CHINA'S CYBER DOMINANCE OVER INFORMATION SECURITY: A CASE STUDY OF AUSTRALIA

H.R.L Perera*
Department of Social Sciences, Sabaragamuwa University of Sri Lanka

Abstract

Offensive cyber operations had become a recent interesting phenomenon world over. Cyber-attacks have been used by various stakeholders around the world to obtain their preferred outcomes. Among the Cyber giants in the world China has become one of the main cyber powers in the world. Some of Their cyber activities has a direct link with their political intensions. This research paper will be looking at whether China has become a threat to the information security of Australia. For this particular research I have used Secondary data. The analysis has been done through materials such as research papers, online publications, dissertations and YouTube interviews etc. Content Analysis method has been used to analysis the qualitative data. According to the conclusion of the research is that China has become kind of a threat to the information security of Australia. Where the critical and sensitive information has been stolen by the cyber activists of related to China. Furthermore, there were new security dilemmas has been formulated because of these cyber-attacks.

Keywords: *Australia, China, Cyber-attacks, Cyber Power, Information Security.*

**Corresponding author: Tel: +94*763232868*; Email: ruchira.lahiru21@ gmail.com*

Introduction

Cyber Technology has become one of the most interesting topics worlds over. Initially it was used for the enhancement of Information Technology and to make human life more convenient. However later on cyber-Technology has been used for aggressive measurements. Therefor cyber security has become one of the main branches under the study field of security. Intensive growth of cyber actions such as hacking and cyber-attacks has prompted a threat to national as well as international security. Considering Cyber-attacks various stakeholders conduct cyber-attacks for various reasons. (Kremling & Parker, 2018). It can be a hacker who wants to achieve personal outcomes or it can be an organization willing to conduct attacks against their competitors. Otherwise, it can be a nation-state who are conducting cyber-attacks against other political actors to gain their political outcomes. If a nation state conducts a cyber-attack against another nation state or international organization, we identify such activities as cyber warfare. .(Kremling & Parker, 2018) Because those attacks directly has a political intension and those are politically motivated. Cyber Power has become one of modern mode of influencing other than the hard power and soft power. (Nye, 2014). We also identify them as state sponsored cyber-attacks when there is a clear involvement of a nation state. Today world over there are many nation states which has been identified as cyber giants such as USA, China, Russia, Israel and North Korea. Where they have great cyber capabilities to influence other stakeholders around the world. In this particular research I will be focusing on Chinese aggressive cyber activities conducted against Australia to bring about a threat to the information security of Australia. There are various ways that we can classify cyber-attacks those are sabotage, espionage, propaganda attacks and economic disruptions. (Zetter, 2019)

The mode of Cyber-attacks which are most common with the dispute between China and Australia is espionage. Espionage is an equal term for spying. It has been typically done by governments to obtain politically or military sensitive data. Espionage campaigns also conducted through cyber methods which is known as cyber espionage or cyber spying. (Valerino & Maness,2018) Therefor the paper will focus on offensive cyber operations against the information security of Australia.

Materials and Methods

This research is based on secondary data. The method of content analysis has been used to analyze the qualitative data off the research. The materials which has been used for this particular research is secondary data relevant to the purpose of the research they are such as research papers, online Publications,

reports, dissertations and interviews etc. The data have collected form open sources. The method of content analysis has been implemented to analyze the above-mentioned qualitative data.

Results and discussion

The results of this research shows that there is a serious threat towards the information security of Australia because of the cyber activities done by Chinese organizations. These offensive cyber operations have been happening for the last few years. In the year 2019 the computer systems of the main political parties in Australia have been hacked cyber-attacks launched against the labour party,

National party and the liberal party in Australia. This cyber incident happened before the general elections of Australia in that particular year. Those are espionage campaigns which seeks to obtain the policies of those political parties, Australian government claimed that information breach done by a state sponsored stakeholder. The policy documents of various political parties are critical information because it illustrates about policies regard to national security and foreign policy economic policy and etc. It is clear that stealing such kind of data through offensive Cyber activities is an obviously threat to information security of Australia. (Sky News, 2019)

Another critical cyber-attack took place in the Australian National University in that particular year. The details of more than 20000 students and Academic Staff has been stolen. .(afr.com,2019) The data accessed by the aggressor includes names, addresses, contact numbers and other personal details of the students not only that information such as text, finance, payroll information, bank account details and passport details are also included among the data which has been stolen by the aggressor.(afr.com,2019)

Furthermore, Australian liberal senator James Patterson exposed that the Chinese government has access to the data in the social media platform of Tiktok. Therefore, the government is collecting data about the Australian Tiktok users. According to Senator Patterson these data can be used to conduct disinformation campaigns in order to manipulate the public opinion of Australian Tiktok users. Although these social media platforms functions through an Algorithm it can be manually programmed to achieve such outcomes. Not only data of the ordinary Tiktok users but they attempt to collect some other sensitive data of the government as well. (SkyNews,2022)

An American cyber security agency knows as Proof Point identified another cyber espionage campaign targeting Australian media, defense and telecommunication companies. And they have shown a special interest on

matters relevant to South China Sea as well. Currently there is an ongoing dispute among China Australia and other western powers as well. South China Sea has become one of the strategically important stand points of the Indo-Pacific. The accused hacking group known as (TA423 Red Ladon) Red Ladon is a China-based, espionage-motivated threat actor that has been active since 2013, targeting a variety of organizations in response to political events in the Asia-Pacific region, with a focus on the South China Sea. Targeted organizations include defense contractors, manufacturers, universities, government agencies, legal firms involved in diplomatic disputes, and foreign companies involved with Australasian policy or South China Sea operations. (Proofpoint, 2022)

Based on the above-mentioned cyber incidents we can clearly identify that Australian information security is clearly under threat because of destructive cyber activities conducted by Chinese government and Communist party related authorities. Mostly the Australian authorities has not been able to protect they are critical information on sectors such as universities administrative sector healthcare sector, Media, Public data and matters related to other critical infrastructure moving beyond that highly sensitive data of their political parties also has been hacked. Therefore, we can clearly determine that they are the information security is clearly and a threat.

Conclusions and Recommendations

There are certain research findings that can be illustrated in this paper especially all of these operations are politically motivated these attacks are state-sponsored. China might be involving directly in these offensive operations who otherwise they could hire a non-state actor to conduct these offensive cyber-attacks.

Nonetheless certainly there are political motivations at the first place. China wants to dismantle the critical Infrastructure in Australia. They wanted to establish their cyber dominance over Australia. There are various political factors for politically motivated cyber-attacks. Especially Australia is one of the best friends of USA in this South Pacific region and for the more there are issues related to the South China Sea. Use of cyber power is somewhere in between the conventional soft power and hard power this is the most modern method of influencing and manipulation. Therefor it is clear that China has implemented its offensive cyber capabilities to steel the critical information in Australia.

As per the recommendations Cyber deterrence is one of the major topics that are currently discussed by Cyber strategy experts' world over. Nonetheless in

order to counter this situation Australia should work to improve their network security. However, implications of cyber security will not be enough to counter such attacks. Because in the cyber domain connectivity creates more and more vulnerabilities. Most connected nations are the most vulnerable in the cyber domain. There for Australia should focus on their foreign policy as well to counter balance such kind of cyber threats.

References

Affr.com,(2019), *ANU cyber-attack began with email to senior staff member*, [Online] Available at https://www.afr.com/politics/federal/anu-cyber-attack-began-with-email-tosenior-staff-member-20191001-p52wpv (Accessed 15th July 2022)

Kremling. Janine and Parker Amanda, 2018. *Cyber Space, Cyber Security and Cyber Crime*. Sage Publishers, London.

Lin.Harbert and Zegart.Amy, (2018), *Bytes, Bombs and Spies, Brooking institutions press*, Washington D.C.

Nye.Joshep,2014, *Cyber Power*, [Online] Available at https://projects.csail.mit.edu/ecir/wiki/images/d/da/Nye_Cyber_Powe1.pdf (Accessed 13th August 2022)

Proofpoint.com.(2022),*Rising Tide: Chasing the currents of Espionage in the south China Sea*,[Online] Available at https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea (Accessed 11th November 2022).

Sky news, (2019) *Australia should name and shame the cyber-attack perpetrators*, [Online] Available at https://www.skynews.com.au/(Accessed 15th July 2022)

Skynews.com.au. (2022), *Chinese Cyber Attacks on Australian targets, defense and energy information in months long hacking*, [Online] Available at https://www.skynews.com.au/australia-news/chinese-cyber-attack-on-australia-targets-defence-and-energy-information-in-monthslong-hack/news-story/23f55f01c93e7b5827f20bf48cfdef67, (Accessed 11th November 2022)

Valreiano, Brandon and Maness. Rayan, 2018, *International Relations Theory and Cyber Security*: *Threats and Conflicts*. [Online] Available at https://www.researchgate.net/publication/326845990.

Zeter.Kim,(2019),*Countdown to Zero day*, Crown publishers, USA.