Will Cyber Warfare Become a Threat to Contemporary International Security?

Yutong Wu[1], Yudi Huang[2, *]

[1]*Hwa Chong Institution, 661 Bukit Timah Road, 269734, Singapore*
[2]*Hangzhou Xuejun High School, No. 188 Wensan Road, Hangzhou, 310002, China*
[*]*Corresponding author. Email: lydiahuang0202@gmail.com*

ABSTRACT
With the development of nuclear weapons and countries' abilities to launch destructive attacks, cyber warfare has become a new alternative for future forms of conflicts. This paper will discuss the concept of cyber warfare and the reasons why it constitutes a serious threat to international security from four perspectives. We will examine reasons include inefficient deterrence to harmful cyber attacks, limitation in legislation which leads to a lack of solution, the tendency of cyber attacks to escalate and its threat to politics. It will also conduct an analysis of the future of cyber warfare, including possible undesirable outcomes and difficulties in finding solutions.

Keywords: *cyber warfare, international security, deterrence*

1. INTRODUCTION

With the revolution in global politics and technology, new contemporary threats to international security have also emerged, undermining the stability of the world's economy, security, and politics both domestically and internationally. It is thus essential for us to understand the threats we are facing, so that we will be able to defend ourselves and preserve the peace.

In this era when violent regional conflicts are rare due to the advent of nuclear weapons and the better understanding of peace after the massive world wars, conventional war is no longer a serious threat to contemporary international security. Instead, relatively newer means such as cyber warfare began to have greater influence due to strong social reliance on the internet.

Contemporary society is operated largely dependent on modern information technology from daily activities to resources allocation such as health care, financial services and infrastructure construction. Even some weapons are controlled by computers and the actions of military forces depend on networks that share information about battlefields.

In 2007, malicious cyber activities did not register on the Director of National Intelligence's list of major threats to national security in the US. In 2015, however, they ranked first.[1] It is particularly important since its damage is rambunctious due to the complexity of technology and the potential of large-scale impact, with normal citizens would also be affected. Threats to cyber security might influence multiple fields including politics, economics and national security.

With attacks as simple as a virus, hackers, criminals, terrorists or state actors can steal intellectual property and confidential information, destroy the operation of physical machinery or deny the availability of normally accessible services.[2] With increasing number of users, functions diversifying of cyberspace, countries are more vulnerable to attacks by cyber instruments. One example is how cyber worm Stuxnet [3], which was used to attack Iran's nuclear program. Then it had affected other countries such as China, South Korea, the United States.

2. INEFFICIENT DETERRENCE TO HARMFUL ATTACKS

2.1. Problem of Attribution

It is extremely difficult to track lines of malicious code and identify attackers in cyberspace, as they can use the Internet to mask the origins of their attacks. Moreover, even if the devices are found, the ultimate instigators may still be unknown. What's worse is that sometimes states outsource their attacks to non-attributable third parties, including criminal organisations. This acts on the loopholes of legislation, making it difficult to trace and regulate.

2.2. Four Types of Deterrence Methods

Joseph S. Nye Jr. identified four types of deterrence and dissuasion [4], threat of punishment, denial by defence, entanglement, and normative taboos. However, each type has its limitations.

a. Threat of punishment is less significant in cyberspace due to problems of attribution and difficulties in determining for how long and what assets can be held at risk.
b. Denial by defence, which can be done through building resilience to networks, diving up the cost of attacks etc., plays a larger role in dealing with non-state actors

than with major states whose intelligence services can formulate an advanced persistent threat.

c. Entanglement refers to the fact that interconnectivity among stakeholders imposes serious costs on the attackers and the victim. However, this is relatively less of a deterrence for countries that lack cooperative relations with others, such as North Korea.
d. Normative taboos serves as a reputational deterrence, where an attack can violate the norm and damage a country's reputation. Thus, how states value their reputation and their international status should be considered. For countries such as North Korea, it appears that only Denial by Defence can achieve significant effect of deterrence, making it hard to prevent a cyber attack from North Korea unless highly resilient defence systems are in place.

2.3. The Threat of Non-kinetic Cyber Attacks

Non-kinetic cyber attacks refer to a class of cyber attacks that cannot cause direct or indirect physical damage, injury, or death. Due to the lack of deterrence, they are sometimes more dangerous than kinetic cyber attacks.

If a country like the United States suffered from a large-scale kinetic cyber-attack that cut off the electricity in California and caused the death of thousands of citizens, the US would find the attacker and strike back with necessary means. However, if a country hostile to the US hires hordes of people to post comments on the Internet and ruin the reputation of the US, it is much less apparent for US officials to notice these attacks and to launch an effective retaliation. This might provide an incentive for the attacker to carry out similar attacks in the future, believing that the benefit of attacking will exceed the cost.

3. LIMITATION IN LEGISLATION

Another important aspect is that international law is ambiguous regarding what constitutes the use of force when cyber attacks are concerned. It is agreed by the International Group of Experts that "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[5]

Yet, for cases that beget no immediate physical consequences, there is no definite threshold for the use of force. An approach that consists of eight key, non-exclusive factors to assess a cyber operation is proposed by the International Group of Experts. This approach depends on a holistic evaluation of the attack, making the assessment process time-consuming and complex. The lack of a definite prohibition in international law may provide an incentive for attackers to adopt this kind of cyber attacks, which can sometimes prove to be no less destructive than kinetic cyber attacks.

Moreover, loopholes in legislation exist. "Cyber attacks that cause repairable physical damage with no long-term consequences and no injury to humans have not been treated as use of force or armed attacks."[6] This makes continuous multiple attacks a possible choice for malicious actors to impose destruction on a country. The International Group of Experts agree that only attacks which are severe enough under the category of "use of force" constitute armed attacks, which are the conditions that states can exercise self-defence. Due to the absence of a definite threshold for armed attack regarding cyberspace, although it is permitted for states to consider the accumulated effect of multiple attacks for retaliation, the assessment process would still be a problem. In these cases, punishment may be milder compared with conventional attacks and kinetic cyberattacks.

4. TENDENCY OF ESCALATION

One major misconception about cyber warfare is to see the cyber realm in isolation. A response to a cyberattack can be from all sectors. McNamara's law states that it is impossible to confidently predict the effects of using military force because of risks of accident, miscalculation and misperception. Likewise, the law applies to cyber warfare, only the risks are greater due to the complexity of technology.

The peculiarity about cyber warfare is that complicated technical issues may create unexpected impact and the sufferer might mistake the intent of the attacker.

Sometimes, the attackers themselves do not know the scale of their attacks before they strike. Because targeted vulnerabilities may be patched and some networks are more resilient than others. Attackers are not sure of the timing, persistence or scope of the effects of their cyberattacks.[7] Therefore, the situation may escalate quickly and be out of control. For example, Stuxnet damaged the property of some parties outside of Iran, which sustained only 60% of the Stuxnet infections.[8] This may escalate the conflict if the affected states can identify the attackers and retaliate through other ways.

5. THREAT TO POLITICS

Cyber attacks are often used for political signaling that manipulate people's perception of their national affairs. This can be seen from how Russia hacked the Democratic National Committee (DNC) computer network in an attempt to influence the 2016 US presidential election, according to a indictment of Robert S. Mueller. Furthermore, during the 2008 Russia–Georgia war, Moscow made use of bonets originating from Russian cyberspace to silence the Georgian government websites and independent media caused the government cannot communicate to its people effectively. James P. Farwell and Rafal Rohozinski contended that "cyber can nevertheless be a tool to discredit, destabilise and weaken the authority of adversarial regimes." Governments are increasingly reliant on the Internet. Internet voting examples have taken place in over 17 countries including Australia, Canada, France,

the UK, etc., which amplified the detrimental effects of cyber attacks.

6. NEW CYBER THREATS UNDER COVID-19 PANDAMIC

Global pandemic, with COVID-19 as the most recent case, can further worsen the situation. The increased reliance of businesses, organisations and schools on the internet for remote working and learning has rendered them more vulnerabe to any form of information leakage and malicious cyber attacks. Tope Aladenusi has pointed out that "there is a possibility that an organisation's unpreparedness will lead to security misconfiguration in VPNs thereby exposing sensitive information on the internet and also exposing the devises to Denila of Service (DoS) attacks."
Cyber criminals may also capitalise on COVID-19 related applications and use them as a disguise for malicious activities. "Not only are businesses being targeted, end users who download COVID-19 related applications are also being tricked into downloading ransomware disguised as legitimate applications." With the normal functioning of security agencies hindered, the detection of malicious cyber activities can be more difficult, and responding to such activities can be more complicated.[9]

7. THE FUTURE FOR CYBER WARFARE

7.1. Possible Undesirable Outcomes

Jason Healey has pointed out three possibilities of undesirable future concerning cyberspace in his paper, namely Conflict Domain, Balkanisation and Cybergeddon.[9]
Conflict Domain is a probable future situation where cyberspace has a range of human conflicts similar to air, land, space and maritime domains as states may not limit their retaliations to cyber only. Balkanisation, where nations build sovereignty and borders, results in a collection of smaller and isolated internets. The least possible yet most destructive situation is Cybergeddon, where attackers can achieve a wide range of effects with little input, making large-scale, internet-wide disruptions easy and common. As a result, these circumstances may take a heavy toll on the level of trust between states, disrupting transnational commerce and interconnectivity.
A combination of Conflict Domain and Balkanisation may also be plausible. Countries such as China with relatively controlled cyberspace may be more isolated from other countries and relatively less vulnerable to external attacks. Western countries that are more resistant to the idea of state controlled cyberspace may have more interconnected cyberspace and thus be more vulnerable to external malicious attacks, which may escalate into Conflict Domain. For example, a 2017 cyber attack called Notpetya that initially targeted Ukraine quickly spread to infect the cyberspace of France, Germany, Italy, Poland, the UK and the US. The attack has resulted in the transportation and infrastructure system crippled.[10]

7.2. Difficulties in Finding Solutions

Firstly, policy makers are not willing to put resources in solving this problem. Without enough knowledge about this field, they often choose to ignore this problem and keep their focus on issues more to their understanding. For instance, in the US, there are insufficient motivations for an adequate sense of urgency and ownership of cybersecurity problems.[11]
Secondly, even if they are willing to solve the problem, both technical and non-technical aspects such as political consideration need to be addressed.
For instance, the insertion of Russian and Chinese malware in the US power grid in 2011 was probably designed as a reminder of those countries' capabilities in order to deter possible attacks by the US. Therefore, the solutions to these attacks must have political meaning as a response.
Furthermore, due to the constant development of IT tools and techniques, making solutions stay relevant become more complicated. Therefore, software and hardware providers to be included in the process of strengthening cyber security is necessary. Policymakers should hire IT experts to draft relevant legislation. Companies that supply the computers and its software should be held responsible for the malfunction of their products. Although specializing these responsibilities in law is redundant, they should sign a contract with the government beforehand, explaining the extent of their obligations.

8. CONCLUSION

In recent years, cyber attack has escalated into a prevalent phenomenon and has the potential to become the most important threat to international security due to the problems of deterrence, legislation, escalation and political effects. These properties of cyberattacks might cause undesirable future and make conflicts more difficult to settle. Cyberspace may thus replace conventional military fields to become the future battleground for countries.
Therefore, decision makers should avoid limiting their policies to the classical theory of deterrence and vary their strategies of dissuasion. With the rapid technological advancement in cyberspace, they should also focus on the most important attacks, understand their contexts and devise deterrence strategies using combinations of the four deterrence measures. Clear law enforcement to address the various loopholes is needed as well.
Contemporary technologies do not have the effective methods to deter cyber attacks yet, and the low cost of these attacks give them greater potential to be used by terrorist groups or other cyber criminals. New technology should be created to examine if a country steals national security information from its opponent or if organizations are using

online platforms to guide the public to support or resist political activities. Important questions like how to set an effective and correlative system to detect cyber activities, while not violating the privacy of cybercitizens, should be studied in the future.

ACKNOLEDGMENT

The authors wish to thank Nuno Monteiro, associate professor of the political science department in Yale University.

REFERENCES

[1] R. James. Clapper, Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community, Senate Armed Services Committee, 114th Cong., 2nd sess., 2016, February 9.

[2] C. David, B. Thomas, and S.L. Herbert, Editors, At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues, National Academies Press 2014

[3] P. James. Farwell and Rafal Rohozinski, Stuxnet and the Future of Cyber War, 2011, vol.53, no.1, pp.23-40.

[4] S. Joseph. Nye Jr, Deterrence and Dissuasion in Cyberspace, 2016/17, Vol.41, no.3, pp.44–71.

[5] N. Michael. Schmitt, International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed, 2012, Vol.54, pp.14–37.

[7] S. Joseph, Nye Jr, Deterrence and Dissuasion in Cyberspace, International Security Winter 2016/17, Vol. 41, no.3.

[8] P. James. Farwell and Rafal Rohozinski, Stuxnet and the Future of Cyber War, 2011, vol.53, no.1, pp.23-40.

[9] Tope Aladenusi, COVID-19's Impact on Cybersecurity, 2020

[10] H. Jason, The Five Futures of Cyber Conflict and Cooperation, edited version, 2011, pp.1-6.

[11] G. Andy, How the worst cyber attack in history hit American Hospitals, 2019.

[12] Clark, Berson, and Lin, Editors, At the Nexus of Cybersecurity and Public Policy.