CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Master's thesis

2023 **Sudhanshu Kadre**

CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Sudhanshu Kadre

The (New) Security Dilemma: Impact of Technological Innovation on the Security Dilemma

Master thesis

Prague 2023

Author: Sudhanshu Kadre, Bc.

Supervisor: Mgr. Petr Špelda, Ph.D.

Academic Year: 2022/2023

Bibliographic note

Kadre, Sudhanshu. *The (New) Security Dilemma: Impact of Technological Innovation on the Security Dilemma*. 53 p. Master thesis. Charles University, Fakulty of Social Sciences, Institut of Political Studies. Supervisot prof. Mgr. Petr Špelda, Ph.D.

Abstract

The enduring concept of the security dilemma seen from the lens of the technological revolution in Information Security provides a different perception than the traditional version of the dilemma. Moving from apparent to perceived threats, the underlying fear and uncertainty between state actors in an anarchic system have witnessed an increase. This thesis has the objective to study the effect of the advancements in Information and Community Technology, particularly in Cybersecurity, on the perception of the security dilemma. By analysing the basis of Information Security theory while simultaneously probing the cyber threat landscape through the use of case studies of cyber attacks and cyber diplomacy, the thesis highlights the relevance of the security dilemma in cyberspace.

Keywords

Security dilemma, cyber warfare, information security, international relations, critical infrastructure, network security, cyberattacks

Range of thesis: 53 Pages; 14,455 Words; 95,964 Characters

Abstrakt

Přetrvávající koncept bezpečnostního dilematu viděný optikou technologické revoluce v informační bezpečnosti poskytuje jiné vnímání než tradiční verze dilematu. Pohybem od zjevných k vnímaným hrozbám došlo k nárůstu skrytého strachu a nejistoty mezi státními aktéry v anarchickém systému. Tato práce má za cíl studovat vliv pokroku v informačních a komunitních technologiích, zejména v kybernetické bezpečnosti, na vnímání bezpečnostního dilematu. Analýzou základů teorie informační bezpečnosti a současně zkoumáním prostředí kybernetických hrozeb pomocí případových studií kybernetických útoků a kybernetické diplomacie práce zdůrazňuje relevanci bezpečnostního dilematu v kyberprostoru.

Klíčová slova

Bezpečnostní dilema, kybernetická válka, informační bezpečnost, mezinárodní vztahy, občanská infrastruktura, síťová bezpečnost, kybernetické útoky

Rozsah práce: 53 stran; 14 455 slov; 95 964 znaků

Declaration of Authorship

1. The author hereby declares that he compiled this thesis independently, using only the listed resources and literature.

2. The author hereby declares that all the sources and literature used have been properly cited.

3. The author hereby declares that the thesis has not been used to obtain a different or the same degree.

Prague 01/02/2023 **[Sudhanshu Kadre]**

Contents

Introduction

The primary organizing mechanism of the international system is structured around power balances, aiming to maintain stability in an uncertain global environment. However, within this environment lies the potential for destabilization—a complex interplay of processes seeking to disrupt power balances and hinder the efforts of statesmen and diplomats in upholding a secure international order. The most crucial dynamic among these complexities is known as the 'security dilemma,' a cornerstone of international affairs, demanding close monitoring and skilful management to safeguard global order from instability and conflicts. Traditionally, the security dilemma revolved around the accumulation of resources that posed direct threats to a nation-state's security. Existential concerns such as Weapons of Mass Destruction (WMDs) played a significant role in heightening state insecurities during the twentieth century's early and mid-phases. The concept of dual-use in science and technology further motivated states to take measures to balance perceived security disparities with their adversaries, especially evident during the Cold War era, where ideological divisions were prominent between hegemonies of opposing blocs. In the contemporary context, globalization and technological innovation have ushered in drastic changes to the dimensions of the traditional security dilemma. The evolving global economic and technological landscape has diversified the perceived apparent threats to state security, necessitating a thorough re-evaluation and adaptation of strategies to maintain international stability.

The technological advancements in the post-Cold War era, especially the Information and Communication Technology (ICT) revolution, have significantly altered how states perceive the security dilemma. The widespread adoption of dual-use technologies has presented states with the challenge of striking a balance between national security interests and the economic and social benefits derived from these technologies. Dual-use technologies have opened up new avenues of securitization, such as cybersecurity, which, as the term "dual-use" implies, can be exploited by state actors to conduct attacks in the international system.

While the origins of Weapons of Mass Destruction (WMDs) were deeply rooted in the dual-use nature of cutting-edge scientific developments, a key distinction exists between WMDs and contemporary threats like offensive cybersecurity vectors. Modern trends in ICT reflect a perceived sense of threat, contrasting with the overt and apparent forms of threats observed during the Cold War era. This evolving threat landscape has prompted states to prioritize cybersecurity and invest substantially in defensive capabilities to mitigate risks effectively. These transformations can be attributed to various factors, including globalization, economic interdependencies, and technological innovation.

As with all scientific and technological progress, the evolution of ICT concepts has expanded its applications, inherently increasing the dual-use nature of the technology. In the case of nuclear weapons development, states can rely on several indicators to identify threats, enabling them to formulate concrete response plans based on observable patterns. Conversely, non-direct threats posed by offensive actions, such as cyberattacks, amplify state insecurity due to their less apparent nature. Consequently, nation-states must develop comprehensive responses to potential attacks on their critical infrastructure, leading to heightened insecurity. The non-apparent nature of perceived threats thus tends to elevate state insecurity more than overt and explicit threats.

The trend of enhancing security resilience in response to perceived threats brought about by the ICT revolution has been particularly notable in the Western world since the late 1900s. To protect critical infrastructure from cyber-attacks, institutions like the National Institute for Standards and Technology (NIST) in the USA and North Atlantic Treaty Organization (NATO) in Europe have devised cybersecurity guidelines and standards. Additionally, intelligence agencies such as the National Security Agency (NSA) have intensified their focus on cyber espionage (offensive strategy) and cyber resilience (defensive strategy) to safeguard national security interests. The non-lethal nature of cyber-attacks contributes to the security dilemma, as democratic states require almost unanimous domestic support to respond effectively to existential threats directly linked to human life loss. However, when threats do not involve direct loss of human life, diverse political motivations can influence the response, affecting its timing and effectiveness, thereby increasing overall state insecurity.

The concept of the security dilemma has been extensively researched, ranging from historical case studies like the Cuban Missile Crisis to issues of domestic sovereignty like the China-Taiwan tensions. Nevertheless, most research has focused on threats related to physical harm and conventional weapons. The ubiquity of ICT in critical infrastructures creates vulnerabilities that threat actors may exploit, resulting in harm to property and intellectual assets. As the Western world experiences relative peacetime, conflicts between state actors have evolved from all-out offensives to strategic and discreet manoeuvres, making the attribution of blame more complex. This paradigm shift calls for a change in research approach, incorporating the concept of perceived threats to assets like critical infrastructure in the security dilemma. This thesis aims to address this research gap by analyzing the security dilemma with an emphasis on the relationship between ICT and security. The primary research question is "What is the relevance of ICT innovation to the perception of the security dilemma?". However, for the sake of keeping the scope of the research study limited in an effort to avoid dilution, the thesis would specifically focus on the innovations in cybersecurity, as a subset of the ICT revolution, and their effects on the security dilemma.

The thesis would begin by discussing the relevant literature associated with cyberwarfare and the role of IT in state operations. The analysis of the chosen articles would entail critique, support and further probing by the researcher, in an effort to highlight the importance of the research topic. Following the literature review, the theoretical conceptualisation of the research topic would consist of delving deep into the conventional perception of the security dilemma. This investigation would not only provide a reference towards the conventional security dilemma, which would be used multiple times in later sections but would allow a seamless segway to the new interpretation of security dilemma with the undertone of the relationship between IT and security studies. Apart from discussing the avenues of security studies, the theoretical conceptualisation would also entail exploring crucial terminologies of the IT security lexicon. To limit the overpowering of the technological tangent, the exploration of Information Security concepts would be kept to a minimum and in simplified tones. This would be followed by a discussion of the methodological approach taken in this research study. The section on methodology would entail the primary methodological approach chosen for this study and the reason behind doing so. Subsequently the topics of the nature of data, method of data collection and analysis would be depicted succeeded by the operationalisation. After highlighting the methodology, the discussion of the empirical findings of the research would be elaborated to form a frame of reference to probe the thesis question. The discussion of the empirical findings would form the major part of the thesis. Ultimately the conclusion of the thesis would provide a summary of the key points discussed.

Literature Review

Cerny's work pioneered the discourse around the questioning aptness of the traditional sense of the security dilemma in the status quo[1]. The author fixates on the Cold War being the watershed moment which initiated the changes in the incentive structure in the international order that has led to developments, "(1) an increasing divisibility of benefits in a globalizing world economy and (2) the declining effectiveness of interstate mechanisms at preventing defection not only by states ('defection from above') but also by non-state, sub-state and trans-state actors ('defection from below')".[2] Through his arguments, he depicts the need for a change in the approach of how the scholarship and the world perceive the security dilemma. However, as per the research gap proposed by this research study earlier, the author has kept the element of technology as a far-off tangent rather than a core part. This is a major downside of Cerny's ground-breaking research, the foundation to the mobilisation of the "by non-state, sub-state and trans-state actors" has been the increase in accessibility of technology.

[1] Cerny, Philip. (2000). *The New Security Dilemma: divisibility, defection and disorder in the global era*. Review of International Studies. 26. PP: 623–646. DOI: 10.1017/S0260210500006239

[2] *Ibid*

The foundation of his critique can be used to further probe the traditional framework of the security dilemma in light of cyber warfare. However, it is of the utmost importance to reframe Cerny's arguments with the consideration of advanced cyber threats in the current international landscape. These threats, although acted upon by threat actors, are based on vulnerabilities that persist in network infrastructure caused either by user negligence or developer mishaps. The interests of state, non-state and trans-state actors need to be investigated against the backdrop of each entity's cyber capabilities, whether documented or perceived.

Tang's encapsulation of the traditional framework of security dilemma forms a great reference that can be used to compare and contrast the research[3]. The basis of Tang's argument revolves around the assumption of the prevalence of an anarchic state, in which the state actors are considered to be defensive realists. Tang adds to his explanation with an emphasis on the perceived offensive display of even a purely defensive build-up. Any kind of alteration in a state's materialistic capability in the perception of its adversaries will ultimately affect the apparent threat. As a result, in a real-time scenario, adversarial states can incorporate countermeasures to defensive measures as well. Through a feedback cycle, this interplay between actions and reactions reinforces the inherent fears present in the perception of the states in the international system. These fears are amplified in terms of cyber "insecurity", given the factors of weak attribution towards operations and increased threats for false-flag operations. Tang concludes his explanation with the depiction of possible consequences of this feedback loop, threats of war or actual war. This study strongly supports Tang's core arguments of state actors being defensive realists, especially in the case of offensive cyber incursions. As would be shown

[3] Tang, Shiping. (2009). *The Security Dilemma: A Conceptual Analysis*. Security Studies. 18 (3). PP: 587-623. DOI: 10.1080/0963641090313305

throughout the research study, in terms of cyber operations, even actions with offensive direction can be classified as defensive operations. It's reasonable for a state to be uncertain about the intentions of another state, ally or not, in an anarchic system as stated by Tang, given the tortuous history of international relations. However, one important element present in almost all traditional concepts of security studies is the relationship between the action (which when observed leads to the build-up of insecurity) and the initiating state actor. Based on this relationship, the threatened state can justify its actions under the notion of pre-emptive defensive bolstering. This dynamic entirely changes in terms of cyberspace and the perceived threat of cyber-attacks. With no definite tangent of attribution, it's almost impossible for the threatened state to justify its action as defensive to the international community. This issue of the absence of attribution is one of the central focus of this research study.

Buchanan captures the essence of the security dilemma's significance in cyberwarfare and state affairs[4]. Furthermore, he posits that the security dilemma still holds in terms of the dynamics of cybersecurity with no alteration of perception. Even from a social scientist's perspective, Buchanan delves deep into the technical elements of the issue with keeping the terminologies easy to understand. The author's work would be taken as a central inspiration towards this study's research approach, especially from a methodological point. However, for a better grasp, the scope depicted by Buchanan needs to be limited to a few central concepts alongside the further simplification of the technological tangents of the discourse. This research highlights the secondary argument made by Buchanan; not only does the security dilemma applies to the avenue of cyber war, but the effects of the security dilemma are greatly amplified. Going back to Tang's

[4] Buchanan, Ben. (2017). *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford Academic. DOI: 10.1093/9780190665012.001.0001

depiction of the traditional concept of the security dilemma, one of the many core factors behind the phenomenon was the inherent mistrust between state actors[5]. When seen through the lens of the powerplay in the international community during The Cold War, the effect of just the idea of clandestine movements on a state actor's perception led to a precursor to pre-emptive strikes.

This important dynamic of anticipatory self-defence, which could be considered one of the outcomes of the security dilemma, has been codified in the Customary International Law (ICL) under the "Caroline Principle"[6]

As per the principle, there exists legal justification for a state to engage in anticipatory self-defence in the presence of two conditions:

"1. The use of force must be necessary because the threat is imminent and thus pursuing peaceful alternatives is not an option (necessity);

2. The response must be proportionate to the threat (proportionality)"[7]

The two conditions of necessity and proportionality can be only proven when the threat is attributed to an actor. However, as Buchanan puts it, the uncertainty due to the lack of attribution amplifies the security dilemma in the case of cyberspace.

[5] Tang (594)

[6] Paddeu, Federica. (2020). *Origins of the Right of Self-defence in International Law: From the Caroline Incident to the United Nations Charter, written by Tadashi Mori*. Journal of the History of International Law. 22. PP: 595-600. 10.1163/15718050-12340175

[7] Tait, Adam P. (2005). *The Legal War: A Justification for Military Action in Iraq*. Gonzaga Journal of International Law. 96

In a thorough retrospective of the history of cyberspace, Singer and Friedman bridge the gap between revolutionary IT traits and perceived threats attributed to cyberattacks[8]. Along with Buchanan's work, this book could be used as a reference to provide a historical preface to cyber warfare. However, unlike Buchanan's work, Singer and Friedman provide a cursory glance at the threat landscape in cyberspace. In doing so, they keep the topics of the text as non-technical as possible with a very basic language with no confusing jargon used to explain the terminologies of network security. Furthermore, Buchanan would agree with the authors when they delve deeper into the human errors, posed as the "weakest link" in the chain of cybersecurity, by connecting it back to the subject of state insecurity in regards to network architecture[9]. Singer and Friedman. Aside from being a great introductory text into cybersecurity and cyberwar, the book goes off on a plethora of varied tangents.

As a foundational basis, the generalised approach is optimal, however, due to the dilution of the scope the core issues like cyber resilience, threats posed to critical infrastructure and the lack of attribution are only touched on the surface. For a better cohesive understanding of the perceived threats posed by offensive cyber operations, Buchanan's specificity needs to be incorporated into the generalised narrative tone of Singer and Friedman. Unlike Singer and Friedman, Buchanan's book provides a direct correlation between the security dilemma and the cyber threat landscape. Components like the role of intelligence agencies and the different attack vectors utilised by threat actors need to be explored, although in a basic manner, to answer the provided research question of this thesis. The approach taken by the authors in this work is perfect for this study, however,

[8] Singer, P.W; Friedman, Allan. (2013). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press

[9] Buchanan (62)

the scope is still a bit too general. As mentioned earlier, the generalised approach taken by Singer and Friedman would be utilised in conjunction with the specificity used by Buchanan and the other authors mentioned in this literature review.

As mentioned earlier, the innovation associated with IT needs to be explored to get a better understanding of the research questions, however on the other hand the simultaneous militarization of this technology is of the same importance, if not higher. Salminen and Kerttunen explore the militarisation of the IT revolution and its effect on state security at an international and national level[10]. In the article, offensive cyber capabilities are used as an argumentative basis to ascertain the threats posed to international security. Although not planned by the authors, the article is a great addition to this research study primarily due to the brilliantly written section on the threats to international security. The security dilemma essentially is modelled in a dual-state scenario with a handful of prerequisites, as depicted by Tang. However, by evaluating the threats posed by the militarisation of IT innovations, the alteration of the state's perception of the security dilemma can be investigated. It is important to note that while the article offers valuable insights, there are a few areas where further elaboration or analysis could have been beneficial. For instance, a more detailed exploration of the implications of offensive cyber capabilities on state sovereignty and the international norms governing warfare in cyberspace would have strengthened the argument.

Additionally, discussing the potential countermeasures and strategies that states can adopt to mitigate the risks posed by cyber-military capabilities would have provided a more well-rounded perspective on the work of Salminen and Kerttunen. However, the case

[10] Salminen, Mirva; Kerttunen, Mika. (2020). *The Becoming of Cyber-Military Capabilities*. Routledge Handbook of International Cybersecurity. PP: 94-10

selection of authors doesn't justify itself. Firstly, the authors don't justify the selection of his case study state of the US and the Netherlands. The selection of the US under such a research topic is justified by the geopolitical significance of the state in terms of heightened "cyber-tensions" with states like the People's Republic of China (PRC) and the Russian Federation. On the other hand, the research itself doesn't focus a lot on the Netherlands, as most of the reference frames are based on US capabilities. Furthermore, the ideal case scenario for a case study would be that of contrasting elements in terms of cyber strategy while highlighting the overarching similarities. As the research topic is heavily based on the militarisation of cyber-innovation, a better choice of the counterpart of the US in this study would be either PRC or Russia (the former being an ideal choice). The dynamic between PRC and US-based cyber operations has been used to depict the non-apparent threat of offensive cyber intrusions by Buchanan, Singer and Freidman.

For a war to be justified, there are certain requirements it needs to adhere to International Humanitarian Law (IHL), which brings forward the concept of an ideal war. As per the status quo, the concept of a cyber war cannot be compared with traditional warfare in terms of the requirement laid out in IHL, it requires to be analysed as a separate case. Jenkins analyses the ideal of a "cyber war" by bringing in the requirements of justified warfare under IHL (Jus in Bello)[11]. The underlying threat that's perceived in a security dilemma is attributed to potential offensive warfare. Jenkin's commentary could be used to question the offensive nature of cyberwarfare (between state actors and between state and non-state actors) by comparing it with conventional military warfare. Although the moral discussion of the "ideal war" is important for the chosen research topic, the primary connection that would be used in this study would be the justified conditions of waging

[11] Jenkins, Ryan. (2016). *Cyberwarfare as Ideal War*. Binary Bullets. PP: 89-114

cyber war. As observed in the majority of scholarship about cyberwarfare, the legal aspect of the lack of physical tangibles associated with cyber operations isn't focused on. As per the security dilemma, war is considered to be the inevitable outcome between the states with increasing insecurity. However, as compared to other means of showing proof of militarisation (as a justification of pre-emptive retaliation) through intelligence gathering, doing so for cyber capabilities isn't as straightforward. Most states get evidence of others' "cyber bolstering" only through intrusive operations, which although meant to be defensive can easily be considered as an offensive operation thus being considered as the first act of aggression itself[12]. Inconsistencies like these are what make Jenkins' approach very interesting to be included in discussing the issue of the lack of attribution and how it affects the security dilemma.

In his United Nations Institute for Disarmament Research (UNIDIR) published work, Melzer poses the most important question regarding cyberwarfare and its connections to security dilemma: "Does a cyberattack constitutes a use of force according to international law?"[13]. Along with Jenkins's line of analysis, Melzer's work can be used to reinforce the cause behind the heightened state of insecurity regarding cybersecurity[14]. Following the line of enquiry posed by Jenkins, Melzer's approach to the legality behind cyber warfare in the current structure of international law can be used to add depth to this study. Melzer's enquiry into the extent of the justification of cyber war as per Jus ad bellum (the body of law under international law that governs the legal justification of war) poses an interesting question of whether the security dilemma is affected by this ambiguous teeter-totter of "legal or not" when it comes to cyber warfare.

[12] Buchanan (77)

[13] Melzer, Nils. (2011). *Cyberwarfare and International Law*. UNIDIR Resources: Ideas for Peace

[14] Jenkins, Ryan (92)

However, the difficulty in monitoring cyber "acts of aggression" is not considered by the author, rendering most of his arguments solely relying on UN instruments for enforcing the UN Charter, one of the fundamental documents in maintaining international peace and security[15]. The issue does extend to our chosen topic as the definition of the "use of force" determines what weaponry can be considered as potential threats. As per the traditional security dilemma, the unprovoked use of a whole spectrum of weapons from conventional arms like Small Arms and Light Weapons (SALW) to WMDs is considered to be a "use of force"[16]. Primarily the aforementioned weapons comprise a direct possibility of the loss of human life and as such the highly regulated governance regime on them is to be expected. However, unlike conventional arms, cyber "arms" can be used to execute surgical attacks that could have virtually no loss of human life. This is where the nuances of cyber attacks need to be inspected. While almost the entirety of the spectrum of cyber attacks poses a virtual existential threat to human life, the targets of these attacks can have a significant impact on the facilitation of human life. Public institutions like schools and hospitals can be targeted by cyber-attacks, similarly energy grids and water processing plants.

All these institutions comprise an important part of the critical infrastructure network in states, dismantling them would directly affect the quality of human life. Considering Melzer's line of questioning is of the utmost importance to impart depth in the research sub-topic of the connection between security dilemma and vulnerabilities in critical state infrastructure that can be exploited by threat actors.

[15]United Nations. (1945). *Charter of the United Nations.* UN Secretariat. 1 UNTS XVI

[16] *ibid*

To continue the discourse on the significance of cybersecurity in the field of critical infrastructure (to be specific, Industrial Control Systems (ICS)), we need to review the work by Eleonora et al. on the same topic[17]. While the sub-sections regarding the ethics of cybersecurity in national security can be an interesting addition to the theoretical conceptualisation, for the main discussion of this study, the parts regarding technical aspects of cybersecurity of critical infrastructure and ICS will be focused on. One of the salient points made by the authors needs to be highlighted: The enhanced connectivity of critical infrastructure leads to an increase in its vulnerability which increases the political incentive to enhance prevention against internal (domestic and non-state actors) and external threats (enemy state actors).

This point directly encapsulates the spirit of the thesis topic of this study which highlights the relationship between innovation and the deepening insecurity between states in the international order. However, in the earlier section, while defining the different types of attacks on critical infrastructure, the authors have missed out on various possibilities due to the overcomplication of the attack scenarios. While defining their "merely cyber" attack (the authors consider "a virus or trojan" examples in this category) the authors fail to incorporate possible tangible consequences. Furthermore, by putting "a virus or trojan" in the same category, Buchanan would agree that the authors unknowingly highlight the issue with the major part of social science scholarship about cybersecurity: the technical inconsistencies in depicting cyber-attacks.

[17] Viganò, Eleonora. Loi, Michele. Yaghmaei, Emad. (2019). *Cybersecurity of Critical Infrastructure (The Ethics of Cybersecurity)*. Springer. DOI: 10.1007/978-3-030-29053-5_8

The word "trojan" can be associated with trojan horse malware (malicious software) which simply put is software that looks legitimate but when interacted with can take control of your data (much like the ancient Greek analogy)[18]. It should be focused on that for the complete weaponization of the trojan horse malware, there needs to be user interaction, as such the user is involved in the process (again much like the analogy where the Romans had to open the door). On the other hand, viruses don't need any user interaction to proliferate and harm the user's system. Given this depiction, it wouldn't make sense to pigeonhole these two attack vectors in a category which entails attacks with no physical tangibles. If you consider an ICS to be attacked by a trojan horse malware, once the deployment is successful, the system can be halted by the perpetrator amongst other actions. The narrative describing the importance of cybersecurity vulnerabilities of critical infrastructure and ICS can be made into a holistic approach by adding the technical descriptions of the attack vectors.

Like the security dilemma, other classical concepts of security studies have been affected by the introduction of cyberspace as a new avenue for warfare. Brantly's work on analysing the deterrence theory can be taken as a parallel to this study's analysis of the security dilemma[19]. Similar to this research study, Brantly has reviewed the current literature in terms of cybersecurity (from a social science perspective) and argued that "cyber deterrence" is already a reality and needs to be understood much more comprehensively. Furthermore, unlike set aside from the rest of the scholarship, the author brings in the theory of deterrence by denial (broadcasting defensive capabilities to

[18] Wijayarathne, Senesh. (2022). *Trojan Horse Malware - Case Study*. Sri Lanka Institute of Information Technology

[19] Brantly, Aaron. (2018). *The cyber deterrence problem*. 10th International Conference on Cyber Conflict. PP: 31-54. DOI: 10.23919/CYCON.2018.8405009

attacks that could be used for threatening) in the realm of cybersecurity. Denial by deterrence is very closely linked to the security dilemma as the primary intention of the latter is to bolster defensive capabilities to broadcast to the enemy that the state can defend against its new-found capabilities.

Theoretical Conceptualisation

In the realm of international relations and geopolitics, a conventional realist understanding of the security dilemma stems from the prevailing anarchic nature of the global system. In the field of international politics, Waltz describes an anarchic system as a state within the international order characterized by recurring patterns of behaviour[20]. Within this context, the actions of existing states assume a structured and discernible pattern in the eyes of their allies and adversaries alike. Waltz portrays the current international system as deeply decentralised and anarchic. Such an anarchic state breeds fear, uncertainty and distrust between state actors which acts as a foundational base for the security dilemma[21].

The three primary academics that spearheaded the traditional conceptualisation of the security dilemma have been John Hertz, Hebert Butterfield and Robert Jervis. The thought process adopted by the authors identified structural commonalities between the myriad of definitions of the security dilemma that were posited at the time. Tang, whose depiction of the security dilemma would be taken as the theoretical foundation for the

[20] Waltz, Kenneth. (1979). *Theory of International Politics*. Addison-Wesley

[21] Hertz, John. (1950). *Idealist Internationalism and the Security Dilemma*. World Politics. 3(2). PP: 157–80. DOI: 10.2307/2009187

purpose of this thesis, incorporated the similarities pointed out by Butterfield, Hertz and Jervis (collectively termed the "BHJ" definition by Tang) and added that as the foundation of his own conceptualisation of the security dilemma. As per Tang, the phenomenon of security dilemma possesses certain definable telltale signs:

> "Under a condition of anarchy, two states are defensive realist states—that is, they do not intend to threaten each other's security. The two states, however, cannot be sure of each other's present or future intentions. As a result, each tends to fear that the other may be or may become a predator. Because both believe that power is a means toward security, both seek to accumulate more and more power."[22]

Furthermore, Tang's conceptualisation can be reinforced by Buchanan's addition of the offence-defence balance[23]. Initially, Tang added to his definition, the perceived magnitude of the offensive nature of a purely defensive attitude. However, by considering the offence-defence balance portrayed by Buchanan, Tang's conceptualisation can be further expanded. The offence-defence balance essentially questions whether in an isolated condition, the offence has the advantage in terms of dominion or it's the defense. Security dilemma bases the perception of threat on the bolstering of either offensive or defensive capabilities of a state actor in an anarchic system.

Even if, such an increase in the state's defensive capabilities can be considered to be expected in an anarchic system, the perceived threat still leads to misinterpretation of intentions. This theoretical baseline gives a reference to the perception of either the

[22] Tang (594)

[23] Buchanan (103)

offensive or defensive manoeuvring from the state’s point of view and its threat evaluation. Tang’s depiction of the security dilemma ends with discussing the possible results of the phenomenon, either the proclaimed threats of war or actual warfare. This is where the traditional perspective falls short in terms of considering the situation of cyber warfare. Compared to traditional warfare, the avenue of a cyber war would be considerably complicated given the intangibles associated with it. A feedback pattern ensures that the states engaged in a security dilemma, based on perception, unknowingly reinforce the underlying fears behind their actions which in turn facilitate an increase in insecurity. This feedback system is used as a conclusion point by Tang in his conceptualisation, depicting the inevitable result as a heightened state of alert due to threats of war or an actual violent confrontation. Alongside the BHJ definition, Tang’s addition to the conceptualisation of the security dilemma highlights certain factors like the absence of hostile intentions between the states, an international state of anarchy and the gathering of some materialistic power that ultimately acts as a threat to other state actors in the international system.

For this thesis, the pair of definitions from Butterfield, Hertz and Jervis; and Tang, would be considered as the traditional perception of the security dilemma. The traditional security dilemma is identified by the direct threats posed by conventional warfare, like WMDs and SALW. However, for the purpose of the research of this thesis study, the basis of the threats posed by the cyber capabilities of the state needs to be explored from a theoretical perspective. Although intangible, the threats posed by cybersecurity vulnerabilities play a great role in rogue actors (state or non-state) exploiting them.

For the purpose of understanding cybersecurity threats, the fundamentals of the professional field of information security need to be reviewed. In the lexicon of information security, all rogue processes can be considered as a subset of the Confidentiality, Integrity and Accessibility (CIA) triad[24]. The CIA triad forms the fundamental solution framework for all cybersecurity patches (fixes).

Confidentiality is the element that describes the intended encryption of data in order to make sure only users with the right level of access can see the content. Taking the example of an asymmetric cryptography algorithm like the RSA (named after the MIT scientists that first described it in 1977, Rivest–Shamir–Adleman), the process is used to create two separate keys that work together to encrypt the data. In RSA or other asymmetric algorithms, a key pair is produced; a public and private key. The public key is used for encryption and as the name suggests is open for public access by the sender, receiver and the rest of the internet. However, the private key (used for decryption) is meant for the access of only the sender and receiver. Attack vectors that are aimed at acquiring access to systems or data packets that the attacker isn't authorised to access are categorised under the umbrella of confidentiality attacks. The attacks not only comprise the unauthorised viewing of the data packets but alter it as well (however, the latter action is better classified as a data integrity attack). In the finance world, actors like day traders rely heavily on confidentiality to make sure to ensure their upper hand on their competitors which can be compromised by an attacker cracking their encryption system and viewing their trades before they enter them.

[24] Amalarethinam, George & Leena, H.M. (2017). *Enhanced RSA Algorithm with Varying Key Sizes for Data Security in Cloud*. 2017 World Congress on Computing and Communication Technologies (WCCCT). PP: 172-175. DOI: 10.1109/WCCCT.2016.50

An example of a confidentiality attack is the Man-In-The-Middle (MITM) attack, where the threat actor hijacks the informational stream between the sender and receiver. In an MITM attack, the attacker sits between the sender and receiver (unknowingly to both) and gains access to all the information being sent back and forth. Furthermore, all attacks aimed at acquiring sensitive user credentials (usernames, passwords, answers to security questions) can be classified as confidentiality attacks. In most cases, confidentiality is ensured through good practices revolving around password management and using Multiple Factor Authentication (MFA) where in addition to a single factor used for identity authentication (most often a password or a Personal Identification Number (PIN) code) a second factor is used (most often a confirmation through a second device like a mobile phone)[25].

Moving on to the "I" of the CIA triad, data Integrity is associated with the content of the information in the data packets. In the ideal scenario, it is expected that the content sent by user A has to be received, unaltered, by user B. In such a case, the data integrity is kept safe. However, if user C intercepts the message (while in transit), alters it and sends it to user B, the data integrity of the communication has been compromised. As mentioned earlier, vulnerabilities that put data confidentiality at risk also put data integrity at risk too. Data integrity is maintained based on the information being authentic (based on the source), accurate (tamper proof) and reliable. Attackers can comprise data integrity by bypassing security protocols often used by companies like network Intrusion Detection Systems (IDS) (IDSs would be expanded in further chapters as they're a critical part of the research).

[25] Otta, Soumya; Panda, Subhrakanta; Gupta, Maanak; Hota, Chittaranjan. (2023). *A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure*. Future Internet. (15). PP: 146. DOI:10.3390/fi15040146

Furthermore, an organisation’s security policies and protocols, if inadequate, can be blamed for integrity attacks. Such policies are most often associated with patch updates in regard to major software companies. When companies release software updates, the responsibility falls on the user or the organisation to execute the update, the failure of which could allow an exploit to take place. However, some attacks like Zero Day Attacks bypass this scenario as the patch for the vulnerability is not yet released. In a typical Zero Day scenario, an attacker finds a previously unknown vulnerability in the system of most often a major software company. This allows the threat actor to penetrate the system through an exploit without setting up any alarms. In most cases, even after the company releases a software update for the specific vulnerability, the attacker has already established a backdoor (persistence) in the system for future attacks.

Vulnerabilities associated with data integrity are most often protected by encryption and hashing algorithms. Unlike encryption (which is a two-way process, data can be encrypted and decrypted), a hashing algorithm is used to produce a specific alphanumeric string with the input of any data point (mp3, doc, pdf; any information that can be stored electronically). The alphanumeric string (known as the hash of the file) would be unique to the informational content of that file. If the file’s hash has been sent to the receiver beforehand, the user just needs to put the received file through the mentioned hashing algorithm and compare the hashes, if the hash is different, it is confirmed that the integrity of the file has been tampered with. However, no information about the file content can be extracted from the hash (as it’s a one-way process), making it an ideal process to check for any data integrity vulnerabilities in a network system. Thus, data encryption combined with hash verification acts as a solution directed at both confidentiality and integrity.

Data availability, put simply, refers to the access of data to the users (or customers) that are authorised for reading or editing privileges. The hindrance in the availability of this. Attacks like Denial-of-Access (DOS) and Distributed DOS (DDOS) target data availability to hinder the operations of a domain[26]. A typical DOS attack takes place at the data input part of the website; where the website through web protocols is requested to perform a certain action by a visiting user. For a typical DOS attack, only a single source of traffic is used to crash the target server with a large number of service requests. Unlike a DOS attack, a DDOS attack a group of data sources to achieve the same result as a DOS attack[27]. In a normal setting, domains have enough bandwidth to handle adequate requests at a time. However, threat actors use a large number of accounts to request a certain service and after a threshold is crossed, the website, unable to accommodate a large number of requests, crashes. For a successful DDOS attack (usually, the targets for DDOS attacks are large-scale servers with the capability to handle a large number of service requests), the threat actor or actors need a large number of user accounts on their side. To gather a large number of accounts, rather than requesting the help of that many users, threat actors often build a botnet of a large number of authentic accounts. Put simply, a botnet is a collection of authentic and compromised user accounts/devices which can be controlled by the threat actor without the knowledge of the owner of the account/device[28]. Normally, botnets are formed after a massive zero-day compromise of popular software platforms, like Microsoft, which are used in a majority of devices over the world. The use of botnets is crucial for threat actors as they not only

[26] Tripathi, Nikhil; Mehtre, B.M. (2013). *DoS and DDoS Attacks: Impact, Analysis and Countermeasures.* Institute for Development and Research in Banking Technology. PP: 1-6

[27] *Ibid*

[28] Mendonça, Luís; Santos, Henrique. (2012). *Botnets*. Proceedings of the Fifth International Conference on Security of Information and Networks. DOI: 10.1145/2388576.2388580.

make high click frequency attacks possible but also thwart attribution due to the diversity in geological locations of the device's Internet Protocol (IP) addresses. Data availability attacks can be prevented by systematic monitoring of the user traffic, this can be done by a person (or a group of persons) or software. Any anomaly in the user traffic (when compared to the baseline traffic) could be identified beforehand and contingencies can be constructed to make sure services are not targeted.

All processes and attack vectors, regardless of their intent, that would be discussed in the following research section can be categorised into one of the CIA triads. To understand the effect of the exploit, the vulnerability needs to be analysed regarding the service it affected.

Moving on to core terminologies use in bolstering network security, it is of the utmost significance to expand on network intrusion detection and protection. Information security triage and incident handling are critical components of cybersecurity, and at their core are the Intrusion Detection System (IDS) and the Intrusion Prevention System (IPS). The main objective of an IDS is to detect and identify any attempts at compromising the fundamental components of the CIA triad. To achieve its purpose, an IDS carefully analyses information infrastructure and server traffic, thoroughly examining it for potential signs of external malicious assaults, as well as internal system exploitation or attacks. It plays a vital role in safeguarding the integrity and security of a network by promptly alerting security personnel to any suspicious activities or threats.

IDSs can be broadly classified into two types: Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS)[29]. NIDS primarily focuses on

[29] Napanda, Shah, Kurup. (2015). *Artificial Intelligence Techniques for Network Intrusion Detection*. International Journal of Engineering Research & Technology. 4 (11). DOI: http://dx.doi.org/10.17577/IJERTV4IS110283

analysing network traffic to identify unauthorized, illegal, and deviant activities. It accomplishes this by collecting data packets crossing the network infrastructure using ports or network taps, without directly disrupting the flow of network traffic, thus operating in a passive capacity. On the other hand, HIDS is designed to target and protect specific devices within a network. It diligently monitors and alerts the local Operating System (OS) of the targeted device, seeking any signs of malicious activities or abnormal behaviour. Typically, a HIDS involves a single agent functioning on each system to provide a comprehensive view of potential security threats. In order to effectively track and recognize illegal activities, IDS utilizes pre-defined signatures based on well-known attack characteristics (mostly published online in the form of Common Vulnerabilities and Exposure (CVEs)), leading to the notion of a signature-based IDS. This approach relies on a database of known attack patterns, allowing the system to promptly match incoming traffic against these patterns and raise an alert if a match is found. Another approach used by IDS is the anomaly-based detection method. This technique establishes a baseline of normal server behaviour by monitoring inbound and outbound server traffic data. The system then continuously compares real-time traffic against a baseline that’s decided as per the normal server behaviour, flagging any deviations or unusual activities that may indicate a potential cyber threat. The IDS plays a crucial role in the realm of information security by providing real-time monitoring and detection of potential cyber threats. Its ability to analyse network and server traffic, coupled with signature-based and anomaly-based detection methods, empowers organizations to proactively defend against cybersecurity risks and enhance their overall security posture. By rapidly alerting security teams to potential threats, IDS enables timely incident response and mitigation, safeguarding the CIA triad of critical infrastructure assets. However, cybersecurity solutions can only be theorised with normal conditions as a frame of reference. In real-time conditions, the approach of threat actors significantly deviates from what is considered normal and this deviancy cannot be accommodated in a theoretical conceptualisation.

Methodology

A methodology outlines the way research is conducted, encompassing both data collection and the overall research study's tone. In general, three main methodological approaches are used for research: quantitative, qualitative, and mixed methods[30]. The quantitative approach is commonly employed when studying static elements that can be measured using a known metric system, thus relying on numerical observations. A phenomenon can be analysed quite successfully through a quantitative approach if there is only one interpretation of the event. Furthermore, the requirement to quantify the action being researched is a significant prerequisite for using the quantitative approach. Given that the security dilemma cannot be quantified as per the difference in interpretations of the state actors is difficult to put in a metric. The security dilemma itself is theorised upon the perceptions of state actors pertaining to the power gathering of others in the anarchic state of the international order. Such a phenomenon needs to be studied from an approach that revolves around human interpretations of a phenomenon (for the purpose of this study, state actors would be held in the frame of reference of human activity). The third and final methodological approach, the qualitative approach, emphasizes analysing the significance and interpretation of human-oriented experiences.

[30] Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative, And Mixed Methods Approaches*. Sage Publications, Inc. 3

For this research thesis, a qualitative methodological approach will be utilized. The utilisation of such an approach would allow deeper probing into the dynamic of the security dilemma and the threat perception of cybersecurity vulnerabilities and weapons. The qualitative approach was chosen for this thesis study for a plethora of factors, including as stated above, analysing the dynamic of the security dilemma as a human-led action. Furthermore, the qualitative approach allows the researchers to adapt and refine their study design based on emerging patterns and unexpected findings, ensuring a comprehensive analysis. However, the cons of the approach need to be highlighted as well, alongside methods through which the issue would be dealt with. Due to the small sample size and specific context, the empirical findings may not be easily generalized to a larger scale. The inability of not being able to scale would be accommodated by keeping the overall scope limited to specific case studies, which would be employed in this research study. In a qualitative approach, the researcher's subjectivity and interpretation may influence the findings, requiring rigorous reflexivity to mitigate bias and ensure rigour in the study.

In terms of research, independent variables are decided based on elements that need to be categorised by the researcher and whose effects on the dependent variables are to be studied. For the purpose of this research study’s frame of reference, the element of innovation in ICT, particularly in the realm of cybersecurity, would be assumed as an independent variable while the dependent variable would be the perception of the security dilemma. In summary, the thesis would explore how cybersecurity innovation (independent variable) influences the security dilemma (dependent variable) and would attempt at investigating the implications and outcomes of these interactions.

Considering the type of data to be collected for the thesis, non-numerical textural information would be optimal to assess the effects of cybersecurity advancements on the security dilemma. In order to construct an investigative narrative for the thesis, secondary data. It should be noted that the use of diverse sources may lead to conflicting explanations and opinions. However, such a variation in the data sets would be harnessed constructively through the practice of data triangulation in the research study[31]. By employing multiple data sources, including scholarly and media materials, the research topic will be thoroughly analyzed, allowing for a comprehensive response to the research question. This approach facilitates the exploration of the underlying causal relationships within the reality of the security dilemma and the broader patterns of how it is perceived through the lens of cyber warfare. By maintaining this separation, the thesis aims to gain a deeper understanding of cybersecurity's impact on the security dilemma and how it is understood by various stakeholders, especially when compared to its traditional perception.

Moving to the part of data collection, the method would involve utilizing the researcher's university email and library resources to access full-text secondary academic data. For the purpose of this research study, a unique combination of secondary data collection and archival research would be the most effective approach[32]. The former will allow for obtaining academic sources through research organizations, while the latter will focus on

[31] Carter, N., Bryant-Lukosius, A., DiCenso, A., Blythe, J., Neville, AN. (2014). *The use of triangulation in qualitative research*. Oncology Nursing Forum. 41 (5). PP: 545-547

[32] Bhandari., P. (2020). *Data Collection: Definition, Methods & Examples*. Scribbr (blog)

gathering media reports and government press releases relevant to the selected thesis topic[33]. State reports usually contain biases as the content is heavily influenced by the foreign policy of the state actor, keeping this in mind, the archival approach would be used sparingly to limit any biases in the empirical findings. The implementation of this combinational approach ensures a comprehensive and diverse dataset, facilitating a deeper understanding of the research topic. By accessing secondary academic data through university email and library resources, the study can draw from reputable and peer-reviewed sources. Simultaneously, the utilization of archival research will offer historical context and media perspectives on the issue, enabling researchers to analyze how perceptions and attitudes may have evolved over time. Furthermore, combining these two approaches enables data triangulation, reducing the risk of bias and enhancing the overall credibility of the findings. The integration of multiple data sources contributes to a more robust and well-supported research study, increasing the potential impact and value of the research outcomes.

After collecting data from the aforementioned sources, the research study will utilise a document analysis approach to investigate the correlation between traditional and new perceptions of the security dilemma through the medium of case studies. This particular method of document analysis is a structured process used to assess and evaluate various documents, encompassing both printed and electronic materials, including computer-based and Internet-transmitted content. Similar to other qualitative research analytical approaches, this method entails thorough examination and interpretation of data to extract meaning, acquire comprehension, and establish empirical knowledge[34]. Through

[33] Kabir., S. (2018). *Methods of Data Collection. Basic Guidelines for Research: An Introductory Approach for All Disciplines*. Book Zone Publication. PP: 201-276. DOI: 10.5281/zenodo.5814115

[34] Bowen, Glenn. (2009). *Document Analysis as a Qualitative Research Method*. Qualitative Research Journal. 9. PP: 27-40. DOI: 10.3316/QRJ0902027

document analysis, the research seeks to discern how changes in cybersecurity practices and perceptions impact the security dilemma through the use of case studies. By analyzing the data, the researcher would identify the intervening causal processes that have shaped the shift in attitudes towards the security dilemma. This method allows for a detailed examination of the interactions between cybersecurity measures, international relations dynamics, and evolving perceptions of security threats. The formation of case studies through qualitative research offers a systematic and rigorous approach to understanding the underlying factors that contribute to changes in the security dilemma. By exploring the causal links between the chosen variables, the research can provide valuable insights into the complex nature of cybersecurity's influence on security perceptions.

Empirical Findings

Cyber-Threat Landscape and the Anatomy of a Cyber Attack

According to the 2019 report by Cybersecurity Insiders, the cloud and IoT sectors experienced a significant portion of cyberattacks[35]. Among the prominent vulnerabilities in cloud services, the report emphasizes that hackers exploit the enhanced accessibility of cloud interfaces by users, resulting in reduced resistance to unauthorized access. As per the report, the top cloud vulnerabilities included:

i. unauthorized cloud access

ii. insecure interfaces

iii. misconfiguration of the cloud platform

iv. account hijacking

A major challenge faced by security teams is the limited visibility they have into cloud interface security and compliance. Additionally, issues like the subpar enforcement of adequate security policies in regards to cloud and on-prem (hardware systems found in the offices) and the dearth of qualified security personnel in organisations aid in increasing vulnerabilities.

[35] Cybersecurity Insiders. (2019). *2019 Cloud Security Report (ISC)2.* Cybersecurity Insiders [Web]. URL: https://www.cybersecurity-insiders.com/portfolio/2019-cloud-security-report-isc2/

Radware, a US-based cybersecurity provider, in its 2018-2019 annual report on cyber threats associated with Internet of Things (IoT) devices reported that major vulnerabilities in three aspects of network security need to be addressed:

i. Malware sharing

ii. Lacking invisibility

iii. Denial of service[36]

Reinforced by these findings, offensive cyberspace operations targeting state network infrastructure have been increasing. From a conventional standpoint, an ideal cyber-attack against state network infrastructure comprises three primary steps. Internet-facing parts of the state network interfaces are constantly probed for vulnerabilities, which once found are then exploited. Software intended for spying (Spyware) is embedded in government-based devices to execute passive intelligence gathering. State devices or government personnel profiles are targeted through malicious software which encrypts their data and holds it for ransom (Ransomware).

Before going on towards explaining the specific attack vectors like ransomware, the approach of a cyber attack needs to be highlighted. Once understood, the approach would decode all cyber-attacks that are mostly used against state-based network infrastructure. After a vulnerability is discovered by an attacker, the process is straightforward as this is a rare moment where the target has been caught with its defence down, which in most cases is attributed to human error. However, normally the network infrastructure that contains sensitive data, especially linked to state security, is adequately guarded. For the

[36] Radware. (2018). *2018-2019 Global Application and Network Security Report*. Radware [Web].

purpose of studying cyber threat actors, a general approach to an attack has been constructed known as the cyber kill chain[37].

The cyber kill chain offers a structured framework to deconstruct complex cyberattacks into distinct and non-overlapping stages or layers. This layered approach allows analysts to address smaller and more manageable components of the attack, facilitating effective problem-solving. Simultaneously, it empowers defenders to counter each phase by developing targeted defences and mitigation strategies for every stage of the attack. The cyber kill chain generally consists of seven consecutive stages of actions (see Figure 1) beginning from reconnaissance and ultimately culminating in execution or acting on the set objective.

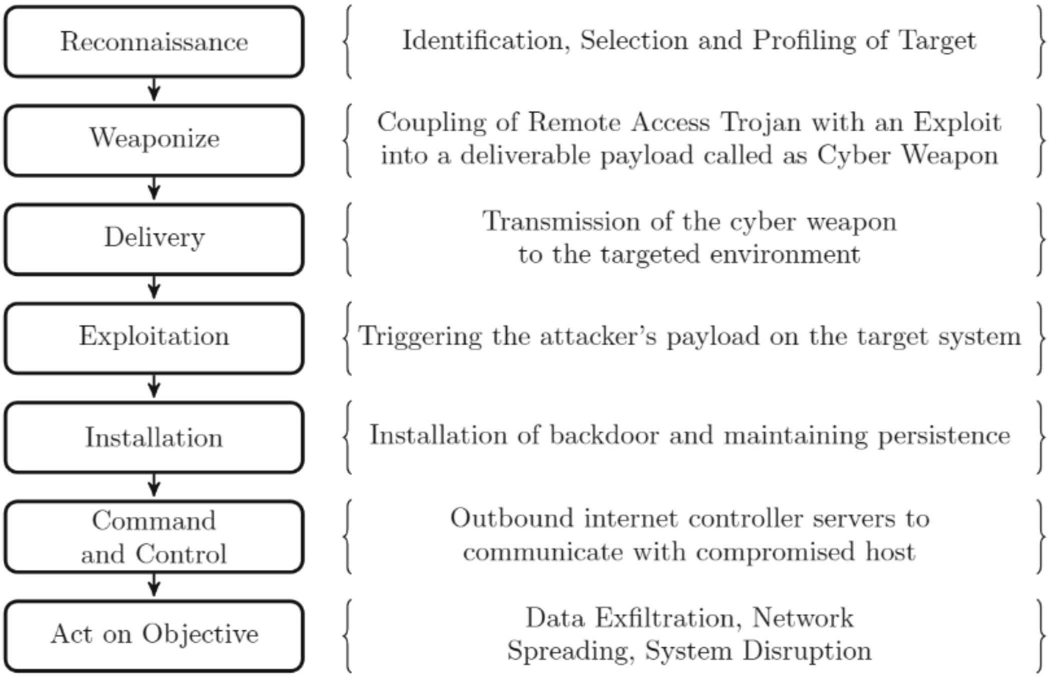

Reconnaissance
Identification, Selection and Profiling of Target
Weaponize
Coupling of Remote Access Trojan with an Exploit into a deliverable payload called as Cyber Weapon
Delivery
Transmission of the cyber weapon to the targeted environment
Exploitation
Triggering the attacker's payload on the target system
Installation
Installation of backdoor and maintaining persistence
Command and Control
Outbound internet controller servers to communicate with compromised host
Act on Objective
Data Exfiltration, Network Spreading, System Disruption

Fig 1: Cyber Kill Chain[38]

[37] Yadav, Tarun; Rao, Arvind. (2015). *Technical Aspects of Cyber Kill Chain*. Defence Research and Development Organisation, New Delhi, India. DOI: 10.1007/978-3-319-22915-7_40
[38] *Ibid*

Reconnaissance refers to the process of gathering information about a potential target, which can be either an individual or an organization. However, in the case of government organisations, intelligence gathering is generally targeted towards employees. This cyber kill chain step involves distinct stages such as target identification, selection, and profiling. In the context of cyberspace, reconnaissance can be considered Open-Source Intelligence (OSINT) gathering. OSINT gathering is conducted by the threat actors primarily via web-crawling websites, conference logs, blogs, social media platforms, mailing lists or newsletters, and utilizing network tracing tools (cookies) to obtain relevant information about the target. The data collected during reconnaissance is crucial for later phases of the cyber kill chain, as it helps in designing and delivering the payload.

Based on the intelligence gathered, the weaponising stage includes the formulation attack of the payload, in this case, called the “cyber-weapon”. The payload itself consists of a Remote Access Trojan (RAT) and an Exploit, the former being the kind of software that grants the attacker access to the payload after delivery and the Exploit simply put, is the malicious software or malware that would later be used to execute the attack[39].

Although every step in the kill chain needs to be carefully executed, the delivery stage is of the most importance for the attack as it’s only in this stage that user interaction is required. For a cyber-attack to achieve its objectives successfully, having the target information is essential (which is gathered in the reconnaissance stage). For the majority of the Exploits to be executed, some form of user interaction is necessary, such as downloading and running malicious files (mostly executable files (.exe)) or accessing malicious web pages on the internet. Furthermore, this user interaction needs to be

[39] *ibid*

tailored in a way that the user believes to be legitimate. This is where the concept of social engineering comes into play with respect to the cyber kill chain. Social engineering is an information security term that describes the systematic manipulation of users with the objective of them enacting a preferred action, in most cases which is clicking a link to a malicious site or downloading malware. Since the popularity of the e-mail system, social engineering has been used to manipulate clicks, which has only risen with the proliferation of social media platforms. However, delivery is a risky stage for attackers as it leaves behind identifiable traces. Consequently, many attacks are executed anonymously by utilizing paid anonymous services, compromised websites, and compromised email accounts to conceal the attacker's identity.

Once the “cyber-weapon” is delivered, the target fulfils the necessary user interaction, the exploitation stage leads to the execution of the weapon on the target's side. Upon execution, the subsequent step involves triggering the exploit. The exploit's objective is to silently install or execute the payload without raising any suspicion. However, in order for exploitation to be successful, a few conditions need to be met. Firstly, the target user’s device needs to be running the OS that the exploit was designed for (this detail is decided after OSINT gathering in the reconnaissance and weaponization stages). Furthermore, the OS version needs to be the one that the exploit was designed for, hence if the OS has been updated, the exploitation stage would fail and the kill chain would be aborted. Anti-Virus (AV) software (if any) installed on the device should not pick up the signature of the exploit during its runtime. When all the specified conditions are met, the exploit is activated, and it will effectively save (if the payload is to be executed at a later time) or directly execute the payload on the target's system. Once the payload is deployed, it establishes a connection with its Command-and-Control twin, notifying it of the successful execution and awaiting further instructions to carry it out. Installation entails the establishment of a backdoor in the target's system in an effort of maintaining persistence. Establishing persistence translates into maintaining an entry into the system regardless of any further software updates in the future.

The Command and Control (C&C) system is a crucial component of remotely executed cyber-attacks. It serves as a means to provide covert instructions to compromised machines from a remote location. Additionally, the C&C system acts as a centralized hub for exfiltrating data from compromised machines. The C&C system would be further expanded during the C&C stage[40].

In the concluding stage of the cyber kill chain, the attacker has infiltrated the system, exploited the targeted vulnerability, established a foothold and now is free to act on the primary objective. This framework is used for almost every cyber attack approach, with the kind of Exploit being changed in the weaponization stage and the kind of delivery system in the delivery stage. Furthermore, the objectives of threat actors are different based on the target organisation, in the case of state-based infrastructure, the objective is mostly to encrypt the data and ask for ransom alongside others. Now that the threat propagation method has been discussed, the assessment of the same needs to be discussed, particularly the difficulty in doing so. Even from the traditional perception of the security dilemma, threat assessment is difficult with respect to creating contingencies in case of future retaliation or even pre-emptive self-defence. However, in the realm of cyberspace, the difficulty in assessing the threat is significantly higher.

[40] *ibid*

Threat Assessment in Cyberspace

A "threat assessment" involves evaluating and analysing the potential risks confronted by various entities, such as nations, businesses, or individuals. The assessment entails a comprehensive examination of potential threats, by state actors in the case of the thesis subject, to determine their severity and potential impact on the state's security. By conducting a threat assessment, states can proactively identify vulnerabilities and implement appropriate measures to mitigate risks and enhance their overall security posture. It is a crucial proactive practice aimed at safeguarding against potential dangers and ensuring the resilience of the entity in the face of emerging threats[41]. There are various factors behind the difficulty in conducting threat assessments, however, the human inclination to "believe the worst" or what's known as "threat inflation" is the most significant contributor. This dynamic lies at the very foundation of the security dilemma where states don't know the entire information about a certain defensive manoeuvre by a different state, which ultimately leads to threat inflation even if there's no threat in reality. A good example of a wrongly executed threat assessment is the 1967 US satellite reconnaissance advancement effort in order to monitor the Soviet's missile capabilities with increased precision.

After a decade of a strategy based on the fear of the strength of the Soviet's missile stockpile, US President Lydon Johnson put a halt on the advancement strategy by stating:

> "We were doing things that we didn't need to do. We were building things that we didn't need to build. We were harbouring fears that we didn't need to have."[42]

[41] Singer; Friedman (148)

[42] *Ibid*

However, compared to the apparent threat to human life posed by missile systems, cyber weapons pose threats that cannot be easily quantified, which makes the process of threat assessment for state actors even much tougher. Every novel malware can be crafted in distinct manners to accomplish diverse objectives. The intangible nature of cyber threats becomes even more critical when attempting to evaluate a potential adversary's actions and intentions. Unlike physical weaponry, cyber threats lack clear indicators, making attribution challenging amidst a plethora of potential state and non-state actors. Even if the source of the attack is identified, determining the adversary's actual motive remains immensely difficult.

Cyber attackers may target systems for various purposes, such as intelligence gathering, data theft, operational disruption, or merely showcasing their capabilities. In the cyber realm, threat assessment involves predicting likely risks, yet many of these risks may only be revealed after an attack occurs. Influenced by “threat inflation” state actors often engage in exploratory intrusions in the network infrastructure of other states under the guise of a defensive reconnaissance. However, a cyber intrusion, regardless of its intent being passive or offensive, can and will be construed as an offensive intrusion by the target state in a condition of security dilemma. In case the state cannot find the intent behind the intrusion or if there exists even a faint hint of ambiguous evidence in the perception of the intrusion, the state would mostly tend to lean on the side of being suspicious. However, this propensity of feeling insecure would be different for the weaker states as compared to stronger states (in terms of materialistic power accumulation)[43].

[43] Buchanan (96)

The Attribution Issue

Three crucial aspects of the capability of cyberwarfare methods to access and employ other computers hold particular significance. Firstly, it operates without the restraints of any geographical limitations. For instance, an individual in the Czech Republic could compromise computers in South Korea, using them to launch attacks on systems located in the US, which might, in turn, be controlled by computers physically based in the PRC. This type of "piggybacking" method is used firstly to cover the tracks of the source of the attack vector and secondly to cast aspersions on other states, thus adopting a false-flag strategy. Secondly, the user of a compromised device is often unaware that it is being used by a remote actor (mostly through RAT software) for malicious purposes.

As discussed earlier, a botnet used in DDOS and DOS attacks employs a similar strategy where the user has no idea that their devices are being used for hacks. During the DDOS attacks of 2007 that targeted Estonian-based websites, 25% of the attacking devices sued in the botnet were US-based, despite the initial source of the attack being traced back to Russia[44]. Thirdly, even with advanced analysis, it is typically challenging to identify the specific device being used to launch a cyber-attack. Determining whether that device is being operated remotely and, if so, by whom, remains a far more intricate task. In numerous scenarios, even when a device is not being accessed remotely through a RAT, it remains a huge issue to ascertain the identity of the user, nationality of the IP, or organizational affiliation of the user(s) using it.

[44] Singer, Freidman (76)

These kinds of issues particularly are of concern if the IP is found to be in places like university libraries or cafes. Places with public Wi-Fi are a hotspot for criminal cyber activity as the router itself cannot save information about the devices connected to it. Furthermore, the advancement in commercial Virtual Private Network (VPN) software adds an extra layer of anonymity to the process. Having this information would be vital during a crisis, but it is seldom accessible promptly, and efforts to gather it raise significant privacy issues. Attribution in cyber incidents is often shrouded in ambiguity. The ability to trace an actor's efforts to a specific location is only the tip of the iceberg. Establishing complicity, particularly in terms of a government's involvement, poses considerable challenges. While sophisticated tools and methodologies can track actions in a particular country or region, proving the government's explicit role as a perpetrator or supporter is considerably more complex.

A significant complicating factor in attribution lies in the difficulty of initially discerning whether an action is hostile or not. For example, a seemingly innocuous shift in routing information at an Internet access point might indicate a routine update, or it could be a malicious attempt to redirect Internet traffic. Similarly, a barrage of unusual traffic hitting a system's firewall could be attributed to a misconfigured application from some corner of the world or a stealthy probe of the system's defences by malicious actors. Unlike traditional weaponry, where radar can quickly identify a missile for what it is, packets in the digital realm do not come with clear labels indicating their intent. Once malware infiltrates a system, it often operates in a clandestine manner without bearing any telltale signs of its origin or intent. Unlike physical weapons like SALW or even WMDs, which can be traced through distinctive signatures, malware rarely offers clues pointing to a specific culprit.

This anonymity makes it challenging for investigators to attribute attacks to any individual or even state actors with certainty. The complex nature of attribution often leads to an attribution dilemma which could be considered as an extension of the underlying security dilemma, particularly in the context of cyber warfare. Investigators must carefully consider their real-world objectives and the potential consequences of attributing a cyberattack to a specific actor. This is where the foreign policy of the state actor comes into play directing the cost-benefit analysis of blaming a certain state, whether ally or foe, for a cyber attack on its network infrastructure. Once the decision of attributing a cyber attack to a state has been made, there exists the desire to communicate knowledge of the perpetrators to the public. By exposing the individuals or groups responsible for the attack, there is an intention to shame them publicly, potentially forcing them to halt their malicious activities.

However, such an approach must be carefully weighed against potential collateral damage, especially if the individuals identified are operating with the direct support of a state actor or have extensive hacking capabilities. Combined with attribution, the issue of disclosing the origin of the attack has been theorised in a statement ‘There are two major roadblocks to international cyber diplomacy (attribution and disclosure dilemma)’ by Ashford[45]. In the process of exploring the thesis subject, it was found that in the realm of cyberwarfare, not only does the security dilemma holds true but is further divided into more underlying dilemmas eclipsing the process from the attack to the defence side.

[45] Lancelot, Jonathan. (2020). *Cyber-diplomacy: cyberwarfare and the rules of engagement.* Journal of Cyber Security Technology. 4. PP: 1-15. DOI: 10.1080/23742917.2020.1798155

“Cyber Weapon” Case Study: Stuxnet

In 2010, the nuclear energy section of the Iran-based Bushehr power plant was scheduled to launch in the month of August, however, the launch experienced a delay[46]. Iranian authorities attribute the delay of the launch to an undisclosed technical issue with the plant equipment. Earlier that year, in the month of June, an AV company VirusBlockAda discovers a worm, which would later be named Stuxnet after they receive a malware sample associated with an Iranian device that forced the system to execute an infinite reboot loop[47]. The peculiar aspect of the worm, as stated by VirusBlockAda, was that it used a zero-day exploit for propagation which was unprecedented for worms at the time, so the news goes public and gained traction. After digital forensic analysis by the AV company, it was released that the worm’s origin and targets were organisations in Iran.

Furthermore, by August it was found out that the C&C servers of the worm disconnected in the Iranian servers, indicating that the Iranian government was already dealing with the issue. By the end of 2010, it was confirmed that the worm was developed in a manner to target the operations of Iranian Uranium enrichment centrifuges configured in the same manner as that in the Natanz uranium enrichment complex. Stuxnet is now known to be the name of a specific computer worm that targets Supervisory Control and Data Acquisition (SCADA) systems found in the control mechanism of industrial controllers. The worm was found to have exploited four zero-day vulnerabilities that targeted devices that ran Windows OS. Upon infiltrating the system, the worm was analysed to have targeted the Siemens Simatic WinCC/Step-7 software, which was utilised to manoeuvre industrial processes.

[46] Baezner, Marie & Robin, Patrice. (2018). *Hotspot Analysis: Stuxnet*. Center for Security Studies (CSS), ETH Zürich. 1
[47] *ibid*

Upon the infection of the aforementioned systems, the worm was able to gain command and control of the Programmable Logic Controllers (PLCs) of the industrial equipment, which were sued to regulate power in them. By being so specific, even though it infected a lot of devices, all the conditions for delivering the payload were only met when the worm reached the SCADA systems of the uranium enrichment centrifuges located in the Natanz enrichment facility. Upon all the conditions being met, the worm acted on its objective which was to gradually fluctuate the rotating speed of the centrifuges which led to irreparable damage to the Iranian nuclear program. Numerous AV experts have claimed that the development of Stuxnet could only have been achieved by a nation-state.

They base this assertion on its high level of complexity, significant resource investment, and apparent specific targeting of centrifuges in Natanz. It is evident that the creator(s) of the worm possessed in-depth knowledge of the Iranian facilities, machinery, and computer systems. On the global scale, Stuxnet, being a watershed moment in cyberspace politics demonstrated a state actor’s capability to construct an exceptionally advanced and aggressive cyber weapon. Furthermore, this instance illustrates that merely isolating a critical infrastructure network from the internet can no longer be deemed a sufficient security measure. Nations have come to recognize the necessity of taking proactive steps to protect themselves from similar attacks. As a result, several states made significant investments in cybersecurity and established military cyber units and centres, aiming to enhance their capabilities in anticipation of potential cyber warfare.

Additionally, some states have initiated a comprehensive review and update of their cyber strategies, specifically focusing on safeguarding critical infrastructures and reinforcing their capacity to respond to cyberattacks within legal frameworks. This case study reinforces the heightened volatile environment of cyber diplomacy which adds to the argument that even the existence of such a level of cyber capabilities with one state actor created a feeling of unease in others given the anarchic system of the international order. Thus, the altered status quo includes much more misinterpretations by state actors leading to security dilemmas.

The Cybersecurity Dilemma in Play: US-China Cybersecurity Landscape

The 2015 U.S.-China Cyber Agreement marked a watershed moment in the history of the US-China cyber-diplomacy with its commitment toward greater cyber-compliance[48]. However, as seen in the following years, the agreement has become an empty shell that is considered to be a failure still in existence. The current state of the US-China Cyber Agreement can be taken as a direct image of the increasing tension between both sides leading to a deadlock. As a precursor to the 2015 discussion, In May 2014, the US Department of Justice (DOJ) charged five hackers belonging to the People's Liberation Army (PLA) with "computer hacking and economic espionage against six American entities within the nuclear power, metals, and solar products industries"[49].

[48] Rollins, John W; Lawrence, Susan V; Rennack, Dianne E; Theohary, Catherine A. (2015). *U.S.-China Cyber Agreement*. University of North Texas Libraries
[49] *Ibid*

U.S. Attorney General Eric Holder provided a direct statement about the indictment during the 2015 discussions:

> “This is a case alleging economic espionage by members of the Chinese military and represents the first-ever charges against a state actor for this type of hacking."[50]

When it comes to cyber diplomacy, the hotly debated concept of “cyberspace sovereignty” has been at the centre of the mismatch between the cyber strategies of the PRC and the Western state actors like the US and most of the European Union (EU)[51]. In 2016, a year after the discussion regarding the US-China Cyber Agreement took place, the Cybersecurity Administration of China put out its Cybersecurity Strategy which clearly demonstrates that the Chinese government does not view cyberspace as a global shared space but rather as an area where its national sovereignty is applicable. Consequently, the establishment of cyber regulations must be mindful of and uphold the principle of respecting each nation's sovereignty[52].

On the other hand, the foreign policy of the US and the EU has always considered cyberspace as a form of “global commons” since the release of the Quadrennial Defense Review Report by the US in 2010. The Western perspective highlights the central principle and foundation of global Internet governance, to be the notion of cyberspace sovereignty. It advocates for the creation of universally accepted international regulations and anti-terrorism conventions for cyberspace, under the guidance and leadership of the

[50] *ibid*

[51] Chin, Yik Chan & Li, Ke. (2021). *A Comparative analysis of Cyber Sovereignty Policies in China and the EU*. The 49th Annual Research Conference on Communications, Information, and Internet Policy

[52] *Ibid*

UN. Based on this ideological difference, the cybersecurity strategy of both the US Army and PLA has become very specific and active since the late 2000s.

The US military's Cyber-Command (CYBERCOM) was established in 2010 as the primary driver of the US's cyber strategy under the DOD[53]. Even the placement of its headquarters could be considered a strategic move having the NSA at its neighbour. The proximity allows the two organisations the ability to share cyber intelligence and personnel with relative ease. As a step to further strengthen the bond between the two organisations, the Director of the NSA also serves as the head of CYBERCOM. The US cyber strategy is focused on addressing three questions:

i. What should be CYBERCOM's mission area and responsibilities?

ii. How far should the US military venture to retain manoeuvrability in cyberspace?

iii. How can the US maintain deterrence in both cyberspace and the real world?

While addressing the first issue, the wider roles taken by CYBERCOM to deter cyber threats have led to the operations getting closer to the public sector, which in turn leads to a twofold problem. Alongside working on the infrastructure to defend the state network, CYBERCOM along with the NSA had to further widen its scope to defend the public device infrastructure, which is fairly unstructured and scattered. Now addressing the second issue of manoeuvrability, CYBERCOM had to rethink its initial scope of operations. At its time of inception, the organisation was said to simply focus on "the day-to-day defence and protection of all DOD network"[54]. Based on its responsibilities, the

[53] Singer, Friedman (134-144)

[54] *Ibid*

overarching themes of the CYERCOM's strategy include, "treat cyberspace as an "operational domain" as the rest of the military does the ground, air, or sea; implement new security concepts to succeed there; partner with other agencies and private sector; build relationships with international partners; and develop new talent to spur new innovation in how the military might fight and win in this space."[55]

The following decade saw astronomical changes in role distribution and overall active personnel. The growth hacking activity attributed to the PRC, especially the Second Bureau of The Third Army (PLA) also known as Unit 61398 or APT1. APT1 is an Advanced Persistent Threat (APT) registered by the US and its allies with allegations of Chinese state-sponsored hacks. An APT is generally a non-state actor, either acting independently or state-sponsored, possessing exemplary skills and resources for the purpose of executing cyber attacks having high-level targets like multinational corporations, international organisations or governments.

Central to this escalation is the notion of "informatization," a defining feature of the Chinese military's cyber operations strategy. As highlighted in a significant Chinese military report, modern armed forces, particularly the U.S. military, heavily depend on information. Therefore, the party that gains supremacy in the cyberwar battle will take control of the "new strategic high ground." Furthermore, taking over the "upper hand of the enemy" will be decided by "whether or not we're capable of using various means to obtain information and of ensuring the effective circulation of information; whether or not we are capable of making full use of the permeability, sharable property, and connection of information to realize the organic merging of materials, energy, and

[55] Singer and Friedman (135)

information to form a combined fighting strength; [and] whether or not we are capable of applying effective means to weaken the enemy side's information superiority and lower the operational efficiency of enemy information equipment."[56]

The significant military activity and strategic planning in the cyber domain undoubtedly raise concerns among other nations observing China's unprecedented rise in economic, political, and now military influence. However, amidst the apprehension, it is essential not to mistake ambition for complete capability. Despite the challenges, PRC's expansion in military cyber power carries two significant implications, mirroring the growth of America's military cyber capabilities. Just like in the US, there is uncertainty regarding the involvement and comprehension of the Chinese civilian political leadership in their military's plans. This concern may be even more pronounced in PRC, considering the considerable latitude the current political system grants to the PLA. Consequently, there is a concern that Chinese military cyber capabilities and operations might surpass the comprehension of civilian leaders, potentially leading to exceeding limits during a crisis that could have been averted.

The apprehension of a militarized cyberspace might actually deter both the US and PRC from engaging in the very cyber conflicts they appear to be preparing for. During a meeting with US officials, a high-ranking Chinese military officer revealed how their views on cybersecurity evolved as both sides enhanced their cyber powers and escalated the stakes in a potential conflict:

> "The United States has big stones in its hands but also has a plate-glass window. China has big stones in its hands but also a plate-

[56] Singer and Friedman (142)

> glass window. Perhaps because of this, there are things we can agree on."[57]

Future of the Security Dilemma in Cyberspace

Throughout this study, the primary thesis question associated with the evolution of cybersecurity and its effect on the security dilemma has been probed and furthermore, it's been posited that the security dilemma holds in reference with cyber warfare. The traditional conceptualisation of the security dilemma had the backdrop of the existential threat of WMD proliferated by two superpowers during the Cold War era, in which most of the actions were straightforwardly attributed to either of two state actors embroiled in a security dilemma. With the ICT revolution, the global threat landscape has changed, and based on the cyberwarfare threats, counter-arguments are prominent that suggest the irrelevance of cybersecurity in terms of the security dilemma. In order to extrapolate the future of the security dilemma with the current threat landscape as the baseline, it's of the utmost importance to consider the counter-arguments.

"The security dilemma is most present in matters of perceived existential threat. The cybersecurity dilemma discusses threats that fall well short of this standard since cyber capabilities are simply not as powerful. As a result, states can reasonably bear the risk of suffering a serious cyber attack because they will be able to retaliate with kinetic weapons."[58][59]

[57] Singer and Friedman (144)
[58] Buchanan (147)
[59] Jervis, Robert. (1985). *From Balance to Concert: A Study of International Security Cooperation*. World Politics. 38-1. PP: 69

Buchanan’s use of Jervis’s statement against the relevance of the security dilemma in the field of cyber warfare is based on the latter’s argument that the cyber threat is not existential and thus doesn’t lead to creating a security dilemma. The argument deserves consideration in the framework of this thesis. From a traditional standpoint, the security dilemma can be considered to be of the strongest magnitude when the apparent or perceived threat is existential, most often comprising a threat to human life. In the cases of existential threats, taking the Cold War as a frame of reference, any kind of intelligence leak could lead to a surprise attack from the view of the state actors. Subsequently, the avenue of intelligence and counter-intelligence interception being considered with security dilemma bolsters the point. The overall risk associated with the either Soviet or the American WMD access program being hijacked by the other, although not direct or existential, was looked at as a real threat by both parties. Thus, even if Jervis’s statement, seen as an objection, deserved consideration, it doesn’t undermine the relevance of cybersecurity (through the form of network intrusions in this example) in the modern perception of the security dilemma.

“A security dilemma is most acute when new evidence increased the apparent plausibility of merely possible threats. In cybersecurity, because of the uneven distribution of capabilities, threats are either obviously plausible (as occurs when weak states fear comparatively stronger ones) or barely possible (as occurs when strong states fear weak ones). Therefore, regardless of the state’s capabilities, the dilemma of interpretation arising from a detected intrusion does not appreciably change a state’s overall fears.”[60]

[60] Buchanan (151-152)

While accepting the strategic defensive advantages of the network intrusions, the above counter-argument posits that cyberwarfare in an offensive capacity is not critical enough to be destabilising. The argument bases itself on the fact that there exists a large gap between the “haves” and “have-nots” in the cybersecurity world. State actors with higher amounts of cybersecurity infrastructures would always have the upper hand over the weaker states. According to the objection, not only would the stronger state weather an attack but would have ample opportunity to retaliate. While the argument holds when the capability of the state actors is seen from a traditional perspective of conventional power and weapons, in the current threat landscape the argument loses its ground.

Firstly, if the security dilemma is purely seen from a theoretical standpoint, case studies between state actors having a significant gap in their military capacity are hardly chosen from a traditional security studies point of view. Similarly, a security dilemma associated with the difference in the cybersecurity prowess of the two states would simply not be a great case study. However, that doesn’t mean that confrontation wouldn’t be critical enough to be destabilizing. Furthermore, although ironic, even in the traditional power dynamic, stronger states have been overwhelmed by weaker states through the use of unconventional strategies like guerilla warfare. From a similar standpoint, states with overall weaker cyberwarfare capability can still prove to be an issue for the stronger states by focusing on less-intensive attack vectors like social engineering. The existence of asymmetric attacks targeting vulnerabilities allows weaker states to use the overwhelming strength of strong state actors to their advantage. Cybersecurity exploits can be considered asymmetric, which gives the weaker state the opportunity to be on level ground with stronger states in terms of cyberwarfare capabilities.

It needs to be highlighted that in comparison, security dilemmas based on the threat of conventional weapons are far more critical than the ones based on the fear and uncertainty of cyberwarfare. However, the basic tenet of the relevance of cybersecurity in altering the perception of the traditional security dilemma holds. Furthermore, with the current rate of growth in cybersecurity technologies, rather than fading, the relevance is most likely to grow in the coming years.

Conclusion

The enduring concept of the security dilemma illustrates that in various scenarios, fears and tensions arise not only between states seeking conflicts but also between state actors striving to ensure their own survival. State actors recognize and understand their own insecurities and take prompt action to address them. However, the risk of unintended threats, amplified by a lack of credible information flow, can lead to the formation of a dangerous cycle of fear. In an anarchic international system, state actors must rely on themselves, giving them a valid reason to fear the worst in terms of escalation of already-held fears. In the realm of cybersecurity, these conditions create a perilous dilemma. Sophisticated attacks like Stuxnet highlight the watershed moment in the international avenue of warfare that has ushered in the time of realistic cyber warfare without the hyperbole of a science fiction backdrop. Network vulnerabilities are an ever-existing problem which cannot be completely stopped but just mitigated. Furthermore, these vulnerabilities allow threat actors to execute carefully planned exploits on a high level, such as the case of Stuxnet utilising multiple Zero-Day exploits at once. Cyber attacks have evolved to a level where the vector using a variety of delivery mechanisms only executes the exploit based on the specific signature of the intended target. Furthermore, through targeting the network security of the state’s critical infrastructure like power grids, water treatment plants and public hospitals, cyber attacks have the possibility to directly pose a threat to human life. However, state actors still have trouble grasping the understanding threats posed by cyber attacks as compared to conventional warfare. Unlike conventional weapons, cyber weapons lack the tangential elements that can be used to push for a policy in a political environment. The case study of US-China cyber relations bolsters the point of increasing insecurity in cyberspace based on ideological and policy-based misinterpretations. The regular “blame game” between the US and PRC further forms the basis of the issue of the sub-dilemma of attribution and disclosure under the overarching security dilemma in cyberspace.

Ultimately, the impact of cybersecurity on the security dilemma revolves around fear and escalation: the fear instigating the creation of the dilemma in the first place and the potential escalation it may trigger if the conditions stay the same. In most cases, policymakers' decisions are shaped by this pattern of fear and escalation between the state actors embroiled in the dilemma. Overcoming the dilemma through cybersecurity advancements relies on various factors, such as increased investments by states in baseline defences in their network architecture, readiness for trust-building measures with other states, and maintaining a long-term security posture which is both scalable and sustainable. However, the possibilities for solutions may diminish if the cost of such actions exceeds what states are willing to bear from a cost-benefit standpoint. Especially states possessing influence have the leeway to either decide to bear the cost of confidence-building measures or just adopt a protectionism stance in terms of cyber defence.

In an anarchic system, states' scepticism of each other and the hesitation to initiate solution-oriented steps that would cost them make sense. While the need for security remains paramount, cyber operations, both defensive and offensive, can significantly contribute to this goal. Nevertheless, the logic of the security dilemma highlights how misinterpretations of cyber capabilities can lead to undesirable outcomes for all state actors. As cybersecurity technology advances and computer networks grow more extensive and potent, the dangers posed by the dilemma, which are very real already in the status quo, will only intensify.

Bibliography

Amalarethinam, George & Leena, H.M. (2017). *Enhanced RSA Algorithm with Varying Key Sizes for Data Security in Cloud*. 2017 World Congress on Computing and Communication Technologies (WCCCT). PP: 172-175. DOI: 10.1109/WCCCT.2016.50

Baezner, Marie & Robin, Patrice. (2018). *Hotspot Analysis: Stuxnet*. Center for Security Studies (CSS), ETH Zürich. PP: 1

Bhandari., P. (2020). *Data Collection: Definition, Methods & Examples*. Scribbr (blog).

Bowen, Glenn. (2009). Document Analysis as a Qualitative Research Method. Qualitative Research Journal. 9. PP: 27-40. DOI: 10.3316/QRJ0902027

Brantly, Aaron. (2018). *The cyber deterrence problem*. 10th International Conference on Cyber Conflict (CYCON). PP: 31-54. DOI: 10.23919/CYCON.2018.8405009

Buchanan, Ben. (2017). *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. Oxford Academic. DOI: 10.1093/9780190665012.001.0001

Carter, N., Bryant-Lukosius, A., DiCenso, A., Blythe, J., Neville, AN. (2014). *The use of triangulation in qualitative research*. Oncology Nursing Forum. 41 (5). PP: 545-547

Cerny, Philip. (2000). *The New Security Dilemma: divisibility, defection and disorder in the global era*. Review of International Studies. 26. PP: 623–646. DOI: 10.1017/S0260210500006239

Chin, Yik Chan & Li, Ke. (2021). *A Comparative analysis of Cyber Sovereignty Policies in China and the EU*. The 49th Annual Research Conference on Communications, Information, and Internet Policy.

Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative, And Mixed Methods Approaches*. Sage Publications, Inc. PP: 3

Cybersecurity Insiders. (2019). *2019 Cloud Security Report (ISC)2*. Cybersecurity Insiders [Web]

Hertz, John. (1950). *Idealist Internationalism and the Security Dilemma*. World Politics. 3:2, 157–80. DOI: 10.2307/2009187

Jenkins, Ryan. (2016). *Cyberwarfare as Ideal War*. Binary Bullets. PP: 89-114

Jervis, Robert. (1985). *From Balance to Concert: A Study of International Security Cooperation*. World Politics. 38 (1). PPS 69

Kabir., S. (2018). *Methods of Data Collection. Basic Guidelines for Research: An Introductory Approach for All Disciplines*. Book Zone Publication. PP: 201-276. DOI: 10.5281/zenodo.5814115

Lancelot, Jonathan. (2020). *Cyber-diplomacy: cyberwarfare and the rules of engagement*. Journal of Cyber Security Technology. 4. PP: 1-15. DOI: 10.1080/23742917.2020.1798155.

Melzer, Nils. (2011). *Cyberwarfare and International Law*. UNIDIR Resources: Ideas for Peace. United Nations. Charter of the United Nations. UN Secretariat. 1 UNTS XVI

Napanda, Shah, Kurup. (2015). Artificial Intelligence Techniques for Network Intrusion Detection. International Journal of Engineering Research & Technology. 4 (11). DOI: http://dx.doi.org/10.17577/IJERTV4IS110283

Otta, Soumya; Panda, Subhrakanta; Gupta, Maanak; Hota, Chittaranjan. (2023). *A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure*. Future Internet. 15. PP: 146. DOI: 10.3390/fi15040146

Paddeu, Federica. (2020). *Origins of the Right of Self-defence in International Law: From the Caroline Incident to the United Nations Charter, written by Tadashi Mori*. Journal of the History of International Law. 22. PP: 595-600. DOI: 10.1163/15718050-12340175

Radware. (2018). *2018-2019 Global Application and Network Security Report*. Radware [Web]

Rollins, John W; Lawrence, Susan V; Rennack, Dianne E; Theohary, Catherine A. (2015). *U.S.-China Cyber Agreement*. University of North Texas Libraries

Salminen, Mirva; Kerttunen, Mika. (2020). *The Becoming of Cyber-Military Capabilities*. Routledge Handbook of International Cybersecurity. PP: 94-10

Singer, P.W; Friedman, Allan. (2013). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Tait, Adam P. (2005). *The Legal War: A Justification for Military Action in Iraq*. Gonzaga Journal of International Law. PP: 96

Tang, Shiping. (2009). *The Security Dilemma: A Conceptual Analysis*. Security Studies. 18:3, 587-623. DOI: 10.1080/09636410903133050

Tripathi, Nikhil; Mehtre, B.M. (2013). *DoS and DDoS Attacks: Impact, Analysis and Countermeasures*. Institute for Development and Research in Banking Technology.

PP: 1

Viganò, Eleonora. Loi, Michele. Yaghmaei, Emad. (2019). *Cybersecurity of Critical Infrastructure (The Ethics of Cybersecurity)*. Springer. DOI: 10.1007/978-3-030-29053-5_8

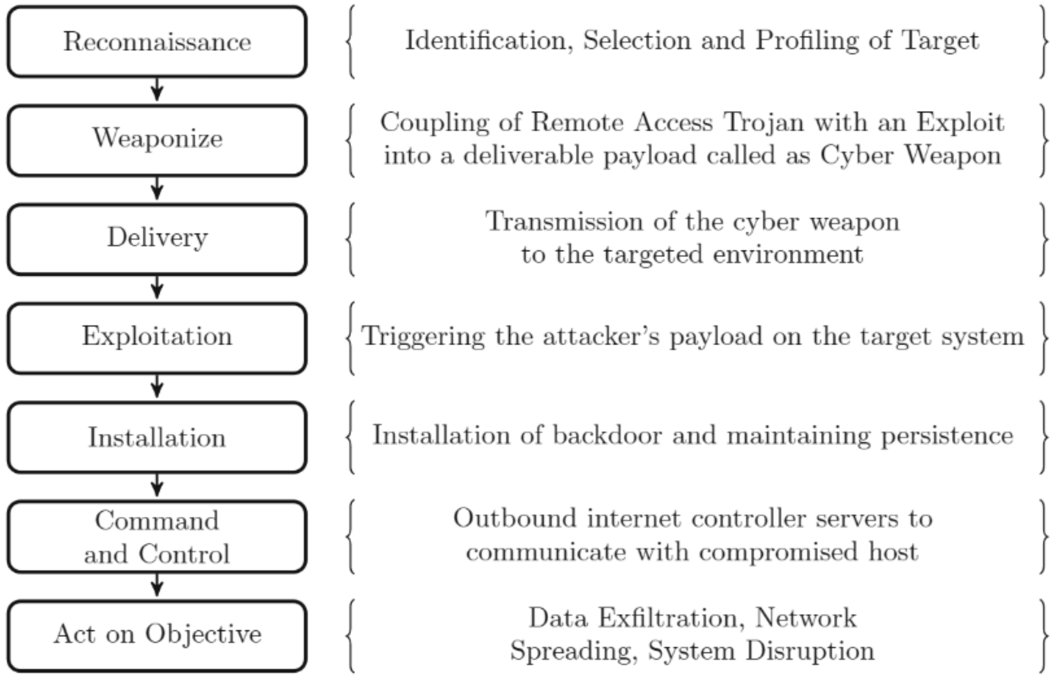
Waltz, Kenneth. (1979). *Theory of International Politics*. Addison-Wesley.

Wijayarathne, Senesh. (2022). *Trojan Horse Malware - Case Study*. Sri Lanka Institute of Information Technology.

Yadav, Tarun; Rao, Arvind. (2015). *Technical Aspects of Cyber Kill Chain*. Defence Research and Development Organisation, New Delhi, India. DOI: 10.1007/978-3-319-22915-7_40

Appendices

Appendix A: Figures


Reconnaissance
Identification, Selection and Profiling of Target
Weaponize
Coupling of Remote Access Trojan with an Exploit into a deliverable payload called as Cyber Weapon
Delivery
Transmission of the cyber weapon to the targeted environment
Exploitation
Triggering the attacker's payload on the target system
Installation
Installation of backdoor and maintaining persistence
Command and Control
Outbound internet controller servers to communicate with compromised host
Act on Objective
Data Exfiltration, Network Spreading, System Disruption

Note: An image illustrating step-by-step the order of a cyber kill chain i.e., the approach followed by a threat actor to execute a cyber attack. Accessed from

Yadav, Tarun; Rao, Arvind. Technical Aspects of Cyber Kill Chain. Defence Research and Development Organisation, New Delhi, India (2015).
DOI: 10.1007/978-3-319-22915-7_40