, especially for the international community. The absence of comprehensive response plans and established international networks to deal with cyber attacks makes the efforts of this committee all that more pressing.

Challenges

The UN must find a balance between limits and regulations and respecting the decisions and policies of sovereign countries. In creating these, the UN cannot overstep and limit the right of a member state to self defense and collective defense laid out in Article 51 of the UN charter. It states "Nothing in the present Charter shall impair the inherent right of individual or collective self defense if an armed attack occurs against a Member of the United Nations"[14] Any changes to the Geneva Conventions, the Law of Armed Conflict (LOAC), or any additional documents constructed must be carefully designed as to not interfere in the cyber defense capabilities of member states. Restrictions on implementation, funding of non state actors, and measures to reduce cyber attacks may be more effective at ensuring peace than onerous constraints that will not be followed by influential powers.

[9] Charter of the United Nations Article 2

[10] "Commission Recommendation (EU) 2017/1584." *Official Journal of the European Union* 60 (September 19, 2017): 36–58.

[11] Public Diplomacy Division. (2019) "*NATO Cyber Defense*".

[12] https://www.sullcrom.com/siteFiles/Publications/SC_Publication_The_Cybersecurity_Act_of_2015.pdf

[13] Nir Kshetri (2019) Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management, 22:2, 77-81, DOI: 10.1080/1097198X.2019.1603527

[14] Article 51, Charter of the United Nations and Statute of the International Court of Justice (San Francisco, CA: United Nations, 1945). https://treaties.un.org/doc/publication /ctc/uncharter.pdf.

There are potential conflicts that might arise between member states regarding restrictions on their military and espionage capabilities. The larger nations with a headstart on development and implementation of these kinds of weapons such as the U.S., China, and Russia will likely oppose measures that curtail further developments of deterrence capability. In addition, given the records of member states like Saudi Arabia, the U.S., and Russia, they will likely use funds to finance proxy cyber warfare and terrorism.

Cyber terrorism is a growing fear as many militant groups across the globe turn increasingly radical and incentivised to grow membership and attack various targets. One of the most basic forms of cyber terrorism is the hacking of various media outlets and social media platforms to post propaganda on websites and television stations. These types of attacks are relatively minor in comparison to more drastic attacks; they demonstrate the potential in the future for more dangerous and larger scale attacks. Hacking groups, while not currently listed as terrorist cells or organizations, often carry out attacks on state institutions as non state actors. These hacks often have devastating consequences.

Cybercrime can be linked to criminal actions of both state and non state actors against corporations, government institutions and individuals. Cybercrime has been cited as a reason in many countries that new businesses are struggling to emerge, a specific problem for developing countries in both Africa and South America. This an issue in South Africa where cases of computer fraud and the wiring of bank funds are crippling entrepreneurial efforts due to lack of funding and financial security.[15] Major criminal operations against financial institutions, such as the 2016 attack in India, which compromised 3.2 million accounts, demonstrates how severe and economically disruptive these attacks can be.[16] Cybercrime, cyber terrorism, and cyber warfare are all international concerns that have the ability to affect all UN member states.

Committee Directives

Cyber technology is constantly advancing and developing. Due to this advancement in technology, much of the world of cyberspace is not fully explored by governments and international organizations. Delegates should begin by accurately defining the realm of cyber crime, cyber terrorism, cyber warfare and their differences and relationships. In addition, the delegates should develop policies that help prevent cyber attacks on other governments, businesses and corporations, and individuals. The lack of previous international standards on cyber security creates a unique opportunity to lay the foundation for future resolutions and possible creation of international agencies to deal with this growing problem. The delegates should also work to establish a framework of intergovernmental bodies to coordinate relief efforts and create a contingency plan to respond in the aftermath of cyber attacks.

[15] Herselman, M.; Warren, M. Cyber crime influencing businesses in South Africa. Issues in Informing Science & Information Technology. [s. l.], p. 253, 2004.

[16] Shukla, Saloni, and Pratik Bhakta. “3.2 Million Debit Cards Compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis Worst Hit.” The Economic Times. Economic Times, October 20, 2016. https://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms.