BIGMUN 2023

DISEC

Topic Research Report

Topic: Working towards creating a framework of ethical cyberwarfare

Oscar Sundahl and Anna Meidahl Hommelgaard

Introduction:

With recent advancements in technology and cyberwarfare, it has become apparent that a regulatory scheme for cyberwarfare is required. This research report will explore the history of cyberwarfare, and some of the actors involved in it. With the proliferation of digital computers and the internet, it did not take long for actors to start utilizing these technologies, giving rise to cyberwarfare. When the effectiveness of cyberwarfare was demonstrated with the Stuxnet virus in 2010, many states began to develop their own cyber weapons. With cyberwarfare being a rather new form of warfare, the laws surrounding it are still unclear. Efforts have been made to try to explore how current treaties and international customary law can be applied to cyberwarfare. However, whistleblower disclosures have shown the degree to which states utilize cyberwarfare through mass surveillance programs, causing controversy. Coupled with these disclosures and a leak of the US cyber weapon arsenal which led to the nefarious usage of said weapons against critical infrastructure, many started to realize the potential dangers of unregulated cyberwarfare. With the UN having taken negligible action on the issue, cyberwarfare is the most unregulated form of warfare, with potentially devastating consequences for civilians. Regulating cyberwarfare is still highly contested by many states, as cyberweapons are a cheap, versatile, and effective option for states to influence global politics and the international security environment.

Definition of Key Terms:

Cyberspace — Cyberspace is defined by the Tallinn Guide as being the environment which is formed by both physical and non-physical components to store, change, and send and/or receive data[1].

Cyber Weapons — Cyber weapons are technological means of warfare that are used, designed, or intended to monitor, steal from, damage, kill and/or destroy a target[2].

Cyberwarfare — The usage of cyber weapons in cyberspace for a particular goal.

Customary international law — Customary international law is one of the forms of international law. It is a form of international law which is not formally written down in a treaty but is rather a set of norms which states recognize as being legally binding. For customary international law to be applicable, its two criteria of uniform state practice and opinio juris must be met, where uniform state practice is that states actually apply the norms in question in

[1] Schmitt 2017, 564.
[2] Schmitt 2017, 452.

practice, and opinio juris means that states believe that the laws in question are valid and real, and applicable to them.

Background Information:

With Konrad Zuse's invention of the first digital computer in 1941, the proliferation of digital computing began. While analog computers had previously existed, digital computers were more flexible, making them more suitable for a wide range of tasks[3]. Then, with the advent of ARPANET in 1969, and the development of the TCP/IP protocol (essentially a unified language through which computers communicate with each other) in 1973, the internet was born. With the accessibility brought by the internet, the establishment of internet based businesses and infrastructure began across the world. And with personal computers getting cheaper, our modern internet age began[4].

Cyberwarfare is a rather new form of warfare, having initially been articulated by Chinese researchers in the mid 1990s as a potential new form of espionage. The Chinese military was also the first known state actor to have employed electronic warfare, with an espionage operation against Lockheed Martin, an American defense contractor, being detected in 2003[5]. While at this point cyberwarfare had only been applied in espionage, this however changed in 2007 when Russian cyber attacks disabled Estonian government websites and banks following the suppression of ethnic-Russian riots in Estonia[6]. The first instance of cyber attacks causing physical damage came in 2010, when a joint Israeli-US virus called Stuxnet destroyed Iranian uranium enrichment centrifuges being used in the Iranian nuclear program[7]. With physical damage being inflicted by the Stuxnet attack, some international experts on warfare began to consider cyberwarfare which induces physical damage as being analogous to an armed attack[8]. This notion of cyberattacks which cause physical damage being analogous to an armed attack began also forming into an opinio juris, culminating into NATO adopting a statement stating that a cyberattack could trigger the alliance's mutual defense clause[9].

With the potential capabilities of cyberwarfare being revealed with the Stuxnet attack, states quickly began investing into cyberwarfare. For western nations this meant establishing military run cyber commands. These are military structures which handle both defensive and

[3] Williamson 2021.
[4] Jefferson University 2016.
[5] Stiennon 2015, 9–10.
[6] Stiennon 2015, 17–18.
[7] Stiennon 2015, 20.
[8] Schmitt 2017, 342.
[9] Stiennon 2015, 18.

offensive operations in cyberspace. However, in more openly hostile states this meant decentralization. In states such as Russia, China, and North Korea, this meant the establishment of state-sponsored hacking groups, essentially criminal gangs which enjoy state protection as long as they operate in a manner which is beneficial to the state in question. This decentralized operating structure enables deniability on the part of the state, as it is criminal gangs rather than their intelligence agencies conducting cyberwarfare[10].

Given that cyberwarfare is a relatively new concept, it is not directly regulated by any treaties. There have been attempts at exploring the applicability of previously agreed upon treaties and customary international law to cyberwarfare, culminating in the Tallinn manuals. The Tallinn manuals are a set of academic papers exploring which treaties and parts of customary international law are applicable to cyberwarfare. Many researchers and experts in the cybersecurity field consider the Tallinn manuals to be the guiding principles by which states should be conforming to in regards to cyberwarfare[11].

In 2013, Edward Snowden, a former CIA employee and NSA contractor, exposed the United States intelligence agencies' and their partners' mass surveillance programs, causing uproar amongst civilians and demonstrating how effective cyberwarfare had become in regards to intelligence gathering. The leaks revealed the extent to which cyberwarfare was taking place, and to the efficacy of the cyber weapons in question[12].

However, the risks of cyberwarfare became apparent in 2016, when the NSA got hacked and its cyber weapons leaked to the public. With these cyber weapons in public domain, the exploits which they revealed were quickly reappropriated into new cyber weapons, culminating in amongst other things, the WannaCry ransomware, a type of program which demands money so that you can access the files on your computer[13]. The WannaCry ransomware infected millions of computers, shutting down critical infrastructure, including thousands of hospitals in the United Kingdom[14].

[10] Stiennon 2015, 25–27.
[11] Conca 2018.
[12] Weinstein 2014, 9.
[13] Loleski 2019, 122.
[14] Ghafur et al. 2019.

Major Countries and Organizations Involved:

The United States — The leading actor in cyber weapons and in their development, and wishes to keep its dominance in the cyber field[15].

Israel — A major player in the cybersecurity industry, having both major offensive and defensive capabilities in cyberwarfare. Does not want restrictions on its cybersecurity industry. Utilizes cyberwarfare against Iran with the goal of hindering the Iranian nuclear weapons program[16].

Russia — Has a long history of utilizing cyberwarfare for its own political and military goals. Utilizes both state-sponsored hacking groups and military units for cyberwarfare. Does not want any international restrictions on cyberwarfare[17].

China — Utilizes cyberwarfare for industrial and military espionage and has significant capabilities in cyberwarfare. Does not want restrictions on cyberwarfare.

Iran — Uses cyberweapons mainly against Israel, does not possess any major cyberwarfare capabilities. It utilizes its cyber capabilities for mainly political purposes, and does not want restrictions on cyberwarfare[18].

North Korea — Utilizes cyber warfare to gain foreign currency, and to promote its political goals abroad. Wants to be a major player in cyberwarfare, and does not want any restrictions[19].

Five Eyes — An intelligence alliance between the US, UK, Australia, New Zealand, and Canada. Utilizes surveillance programs in order to advance both political and national security goals. Does not want restrictions on cyberwarfare[20].

[15] Weinstein 2014, 6–7.
[16] Mekelberg 2022.
[17] Cybersecurity & Infrastructure Security Agency 2022.
[18] The Economist 2022.
[19] Young 2022.
[20] Pfluke 2019, 305–9.

Relevant UN Resolutions:

Resolution 2417 (2018) - S/RES/2417(2018) - This resolution relates to the Geneva conventions, it reaffirms and demands protection of innocent civilians in conflict areas. It relates to the humanitarian requirements of the government during conflict[21].

Resolution 56/121(2002) - A/RES/56/121 - 'Combating the criminal misuse of information technologies' - These resolutions sought to encourage cooperation between Member States to combat the criminal misuse of informational technologies[22].

Resolution 58/199 (2004) - A/RES/58/199 - 'Creation of a global culture of cybersecurity and the protection of critical information infrastructures' - This resolution built off of resolutions like 56/121, and sought Member States to determine their own critical information, and develop strategies in reducing risks to critical information infrastructures[23].

Previous Attempts to Solve the Issue:

The main attempts to solve the issue of cyberwarfare are the resolutions 56/121 and 58/199 as mentioned above. Resolution 56/121 aimed to set up regulations to fight against the criminal misuse of technology. Resolution 58/199 aimed to further specify critical information and aimed for Member States to focus on protecting this critical information, as well as improving their cybersecurity. However overall there has been no clear format regarding the rules or regulations for cyberwarfare from the UN. There have been very few attempts to solve the issue aside from the general improvement of cyber security within the UN.

The Tallinn Manual 2.0 was a manual written by the CCDCOE (Cooperative Cyber Defence Centre of Excellence) as well as many experts involved with law, or more specifically cyber law. The Tallinn Manual 2.0 explores existing rules within human rights laws, diplomatic laws, space laws, and telecommunication laws and explores which rules could be applicable in cyberspace, or cyberoperations. Most of the rules focus on the connection between cyberoperations and the use of force. This manual was very effective in outlining rules and regulations, however many states seem to be unsure in regards to legal certainty in cyberspace[24].

[21] United Nations Security Council 2018.
[22] United Nations General Assembly 2002.
[23] United Nations General Assembly 2004.
[24] Efrony and Shany 2018.

Possible Solutions:

The aim of the discussions should be regarding creating a framework for cyber warfare, defining what type of cyberwarfare is considered unethical, and laying out regulations for cyber warfare.

A viewpoint for this topic, could consider if cyberwarfare is ethical, if the definition of cyberwarfare only causes unethical harm on the innocent civilians. Especially in connection to the Geneva conventions and the countless resolutions regarding civilian safety within war zones. This viewpoint would focus on the idea of cyber warfare.

Another viewpoint could be, that there have been no clear violent attacks of cyberwarfare and therefore creating an ethical framework is unnecessary since cyberwarfare is barely used. This viewpoint would consider cyberwarfare to be of very little danger, and therefore pose no threat. This viewpoint would focus on how little cyberwarfare has been used.

A final viewpoint could consider the impact that modern technology has on a society and the likely grave impact that cyberwarfare would have, mainly on the innocent civilians, in the future. This also relates to the Geneva conventions and resolutions as this viewpoint prioritizes citizen safety. This viewpoint would focus on civilian safety in cyber warfare, especially in regard to critical information gathered online by the individual Member States.

Bibliography

Conca, James. 2018. “When Would Russia’s Cyber Warfare Morph Into Real Warfare? Refer To The Tallinn Manual.” *Forbes*, August 9, sec. Energy. At https://www.forbes.com/sites/jamesconca/2018/08/09/when-would-russias-cyber-warfare-morph-into-real-warfare-refer-to-the-tallinn-manual/, accessed January 6, 2023.

Cybersecurity & Infrastructure Security Agency. 2022. “Russia Cyber Threat Overview and Advisories.” At https://www.cisa.gov/uscert/russia, accessed January 7, 2023.

Efrony, Dan, and Yuval Shany. 2018. “A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice.” *American Journal of International Law* 112, no. 4: 583–657.

Ghafur, S., S. Kristensen, K. Honeyford, G. Martin, A. Darzi, and P. Aylin. 2019. “A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS.” *Npj Digital Medicine* 2, no. 1: 98.

Jefferson University. 2016. “An Internet History Timeline: From the 1960s to Now.” *Jefferson Online*. At https://online.jefferson.edu/business/internet-history-timeline/, accessed January 6, 2023.

Loleski, Steven. 2019. “From Cold to Cyber Warriors: The Origins and Expansion of NSA’s

Tailored Access Operations (TAO) to Shadow Brokers." *Intelligence and National Security* 34, no. 1: 112–28.
Mekelberg, Yossi. 2022. "Cyberwarfare Brings New Element to Israel-Iran Confrontation." *Arab News*. At https://arab.news/2cyna, accessed January 6, 2023.
Pfluke, Corey. 2019. "A History of the Five Eyes Alliance: Possibility for Reform and Additions: A History of the Five Eyes Alliance: Possibility for Reform and Additions." *Comparative Strategy* 38, no. 4: 302–15.
Schmitt, Michael N., ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed Cambridge University Press. At https://www.cambridge.org/core/product/identifier/9781316822524/type/book, accessed January 6, 2023.
Stiennon, Richard. 2015. "A Short History of Cyber Warfare." *Cyber Warfare: A Multidisciplinary Analysis*, 1st ed. Routledge. At https://www.taylorfrancis.com/books/9781317645566, accessed January 6, 2023.
The Economist. 2022. "Iran's Cyberwar Goes Global." *The Economist*, September 17. At https://www.economist.com/middle-east-and-africa/2022/09/14/irans-cyberwar-goes-global, accessed January 7, 2023.
United Nations General Assembly. 2002. "Resolution 56/121 Combating the Criminal Misuse of Information Technologies." United Nations. At https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf, accessed January 4, 2023.
———. 2004. "Resolution 58/199 Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures." United Nations. At https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf, accessed January 4, 2023.
United Nations Security Council. 2018. "Resolution 2417 (2018)." United Nations. At https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/159/35/PDF/N1815935.pdf?OpenElement, accessed January 4, 2023.
Weinstein, Dave. 2014. "Snowden and U.S. Cyber Power." *Georgetown Journal of International Affairs* Georgetown University Press: 4–11.
Williamson, Timothy. 2021. "History of Computers: A Brief Timeline." *Livescience.Com*. At https://www.livescience.com/20718-computer-history.html, accessed January 6, 2023.
Young, Benjamin R. 2022. "North Korea Knows How Important Its Cyberattacks Are." *Foreign Policy*. At https://foreignpolicy.com/2022/02/09/north-korea-knows-how-important-its-cyberattacks-are/, accessed January 6, 2023.