

GROWING THREAT OF CYBER ESPIONAGE AND RELATED LAW

Manali Dhanawade
Digital Forensic Analyst
Pelorus Technologies Pvt Ltd.
manalidhanawade2193@gmail.com

ABSTRACT:

Espionage among nations is not a new phenomenon; it has existed since the early medieval period. The world of spies has evolved with the times, a new type of intelligence gathering capability with various strategies, tactics and tools. This new form of intelligence gathering and deliberate threat uses cyber warfare techniques to gain economic, military, or political benefits. Highly skilled cybercriminals are recruited to damage or shut down government or military infrastructures, or to gain unauthorized access to financial systems. If this is carried out from within the territory of a State, prosecution will take place under domestic law. However, when trade secrets are stolen other than its own state, arbitration becomes more complex and the proper arbitration mechanism may be difficult to establish.

The growing threat economic cyber espionage has a great impact to national security. State-based threat actor teams are comprised of computer programmers, engineers, and scientists that form military and intelligence agency hacking clusters. They have tremendous financial backing and unlimited technological resources that help them evolve their techniques rapidly. International law needs to stay ahead of due to unfair trade practices is added up the curve to abate damages from unfair practices conducted in cyberspace.

This paper illustrates the study of countries affected by Cyber Espionage, its impact on these countries and a brief study of their laws safeguarding them. This paper also deals with the countries from where these cyber-attacks originates from, and an analysis of the laws being imposed on both the scenarios and the challenges faced by the countries and participation of them on an international norms for a uniform cyber security laws all over the world.

I. INTRODUCTION

Espionage is the act of acquiring trade secrets, intelligence and military secrets without the permission of the owner of the information and is hence illegal. Espionage is different from intelligence gathering. In intelligence gathering information is collected through legal and ethical means. Addressing the theft and transfer of trade secrets overseas for innovative technology is a priority focus of the Office of the U.S. Intellectual Property Enforcement (White House, 2013) Espionage is the act of acquiring trade secrets, intelligence and military secrets without the permission of the owner of the information and is hence illegal. Espionage is different from intelligence gathering. In intelligence gathering, information is collected through legal and ethical means. Addressing the theft and transfer of trade secrets overseas for innovative technology is a priority focus of the Office of the U.S. Intellectual Property Enforcement (White House, 2013) Espionage is the act of acquiring trade secrets, intelligence and military secrets without the permission of the owner of the information and is hence illegal. Espionage is different from intelligence gathering.

For hundreds of years, physical attacks by countries have been treated as unacceptable, and hence as reasonable pretext for a forceful response. Extending this principle, the United Nations Group of Governmental Experts declared in 2013 that existing international law (originally developed for conventional combat) also applies in cyberspace (United Nations 2013). Conversely, espionage by countries has been treated as acceptable state behavior, hence not a reasonable pretext. This understanding has been carried over into cyberspace. Every year, various companies lose billions of dollars due to industrial espionage activities from foreign and domestic competitors (America, FBI, 2014). The cost of industrial espionage and Intellectual Property Theft in UK was estimated to be annually £9.6

billion and £7.6 billion respectively from external cyber-attacks, which represents about 62% of costs of all cybercrimes, according to a study released by the Office of Cyber Security and Information Assurance in UK (Cabinet Office, 2011). Thus, a thorough understanding of what factors may potentially decrease the costs from these types of crime are not only warranted but are crucial.

Responsible nations may carry out cyber espionage (violating a system's confidentiality), but they may not carry out cyber attacks (operations that violate a system's integrity or availability). In recent years, the United States, together with like-minded countries, has indicated that it does not feel that all cyber espionage is acceptable state behavior. It has complained about Chinese industrial cyber espionage since early 2010, winning a presidential-level agreement from China to ban such a practice (White House 2015b). It was considering declaring unacceptable the transfer of personally identifiable information harvested from the US Office of Personnel Management (OPM) hack into cybercrime markets (the issue had never been raised because there was scant evidence of any such Cyber espionage involves deliberate activities to penetrate computer systems or networks used by an adversary for obtaining information resident on or transiting through these systems or networks. An economic espionage, where a state attempts to acquire secrets held by foreign companies. Earlier the States conducted economic espionage before the Internet, but the availability of new trading technologies, cyber exploitation rapidly and significantly expanded the activity.

II. THE STRATEGIC THREAT OF CYBER ECONOMIC ESPIONAGE

Cyberspace remains a operational domain for a of industrial espionage threat actors, from adversarial nation- states, to commercial enterprises operating under state influence, to sponsored activities conducted by proxy hacker groups. Next-generation technologies such as Artificial Intelligence (AI) and the Internet-of-Things (IoT) will introduce new vulnerabilities to various nation's networks for which the cybersecurity community remains largely unprepared. The United States remains a global center for research, development, and innovation across multiple high- technology sectors. Federal research institutions, universities and

corporations are regularly targeted by online threat actors seeking all manner of sensitive information and the overall trend remains worrisome. While next generation technologies will introduce a range of qualitative advances in data storage, analytics, and computational capacity, they also present potential vulnerabilities for which the cybersecurity community remains largely unprepared. The solidification of cloud computing over the past decade as a global information industry standard, coupled with the deployment of technologies such as AI and IoT, will introduce unforeseen vulnerabilities to U.S. networks.

Rapid Expansion of global online operational space with Cloud networks and IoT infrastructure.

Threat actors have already performed how cloud can be used as a platform for cyber exploitation. As IoT and AI applications can expand to empower everything from —smart homes to —smart cities, billions of potentially unsecured network nodes will create an incalculably larger exploitation space for cyber threat actors.

Understanding economic espionage as a worldwide, multi-vector threat to the integrity of both the nation and global trade. Cyberspace is a most preferred domain for economic espionage, Sophisticated threat actors, such as adversarial nation-states, combine cyber exploitation with supply chain operations, human recruitment, and the acquisition of knowledge by foreign students in universities, as part of a strategic technology acquisition program.

Governments and their various agents have been exploiting Internet networks by penetrating the electronic networks of foreign companies for nearly a quarter-century. Until 2010, companies chose to ignore the problem, more or less. Then Google publicly claimed that China had stolen source code and used it to spy and to penetrate other companies' networks. At during the meantime, major economic espionage was carried out against large western oil companies and had been traced to a site in China, and another theft lifted security key tokens, which led to the penetration of other firms, including defense contractors in the United States.

In May of 2014, the FBI issued —Most Wanted posters for five Chinese nationals, members of the Peoples' Liberation Army. 9 In *United States v. Wang*, the five were indicted by a federal grand jury for breaking into computer systems

of American companies and stealing trade secrets for the benefit of Chinese companies.⁰ Although there was no chance that the United States would obtain jurisdiction over the accused so that they could be tried, the indictments may have been intended to incentivize negotiations with the Chinese on corporate spying. At first, the Chinese responded by complaining about U.S. hypocrisy and double standards. ¹¹ The Chinese asserted that American authorities have conducted large-scale, organized cyber-espionage activities against government officials, companies, and individuals, in China and many other states. The distinction that our government draws between spying for national security purposes and not spying on companies to give a competitive edge to one's own businesses is not recognized as valid by China, and they pointed out the definition of national security includes obtaining advantages in trade negotiations and for other international economic purposes, including enforcing sanctions regimes and detecting bribery.

Then, in 2015, some seemingly remarkable things happened. Following the indictment of the Chinese hackers and an executive order promulgated by President Barack Obama that authorized sanctions against malicious hackers, the United States and China reached an agreement on a range of cybersecurity matters. In addition to cooperation on law enforcement matters in cyberspace, China reversed its prominent policy committed not to involve in commercially-motivated cyber espionage. The agreement included implementation and compliance provisions, the violation of which could lead to sanctions under the Obama administration executive order. As weeks passed after the U.S.–China agreement was reached, similar agreements were reached between China and the United Kingdom and China and Germany.

III. THREATS FROM THE COUNTRIES

1. U.S. — the superpower hacker

Stacking it up: Capabilities "surpass anything known in terms of complexity and sophistication of techniques," the WSJ writes. One hack to know: Stuxnet, a computer worm that the U.S. allegedly jointly launched with Israel in 2010 to derail an Iranian nuclear facility. Read more via the NYT.

Cyber capabilities in the government: The WannaCry attack that spread to hundreds of countries this May actually originated from a leak or theft via the U.S. National Security Agency (to be clear, the NSA didn't perpetrate the attack). The leader of NSA, Adm. Michael Rogers, is also the leader of the Pentagon's cyber ops arm, Cyber Command, which last December was made into its own cyber fighting unit.

Rogers has said the lawmakers he wanted to build out "offensive cyber capabilities."

2. U.K. — the watchful hacker

Stacking it up: The U.K. is known as host to "one of the world's pre-eminent eavesdropping agencies," known as GCHQ Reuters writes.

One hack to know: British spies allegedly hacked into the world's largest sim card manufacturer, Gemalto, along with American NSA spies in 2012 to monitor voice calls and data-use for billions of cell phones around the world. Cyber capabilities in the government: The British government has acknowledged British spies are developing cyber offensive capabilities in GCHQ and the Ministry of Defence as part of the National Offensive Cyber Programme. Read more on that via Wired.

3. Russia — the political hacker

Russia has appear to hack for political reasons; to serve or harm political candidates, to prop up Russian interests, or to more generally sow doubt around the world in democratic governance. These objectives were seen in the 2016 DNC hack, and the use of bots to spread fake news.

Another hack to know: The 2015 attack linked to Russia shut down electricity for about a quarter-million Ukrainians. Experts are saying Russia may be using Ukraine as a testing ground for other, devastating attacks yet to come

4. China — the economic hacker

Stacking it up: China is known for its industrial espionage efforts, and has allegedly been stealing intellectual property for years.

Two hacks to know: 1. The Chinese military allegedly stole F-35 fighter jet plans from the U.S., which some say allowed Beijing to create the J-31 fighter jet. China denies this. 2. The hack into the U.S. Office of Personnel Management, which has been blamed on China, saw the records of up to 21.5 million U.S. government employees and consultants dating back 50 years stolen.

Cyber capabilities in the government: Beijing has admitted it has explicit units in its government dedicated to "cybercrime", per The Daily Beast.

5. The Israel-Iran match — the geopolitical hacking matchup

Stacking it up: Israel is "among world's most advanced" cyberspying agencies, per the WSJ. Iran is most well known for attacks it allegedly launches in response to perceived geopolitical threats. Read more via the Chicago Tribune.

Top hacks to know: Israel allegedly launched the 2010 Stuxnet hack along with the U.S. to derail an Iranian nuclear facility (read above). Just last year, the U.S. Department of Justice indicted hackers with links to the Iranian government for attacking U.S. banks and a dam in New York.

Cyber capabilities in the government: Unit 8200 of the Israeli Defense Forces is often equated to the NSA, with objectives including signals intelligence, offensive cyber strategy, cybersecurity, and encryption, per the Miami Herald and having thousands of personnel, per Forbes estimates. In 2015 the government announced a new defensive cyber unit to work alongside the government's National Cyber Bureau. Iran's Cyber Defense Command has a defensive mission, per The Institute for National Security Studies (INSS) , which assesses that Iran's Revolutionary Guard plays an offensive role. to handle both attacks and defense. In 2014 a federal grand jury indicted five people from PLA Unit 61398, China's allegedly 100,000 strong military cyber espionage division, for stealing trade secrets from U.S. companies.

IV. LATEST CYBER ESPIONAGE CASES

The listed cyber-espionage incidents will make you believe in the colossal capabilities of cybercriminals.

1. Renewed Cyber Attacks in 2019 from Chinese and Iranian Hackers on US Agencies

It's been recently revealed that Chinese and Iranian hackers are aggressively attacking the government agencies and businesses of the United States. Cybersecurity experts believe that these attacks are a result of Trump's withdrawal from Iran nuclear deal and the trade war with China. In January 2019 the US intelligence chiefs reported that China, Iran, North Korea, and Russia are the main cyber adversaries of the nation. These countries are linked with the cyber-espionage activities like stealing information to influence the citizens and/or to derange the critical infrastructure in the United States. The report clearly mentions the objective of the Iranian hackers, —to gain intelligence and position themselves for future cyber operations.

2. Pakistan's Foreign Affairs Ministry website Hacked Post-Pulwama Attack

Pakistan's Dawn reported in February 2019 that the website of the nation's Ministry of External Affairs has been hacked and various countries mentioned that the website is inaccessible to them. The website seems to be functioning in Pakistan but visitors from other countries like Holland, Australia, Britain, and Saudi Arabia are facing issues while opening it. The report also mentions that these cyberattacks could be originated from India. This is said to be the result of the terrorist strike in Pulwama, Kashmir, which occurred on February 14, 2019. This is not the first time Pakistan is facing such an issue. Earlier in 2017, Pakistan Peoples Party's official website was said to be defaced by Indian hackers. In the same year, another official website, this time belonging to Karachi Police, was hacked and defaced presumably by Indian hackers.

3. Kaspersky's —Slingshot Report 2018

Kaspersky Lab in 2018 exposed the presence of a then-active advanced APT (advanced persistent threats) actor. The malicious loader internally named

as—Slingshot,¹¹ because of the names of the threat actor's unencrypted samples and components. Most victims of the group were individuals and not organizations. The victims of —Slingshot¹¹ belonged to African and Middle Eastern nations. As per Kaspersky's researchers, the first compilation of the attack dates back to 2012. The primary objective of —Slingshot¹¹ was to collect screenshots, keyboard data, network data, passwords, USB connections, other desktop activity, clipboard, and more, which links it to the cyber-espionage pattern. Later, former US intelligence officials came forward to accept that Slingshot is a US military program to gain access to terrorists' commonly used computers

4. Chinese Hacker Group's Cyber- Espionage Campaign

Symantec revealed in June 2018 that a group of Chinese-linked hackers was targeting two United States--based satellite firms. Other than that, the sophisticated hacking group also targeted defense contractors and telecommunications companies in the United States and Southeast Asia. The efforts of the group were believed to be carried out in the interest of the nation. The primary drive for this cyber-espionage campaign was to intercept the military and civilian communications of the victim nations. Hacking with the purpose to intercept is rare but it exists. But in this case, the hacking group deliberately infected the systems controlling the satellites. The motive of their act was to change the positions of the orbiting devices and disrupt data traffic.

The group activated itself in 2013 but after the political agreement between the United States and the Chinese government in 2015, it apparently went underground. Symantec has attributed this cyber-espionage group as —Thrip¹²

5. A Leaked Trump–Duterte Transcript Proving Cyber-Espionage Story 2017

A stolen transcript of a phone conversation between the US President, Donald Trump, and his Philippine counterpart, Rodrigo Duterte, was first uploaded on the Internet through malicious email attachments. These sensitive documents were obtained by a hacker group which was allegedly linked to the Vietnamese government. The documents were hacked from the Philippine government's surveillance. The leak seemed bigger than the revelations of just a few

documents. Cybersecurity investigators soon found that the attack was carried out by a malicious hacker group called APT32 (also known by the name of OceanLotus Group). As per various cybersecurity firms, APT32 is an attributed unit of the Vietnamese government.

Amy Chang, an affiliate of the Harvard Belfer Center's Cyber Security Project, believes that the rise of Duterte in the Philippines is the reason behind the leaked transcript

6. Intensive Cyber-Espionage Campaign of APT28

Against Montenegro's Government Before Montenegro joined NATO in 2017, APT28 (also popularly known as Fanc Bear), a malicious hacking group linked to the Russian intelligence, actively participated in a cyber-espionage campaign against the Montenegrin government. The campaign depicts Russia's desire to intrude in the political affairs of foreign nations. Two booby-trapped attachments had been sent to Montenegrin government officials over the email to load a flash exploit framework through a command-and-control infrastructure.

Other than this campaign, earlier in 2016, the group was also involved in hacking into the Democratic National Committee. Vietnamese Campaign Against ASEAN 2017

An APT group, APT32 (also known as OceanLotus Group), allegedly linked to the Vietnamese government, started attacking the Association of Southeast Asian Nations (ASEAN) as part of its cyber-espionage campaign. The incident response firm Volexity, in 2017, identified and uncovered the widespread mass digital surveillance and the attack campaign of the group. It also targeted the media, human rights, and civil society organizations.

The group conducted the attacks through multiple strategically compromised websites of government, military, media, civil society, human rights, and oil exploitation firms. The attacks were surgical in nature as it targeted only whitelisted visitors of these websites, who were shown a fake screen to gain control of their contacts and emails.

According to cyber security experts, the APT32 group started its activities in 2012 or perhaps even before that. It is known as one of the most advanced APT groups because of its rapidly evolving capabilities.

V. CYBER ESPIONAGE AND INTERNATIONAL HUMAN RIGHTS LAW

Edward Snowden's disclosures revealed that, in addition to conducting cyber espionage against other states, the United States (US) National Security Agency (NSA) had been collecting confidential information belonging to individuals from across the globe. Individuals were targeted on the basis that they were suspected of being involved in terrorist-related activities as well as other criminal enterprises such as drug and people trafficking. As we shall see, however, the surveillance methods employed by the NSA were so pervasive that they invariably resulted in the collection of confidential information belonging to non-suspects (for want of a better word). While International Law is primarily concerned with the regulation of state relations, this regime has come to recognize the prominent role that non state actors play within the international society and has thus endowed them with certain rights and responsibilities. Most notably, through the implementation of treaties and the incremental development of state practice, a sophisticated international legal framework has emerged that imposes conventional and customary obligations upon states to respect fundamental human rights.

The objective of this chapter is to examine whether cyber espionage targeted against individuals violated international human rights law. Space limitations preclude an assessment of how all international human rights regimes apply to cyber espionage. Instead, this chapter focuses upon the International Covenant on Civil and Political Right (ICCPR) 1966 and the European Convention on Human Rights (ECHR) 1950. The ICCPR is prioritized for international legal analysis because it is widely ratified and, moreover, many of its provisions are considered to be reflective of customary international law (including, most importantly, the right to privacy). The ECHR is singled out for assessment because on multiple occasions the European Court of Human Rights (ECHR) – the international court

entrusted with interpreting and applying the ECHR – has examined how online surveillance impacts upon human rights and the Court has therefore generated a rich and interesting jurisprudence on this topic.

The economic cyber espionage confronts a lack of international law on espionage and economic espionage. Although a victim country could assert that spying violates the principles of sovereignty and non- intervention, state practice has accepted state-sponsored espionage such that these appeals are not serious claims. Although cyber espionage is sometimes considered as "cyber attacks" and "cyberwar," no government regards cyber espionage as a prohibited use of force. Other bodies of international law under which espionage issues arise do not prohibit or seriously constrain espionage or economic espionage.

Thus, participation in, and tolerance of, spying indicates that espionage is not considered wrongful acts triggering state responsibility under international law. Persons accused of being spies can be punished, but international law contains protections for spies captured during armed conflict or covered by diplomatic immunity.

VI. International Law, Criminal Law Enforcement Cooperation, and Economic Espionage

Many countries prohibit economic espionage under national law. However, enforcement confronts difficulties because the elements include foreign government participation.. The U.S.-China mutual legal assistance treaty is unlikely to be helpful to U.S. efforts to apply the EEA to perpetrators of economic cyber espionage linked to the Chinese government.

International Law, Protection of Intellectual Property and Trade Secrets

Some experts have argued that the United States should use international trade law's protections for intellectual property against countries engaged in economic cyber espionage. In trade and investment agreements, states have used international law to protect intellectual property rights of private-sector enterprises. The Agreement on Trade- Related Aspects of Intellectual Property Rights (TRIPS) of the World Trade Organization (WTO) requires each WTO

member to protect certain types of intellectual property rights, including trade secrets, within its territory.

However, WTO members have, shown no interest in addressing economic espionage within the WTO despite mounting worries about this practice. However, the economic espionage especially acts of remotely conducted economic cyber espionage involves governments obtaining information from private-sector companies located outside their territories.

Another strategic proposed by experts is for the United States to impose trade sanctions on countries involved in economic cyber espionage and justify the sanctions under national security exceptions in WTO agreements. This approach admits that unilateral trade sanctions would violate WTO obligations and require an exception to justify them. Whether a WTO members invocation of a national security exception could be successfully challenged remains controversial.

Other proposals focus on U.S. law rather than international law. For example, experts have argued that the United States should (1) impose sanctions on foreign nationals and companies that engage in, or benefit from, economic espionage, and (2) permit civil claims in

U.S. courts against foreign governments that steal U.S. trade secrets under the Foreign Sovereign Immunities Act.. These proposals borrow from other contexts, such as countering terrorism and transnational crime.

Application Of Existing International Laws In Cyberwarfare

As per the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security's recommendation, the UN Charter and International Humanitarian Law are the only international laws relevant to cyberspace. Release of Tallinn manual on applicability of these laws to cyberspace has further aided focus on cyber war. It is a study on how existing international laws apply on cyberspace and cyberwarfare. It is characteristically academic and non-binding.

3.1. Use of Force and Right to Self Defence

The UN Charter contains provisions relevant to conflicts in cyber space. Article 1 of the Charter provides for maintenance of international peace and security, Article 2(4) for restraint on use of force. Article 51 protects

the —inherent‖ right to self defence. Article 2(4) of the Charter states that —[All] members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.‖ The term —force‖ was kept ambiguous at the time of drafting Charter. International Court of Justice has stated that under the UN Charter, Article 2(4) and Article 51 apply to —any use of force, regardless of the weapons employed‖. This statement is accurate reflection of international customary law. Conventional weapons are classified and regulated on the grounds of their capabilities of destruction, killings and sufferings. Malwares, on the other hand, do not demonstrably kill. Destruction of properties by it is generally below the threshold of aggressive action. Tallinn Manual states not all cyber operations can be classified as —force‖ by giving example of instances concerning —non- destructive cyber psychological operations intended solely to undermine confidence in a government or economy.‖ The only cyber operations classifiable as —use of force‖ are those which are conducted or otherwise attributable to State and rise to the level equivalent to an —armed attack‖ in terms of scale and effects.

The complication in this framework is that a large number of strategic cyber operations might get away with impunity. Damage to life and property during cyber warfare is largely low in comparison to war waged with conventional weapons. Blood and human dignity are better preserved in the former case. It must be noted that the purpose of both wars differ. While one is aimed to cause destruction of life and property, another executes disorder targeting the CIA triad (Confidentiality, Integrity and Availability). Because of the distinction in their ends, laws must not be equally applied in both cases. Unequal stances ought to be treated unequally. It is submitted that what constitutes use of force in the cyberspace must be evaluated not on the grounds of whether it constitutes —armed force‖ or not (as Tallinn Manual states), but in accordance with the proportional damage that it has caused to the information CIA triad and networking capacities of the system. Until the international legal framework develops a new model to deal strictly with the cyberspace, the existing laws can be used. But they cannot be applied without the mentioned discrimination. It is necessary to pay attention to what is the Potential of Damage (PoD), that is the vastness and sensitivity of information or crucial character of the particular

network of the targeted ecosystem. Consider a State (let's say State A) against which a ferocious cyber attack is done. 90% of its sensitive data is stored in and networking is completely through cyberspace; the State however did not suffer serious complications. Another State (let's say State B) has relatively less cyber networking ecosystem but suffered losses in considerable percentage of the networking system. Now if we consider both the cases we will rightly observe that State A had a greater PoD than State B, although the latter suffered losses.

Sovereignty

Sovereignty, in other words, can be understood as encompassing —the whole body of rights and attributes which a state possesses in its territory, to the exclusion of all other states, and also in its relation with other states.‖

Article 2(1) of the UN Charter states that

—the [UN] organization is based on the principle of the sovereign equality of all its Members.‖

In different domains, the principle of sovereignty is unequally applicable. For example, airspace over a territory is strictly supervised and any unsought intrusion is considered as violation of international law. In reference to seas, on the other hand, transit through territorial sea of another state is permissible, but can constitute international law violation under certain conditions. In the case of space, objects in orbit and outer space (including above another State's territory) are beyond nation's territorial claim and can be exploited by all. But how sovereignty can be determined in cyberspace is a question faced by us. Unlike land, air, water and space, cyberspace is not a natural domain. It is a man's creation interlinking devices and data, suspended on servers and networking suspensions. Attempts were made prior to Tallinn Manual to deal with sovereignty in cyberspace. The challenge, earlier, however, was not to check legality of whether State could violate another State's sovereignty by unaccepted intrusion, but to identify when cyber operations could do so. It was a preliminary step. In view of Tallinn Manual, no State can claim sovereignty over cyberspace per se, but only on cyber infrastructure located on its territory. Regarding the consequences of such sovereignty, it states:

—First, that cyber infrastructure is subject to legal and regulatory control by the State. Second, the State's territorial sovereignty protects such cyber infrastructure. It does not matter whether it belongs to the government or to private entities or individuals, nor do the purposes it serves matter.¶

The view propounded in Tallinn Manual is correct and practicable. Cyberspace is an artificial domain. It is an abstract domain existing in servers and infrastructure which need to be located at certain lands, seas, air or space. We cannot establish exclusive control over this domain of a State because the data and networking essentials are ultimately grounded at fixed and concrete domain which can be either of the four domains (air, land, water and space). If a cyber attack is launched against a State, it means operations have been carried out with an intention to conduct hostilities on the State's websites, data and networking tools. All these targets are rooted and arise from particular technical infrastructures. These infrastructures are located in State's territories. Henceforth, if an attack is done in the State's cyberspace, it equals attack on State's sovereignty. If a State intrudes another State's cyberspace and coerces its government by using cyber tools, it might constitute intervention if such coercion is not otherwise permitted under the applicable provisions of international law.

VII. CONCLUSION

The general concepts relevant to legal development of cyberspace have been discussed. The international community is yet to arrive at common definitions on the subject. Although the nature of this domain is characteristically different from the other domains of land, water, air and space, highly influential accounts and opinions prevail as to how we can apply existing international laws to the new realm. Provisions relating to prohibition on use of force, self defence, armed conflict and humanitarian protection have been interpreted to engulf analogies found in cyberspace. Although voluminous content is available, no authoritative and binding conventions are formulated.

However, one major problem with the case of cyber realm's legal exposition is that the outlooks on policy are shared majorly by the States' militaries. Many influential researches on cyber domain and what regulations can undertake it are brainchild of army think tanks. This is problematic. It is because the militaries

work on subjects with viewpoint of war and strategies to establish dominance and superiority. It extensively ignores the civil life concerned with the subject. The more exclusive focus is paid on cyber wars, more cyber wars might occur.

Cyber espionage was found to differ from conventional espionage, not in its essence, but in its mode of action and field of operation. From the perpetrator's point of view, a significant advantage of cyber espionage is that it is geographically independent, but this simultaneously raises questions related to the legality of its intrusions upon other states' data. However, before a conclusion could be drawn on the putative legality or illegality of cyber espionage, it was concluded that only specific activities related to espionage, but not espionage as such, are prohibited under international law. When addressing the question if cyber espionage could constitute an intrusion into the sovereignty of another state, it was found that for this to be the case, the sovereign territory of states must include also the virtual space through which cyber espionage is conducted. Under the provision that the data intruded upon are physically stored on servers located within the target state, the targeted state has sovereignty and territorial jurisdiction over the data present on those servers. Cyber espionage has bearings on several principles and aspects of international law. In legal discussions on cyber intrusions a commonly mentioned principle is the prohibition of use of force according to Art 2(4) of the UN Charter. However, it was concluded that espionage falls below the threshold of prohibited use of force. This is due to the fact that although cyber espionage might lead to consequences that include elements of (armed) force, it neither inherently nor in essence does so. Furthermore, Art 2(4) is an effects-based prohibition, which is in contrast to the aim of cyber espionage to operate covertly. Since cyber espionage fails to reach the threshold of prohibited use of force, it is relevant to examine whether it is unlawful under the principle of non- intervention. The word intervention can be interpreted strictly, leading to prohibition only of interference that is coercive or dictatorial. However, through the analogous application of caselaw, doctrine and conventions it was found that cyber espionage can indeed be unlawful in that it involves an intrusion into the jurisdiction and sovereignty of the targeted state. A wider interpretation of the principle of non-intervention, where less weight is put on the coerciveness of the purported interference, but more on interference in internal matters of the targeted state, also leads to the conclusion that cyber espionage is unlawful under international law.

Therefore, the answer to whether extraterritorial cyber intrusions through cyberspace by a state into protected data located and belonging to another state, referred to as cyber espionage, can constitute unlawful intrusion under international law into the sovereignty of the state intruded upon, is yes.

VIII. REFERENCES

1. Foreign Economic Espionage in Cyberspace: NATIONAL COUNTER INTELLIGENCE AND SECURITY CENTER
2. Economic Community of West African States
3. Economic Cyber Espionage: The Need for an Amalgamation of WTO Rules and International Law : Mary Elizabeth Lahiff University for Peace
4. THE LAW OF CYBER-ATTACK: Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel
5. International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene
6. International and Foreign Cyberspace Law Research Guide
7. <https://online.norwich.edu/academic-programs/masters/information-security-assurance/resources/infographics/how-nations-use-digital-espionage-against-each-other>
8. <https://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving>
9. <http://guides.ll.georgetown.edu/cyberspace> <http://guides.ll.georgetown.edu/c.php?g=363530&p=4821480>
10. <https://www.michalsons.com/focus-areas/cybercrime-law>
11. <http://theconversation.com/global/topics/cyber-warfare-7023>
12. <http://web.mit.edu/smadnick/www/wp/2017-10.pdf>
13. <https://ccdcoe.org/uploads/2018/10/Art-01-The-Coming-of-Cyber-Espionage-Norms.pdf>
14. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf
15. <http://cyberlaws.net/cyber-laws-different-countries/>
16. <https://www.visualcapitalist.com/countries-least-prepared-cyber-attacks/>