A Theory of Offensive Cyberspace Operations and Its Policy and Strategy Implications

Gazmend Huskaj[1,2], Fredrik Blix[1] and Stefan Axelsson[1]
[1]Department of Computer and Systems Sciences, Stockholm University, Kista, Sweden
[2]Geneva Centre for Security Policy (GCSP), Geneva, Switzerland

g.huskaj@gcsp.ch
blix@dsv.su.se
stefan.axelsson@dsv.su.se

Abstract: The significance of Offensive Cyberspace Operations (OCO) in cyber warfare and national security is increasingly recognised, yet academic literature lacks a dedicated theoretical framework to fully articulate its unique aspects and strategic dimensions. Traditionally enveloped within the broader context of information warfare, OCO's distinct characteristics have often been overlooked. Addressing this gap, our paper aims to delineate the specificities of OCO and establish a structured conceptual model that enhances understanding and operational clarity. To achieve this, the study adopts an interpretive approach, drawing from existing literature on information warfare and cyberspace, alongside official U.S. government and military publications on cyberspace operations. Employing the theory-building method, we focus primarily on conceptualization. This involves creating a coherent conceptual framework through abstraction, synthesis, and diagramming, informed by seminal works in the field. Among the paper's key contributions are detailed conceptual models that shed light on OCO's integration within the broader cyber domain, the influence of U.S. policy and strategy on OCO, and the critical triad for successful operations: access, vulnerabilities, and payloads. Furthermore, we elucidate the primary and secondary components of OCO, specifically cyberspace attack and exploitation, offering new insights into their roles and implications. Thus, the framework includes conceptual maps highlighting OCO's key elements, relationships, and challenges, aiming to advance academic discourse, practical strategies, and policy in cyberspace operations. This effort marks a significant step forward in both theoretical engagement and practical application within the field.

Keywords: Cyberspace Attack; Cyberspace Exploitation; Offensive Cyberspace Operations; Policy and Strategy.

1. Introduction

Offensive cyberspace operations (OCO) are now a part of modern warfare (e.g., Nakasone, 2022, 2023; Sky News, 2024; Jensen & Watts, 2023; Leyden, 2022). Research on cyberspace operations began to gain traction in 2006. Specifically, Jane's Defence Weekly discussed the US Air Force's intent in their October issue to "create and recognize a cyber-warfare command for cyberspace operations" (JDF, 2006). To understand the etymology, the term cyberspace originated from William Gibson's 1982 book "Burning Chrome" (Dictionary.com, 2019). The word 'cyber' descends from Cybernetics, and was coined by Norbert Wiener in his book with the same title in 1948 (Hardesty, 2011). By 1961, the word 'cyber' combined with other terms appeared first in the Wall Street Journal, leading to combinations such as "cyber warfare," "cyber security," "cyber operations" (Dictionary.com, 2019). However, not as much can be said about OCO. How can we develop a comprehensive and theory of OCO that accounts for their technical, policy, and social dimensions?

The authors acknowledge the contributions of existing theories on information warfare (e.g., Denning, 1999) and cyberspace (e.g., Caton & Bartholomees, 2012), but note that they are not focused on OCO. Therefore, the authors have developed a theory for this topic, drawing on the insights of Denning & Denning (2010), JCS (2018), and Lin (2009). Before introducing this theory, brief definitions of cyber warfare and cyberspace are provided. RAND Corporation (n.d.) defines cyber warfare as "the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks." The definition explicitly refers to actions by nation-states that involve attacking and attempting another nation's computers or information networks. In this research, cyber warfare is considered a subset of OCO, which encompasses a broader set of activities.

Cyberspace is defined as "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (JCS, 2018, p. GL-4). Cyberspace operations (CO) on the other hand are defined as "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace" (JCS, 2018, p. vii). Offensive cyberspace operations (OCO) are defined as "Missions intended to project power in and through cyberspace" (JCS, 2018, p. GL-5). Based on these definitions, it may be inferred that OCO are military missions that employ cyberspace capabilities in a very complex man-made technological domain.

This research begins by describing what theory is and how it is developed in applied disciplines. It does so by reviewing what previous researchers have contributed to scholarly research on the topic. Next, the concept of *conceptualisation*, one of five phases in the theory-building process, is described. Its application is done on the reviewed literature on Denning's (1999) "information warfare theory", Lin's (2009) work on "Lifting the veil on cyber offense", Denning & Denning (2010) "The profession of it discussing cyber attack.", and JCS (2018) "Joint Publication 3-12 Cyberspace Operations". Section 3 presents the methodological considerations and Section 4 presents the results of the conceptualisation. The contribution of this paper are the conceptual maps, which in sum, represent a theory of offensive cyberspace operations. Section 5 presents the theory's policy and strategy implications and concludes in Section 6.

2. What is Theory and How is it Developed in Applied Disciplines?

The concept of theory is not universally agreed upon by scholars, but it generally involves a system of statements, constructs, and relationships that explain or describe a phenomenon (Gregor, 2006). Theory can be represented in various ways, such as words, diagrams, or mathematical terms, and it can have different purposes, such as causal explanation, hypothesis testing, or prescription (Gregor, 2006). Theory can also be distinguished from data, facts, or variables, which are not theory but may form the basis of theory (Saunders et al., 2016; Sutton & Staw, 1995; Whetten, 1989). Theory can be as simple as a set of sentences (Simon and Newell, 1956) or as complex as a symbolic construction (Kaplan, 1964). Theory can also prevent the observer from being dazzled by the full-blown complexity of natural or concrete events (Hall and Lindzey, 1957). According to Dubin (1978, p. 26), "a theory tries to make sense out of the observable world by ordering the relationships among elements that constitute the theorist's focus of attention in the real world". One way to order the relationships among the elements constituting the theorist's focus is conceptualisation (Swanson and Chermack, 2013).

In their *General Method of Theory Building in Applied Disciplines*, Swanson & Chermack (2013) state that Conceptualisation, one of five phases in the theory-building process, is about constructing a coherent and rigorous conceptual framework: crucial for theory building. The theoretical conceptual framework represents the central descriptive capability inherent in any theory. Thus, theory is a system of statements, constructs, and relationships that explain or describe a phenomenon, but it is not necessarily a universal or objective truth. Theory can have different forms, functions, and scopes, depending on the researcher's perspective, purpose, and context. Theory can also be influenced by the data, facts, and variables that are available and relevant to the research problem. However, theory is not necessarily a final or definitive answer, but a tentative and provisional one, that can be challenged, modified, or extended by further research. Through the process of conceptualisation, a framework can be developed that represents the core inherent in any theory.

3. Methodological Approach

This study adopts an interpretive approach (Oates, 2005) to develop a theory of offensive cyberspace operations (OCO). Interpretivism suggests that our understanding of offensive cyber operations is shaped by exploring the subjective meanings and motives in human interactions with computer systems. The main sources of data are the existing literature on information warfare and cyberspace, as well as the official documents and publications of the U.S. government and military on cyberspace operations. The study follows the general method of theory building in applied disciplines proposed by Swanson and Chermack (2013), which consists of five phases: problem identification, conceptualisation, operationalisation, testing, and refinement. This paper focuses on the second phase, conceptualisation, which involves constructing a coherent and rigorous conceptual framework that represents the core descriptive capability inherent in any theory. The conceptual framework is developed through a process of abstraction, synthesis, and diagramming, based on the insights of Denning and Denning (2010), JCS (2018), and Lin (2009). The resulting framework consists of several conceptual maps that depict the essential elements, relationships, and challenges of OCO, as well as its policy and strategy implications. The framework is intended to provide a comprehensive and detailed understanding of OCO. The limitations of the theory and research lies because the paper is based on a limited number of sources, and mainly from a U.S. perspective, which may not represent the full complexity and diversity of OCO.

4. Analysis – A High Level Conceptualisation of Offensive Cyberspace Operations Theory

This section presents the conceptual maps as part of the theory, which are akin to network diagrams. These diagrams are created through a process of abstraction, synthesis, and diagramming, informed by seminal works in the field. The placement of concepts within these diagrams is determined by their interconnectedness and

relevance to the theory of offensive cyberspace operations. The diagrams illustrate the key elements, relationships, and challenges of OCO. The purpose of these diagrams is to provide a visual representation of the theory, enhancing understanding of OCO's integration within the broader cyber domain and its policy and strategy implications. Figure 1 as an integral part of the theory, presents a high-level conceptualisation describing OCO and its interconnectedness with the cyber domain. Figure 1 is the results of conceptualisation applied on the seminal works of Denning (1999), Lin (1999), Denning & Denning (2010), and JCS (2018).

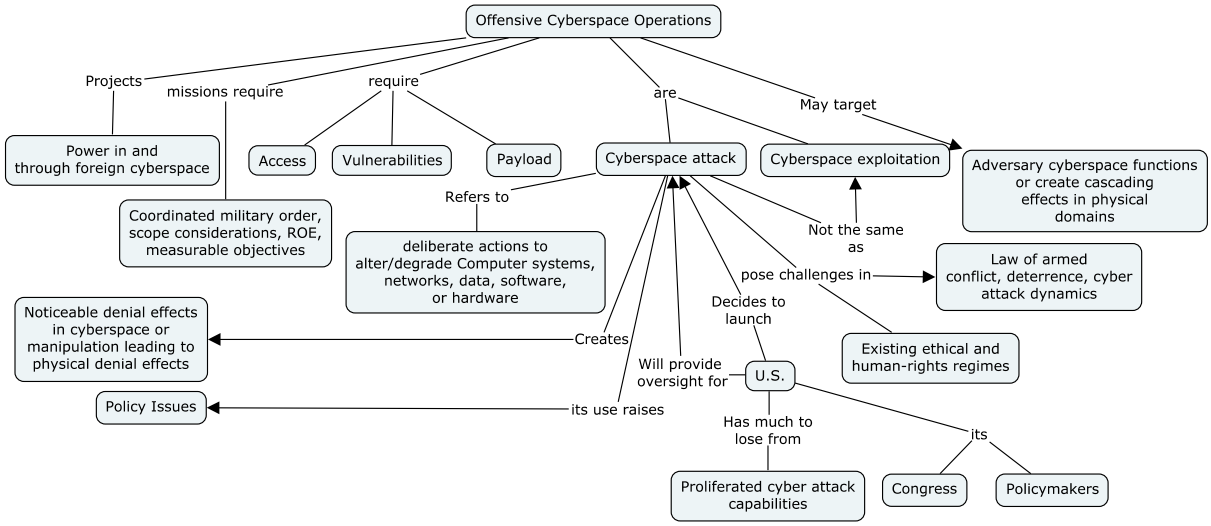

Figure 1: High Level Conceptualisation of Offensive Cyberspace Operations Theory.

This conceptualisation describes what offensive cyberspace operations are, what is required to conduct them, and potential challenges. Following this overview, the section will present and describe detailed conceptualisations to provide a comprehensive understanding of each component that forms this theory. The descriptions are done in a sequential manner that traces the connections from one concept to the next, as they appear in the diagram.

Describing the conceptualisation in Figure 1, Offensive cyberspace operations (OCO) project power in and through foreign cyberspace. Successful OCOs require three elements: access to the target, identification of a vulnerability within that target, and a payload designed to exploit said vulnerability.

These operations manifest in two primary ways: cyberspace attacks and cyberspace exploitation (more under *4.4 Cyberspace Exploitation – A Secondary Component of Offensive Cyberspace Operations*). These two are distinct, with cyberspace exploitation differing from Cyberspace attack. The concept of cyberspace attack is characterised by deliberate actions that alter or degrade computer systems, networks, data, software or hardware. Through such attacks, one can achieve noticeable denial effects in cyberspace or manipulation effects producing physical denial effects in the real world.

However, the execution of OCOs is not without complexities. The deployment and oversight of these operations raise policy issues. This is where governmental policymakers, exemplified in Figure 1 by the U.S. Government, come into play, setting policy directives and strategies for their use. It is crucial to recognise that governments, while developing and having access to these capabilities, also stand to lose significantly from the proliferation of cyber attack capabilities, tools, tactics, techniques and procedures. Finally, OCOs, specifically the component of cyberspace attack, while being a tool of national power, also introduces challenges. They span from understanding and interpreting the law of armed conflict in cyberspace, deterrence and how to deter cyber threats to understanding the dynamics of cyber attacks.

As the reader may note, conducting offensive cyberspace operations is complex, and requires (amongst other things) technical expertise, ethical, and strategic considerations. While the high-level conceptualisation provides a comprehensive overview of OCO and their interconnectedness, the next part of the theory is to go down one level, Level 2, the presents and describes specific areas in more detail. The next area crucial for OCO, is policy.

4.1 U.S. Policy Directing the use of Offensive Cyberspace Operations

This step discusses the importance of policy. Figure 2 presents a conceptualisation of U.S. policy and strategy. This is level 2, a more detailed conceptualisation than Level 1 in Figure 1. This section focuses on presenting and describing the relationships between policy directives, their implications, and how they drive OCO.

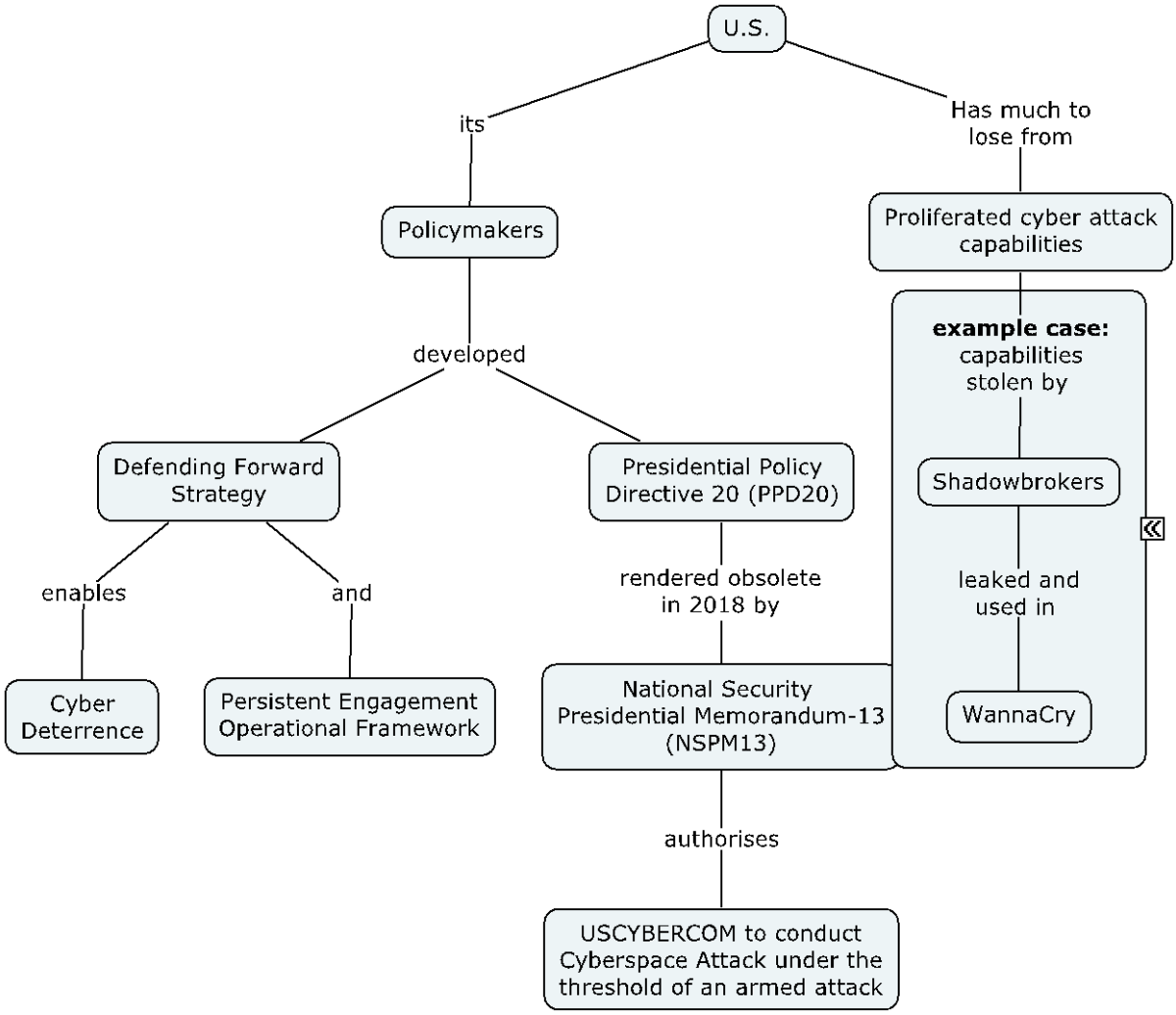

Figure 2: Conceptualisation of U.S. Policy Directing the use of Offensive Cyberspace Operations.

The conceptualisation of policy, exemplified by U.S. policymakers, begins with setting a policy on offensive cyberspace operations. The U.S., as depicted in Figure 2, while being technologically advanced, has also a lot to lose from the proliferation of cyber attack capabilities. Starting from the directive and memorandum developed by policymakers, shows the importance of having policy in place. Firstly, Presidential Policy Directive 20 (PPD20) was developed. This directive treated offensive cyberspace operations like any other tool of national power, mandating that operations with potentially significant consequences, such as leading to human death, required the president's approval. However, as time progressed and likely U.S. policymakers became more certain with OCO, PPD20 was later rendered obsolete by the National Security Presidential Memorandum 13 (NSPM13). NSPM13 provides more operational freedom, allowing the head of USCYBERCOM to conduct offensive cyberspace operations under the threshold of an armed attack without risking generating significant consequences, like human death.

In parallel, policymakers developed the Defending Forward-strategy. This is a paradigm shift in the U.S. approach to cyber deterrence. Recognising the unique challenges in cyberspace, Fischerkeller (2017), (Healey, 2019), and Lewis (2020) realised that a traditional deterrence strategy does not work in cyberspace. Defend Forward changes USCYBERCOM from a defensive to a proactive stance. Instead of just reacting to cyber threats, under the new Persistent Engagement operational framework, USCBYERCOM can take the fight to the adversary's cyberspace.

Figure 2 describes that policies and strategies do not exist in isolation but can be linked to real world cases. The case of the Shadow Brokers highlights this (Fruhlinger, 2022). The Shadow Brokers, believed to be Russian-threat actor, stole alleged National Security Agency (NSA)-tools, and leaked them online. According to publicly available information (Hern & MacAskill, 2017), the North Korean threat actor Lazarus Group used the leaked tools to conduct a cyberspace attack with global repercussions: in particular, health-care sectors suffered the most from this attack. The attack came to a halt thanks to a built-in-kill-switch: the malware first checks if it finds the domain name "iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com" (Fruhlinger, 2022). If it is not found, then it continues its attack. If it is found, the attack stops. A then 22-year-old U.K. citizen named Marcus Hutchins found and registered the domain name, setting a global cyber attack to stop (Gibbs, 2017).

Describing the importance of policy, exemplified by U.S. government policies, directives and strategies, it becomes evident that it is important to know how they direct OCO. At the core of OCO is Cyberspace Attack (CA). Just as policy directs when and how OCO should be used as a tool of national power, the success of CA lies on a triad of essential elements: access, vulnerabilities and payloads. The next section presents and describes the importance of the elements essential for CA.

4.2 The Triad for Successful Offensive Cyberspace Operations: Access, Vulnerabilities & Payloads

Launching a Cyberspace Attack (CA) requires access, vulnerabilities, and payloads. As described in Figure 3, a successful CA requires these three elements. This is level 2, a more detailed conceptualisation than Level 1 in Figure 1.

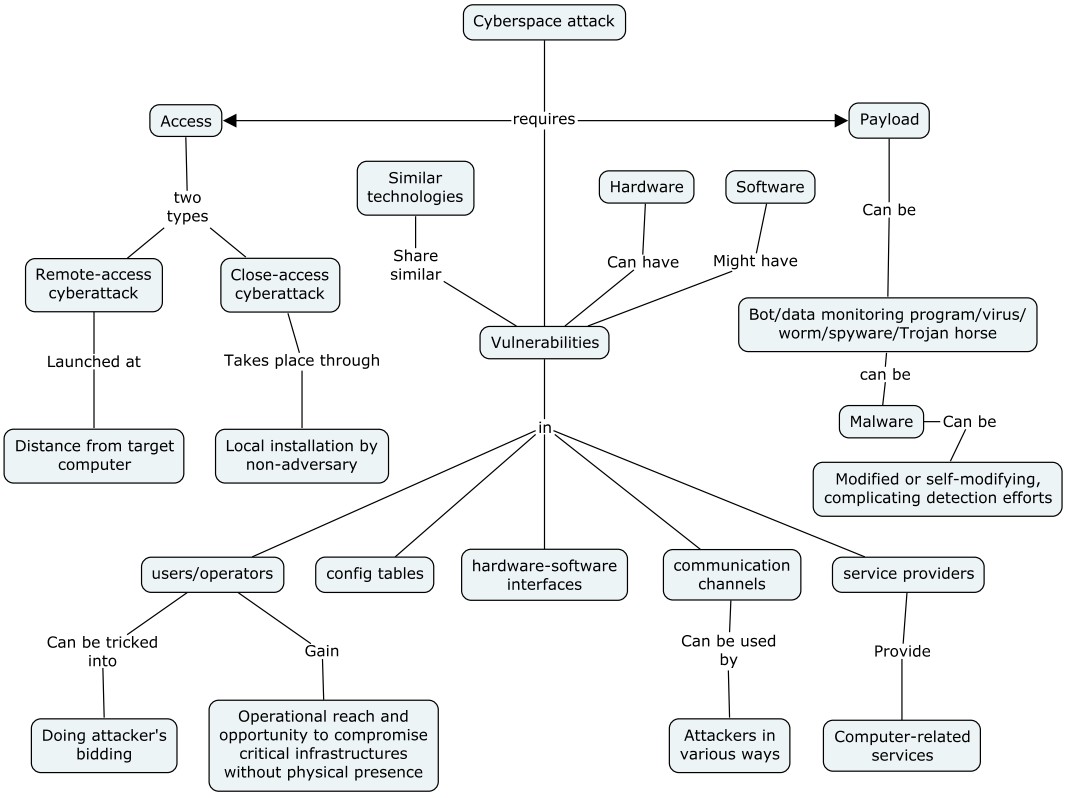

Figure 3: Conceptualising access, vulnerabilities and payload.

Access is crucial. It can be achieved in one of two ways: remote access or closed access. Remote access is launched from a distance, typically through the Internet, to its target computer. Close-access involves a local installation, such as a disgruntled employee. This method can escalate into an insider threat if the employee intentionally compromises the system's security.

Vulnerabilities (flaws, features or user errors) are the entry points an attacker exploits to gain entry. These vulnerabilities are not limited to just software or hardware. Even similar technologies may share similar vulnerabilities. These potential weaknesses can exist in users/operators, configuration tables, hardware-software interfaces, communication channels, and service providers offering computer and cloud-based

services. For example, Figure 3 presents how vulnerabilities in communication channels can be used by attackers in “various ways”, which include spear phishing or man-in-the-middle attacks.

Once an entry point (vulnerability) is identified, an attacker requires a payload (a tool) to exploit it. These payloads can take the shape of various forms: bots, and monitoring programs, viruses, worms, spyware, or Trojan Horses. Bots, derived from the term ‘robot’, denote a computer under the control of an external threat actor. Monitoring programs, viruses, worms, spyware, or Trojan Horses are different types of malicious software (malware) designed to infiltrate, damage, or exfiltrate data from the targeted system. Some of these, especially malware, can have traits like self-modification, further obfuscating their detection. Malware is an integral part of OCO, serving as a payload to exploit vulnerabilities. While malware is a distinct category, it operates in conjunction with other OCO elements like access and vulnerabilities. Malware, is not exclusively separate but is interconnected alongside bots and monitoring programs, forms the arsenal for cyberspace attacks and exploitation, working together to achieve the objectives of OCO.

In summary, the triad comprising access, vulnerabilities, and payloads forms the basis for successful CA. Therefore, it becomes even more important to present and describe Cyberspace Attack, a primary component of OCO.

4.3 Cyberspace Attack – A Primary Component of Offensive Cyberspace Operations

This section presents a conceptualisation of Cyberspace Attack (CA). This is level 2, a more detailed conceptualisation than Level 1 in Figure 1.

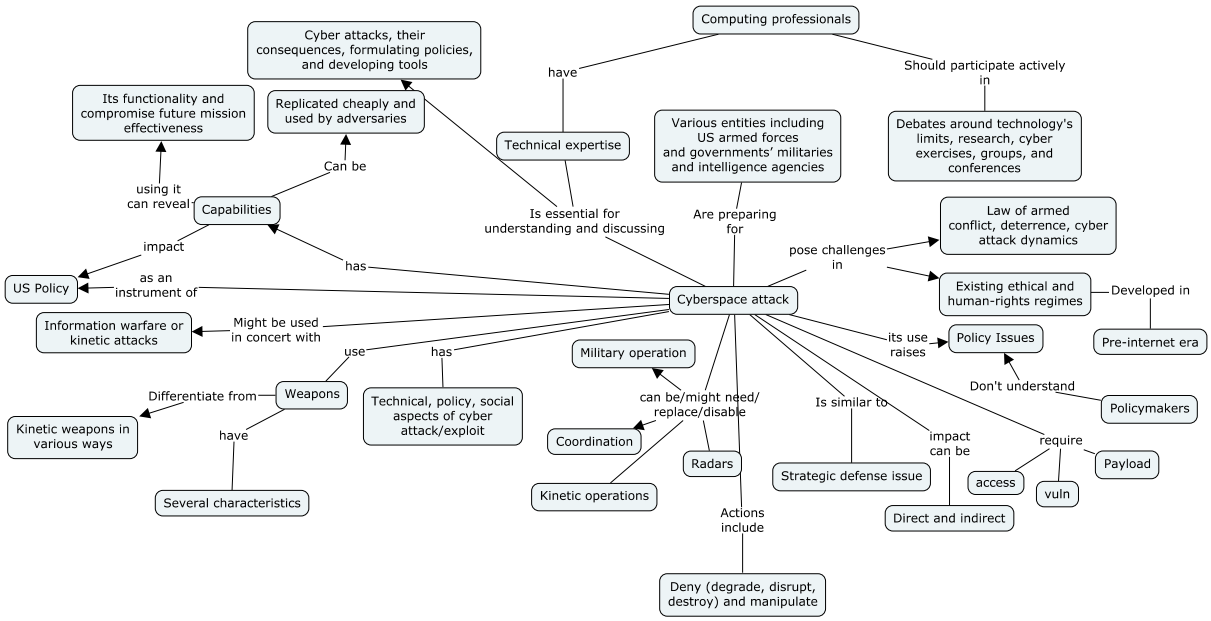

Figure 4: Conceptualising Cyberspace Attack.

Cyberspace Attack (CA) is crucial for OCO, as capabilities are crucial for CA. These capabilities, primarily computer code, are unique in that if used, they can reveal their functionality, risking compromising their future mission effectiveness. Furthermore, because they are code, these capabilities can be replicated cheaply and may be exploited by threat actors.

Technological expertise is essential for not only comprehending CA but also understanding its consequences, formulating policies, and developing tools. Hence, the role of computer professionals is emphasised for their active participation in debates around the limits of technology, engaging in cyber security research, and being part of cyber exercises, groups and conferences.

CA is linked to various policy domains, especially as a tool of national power. Organisations ranging from the U.S. Armed Forces to militaries around the globe and intelligence agencies are preparing for CA. However, since its introduction, it has raised policy challenges. Some policymakers have a challenge to grasp CA, indicating the need for clear policy, strategy, and directives that reflect current realities. Simultaneously, we must understand that some principles, like ethical and human-rights regimes, have been developed in the pre-Internet era.

One of CA's distinct features is its agility. It can function independently or generate synergies with information warfare or kinetic attacks. This capability presents itself as a national instrument in U.S. Policy. Its impact can be direct or indirect, lifting its importance to that of strategic defence issues. CA actions can be considered in a spectrum: from denying and degrading to disrupting, destroying, or manipulating targeted systems.

Furthermore, while CA is heavily based on technology, it has a vast area of operations. It has technical, policy, and social dimensions, presenting challenges to the law of armed conflict, deterrence, and the dynamics of cyber attack. It has distinct weaponry, with several characteristics setting it apart from traditional kinetic weapons.

Finally, CA can be integrated into military operations. It can complement or even replace kinetic operations in certain scenarios, like disabling radars. Executing CA may require coordination so as not to risk any other potential ongoing cyberspace operations.

In summary, CA is a complex component of offensive cyberspace operations. It poses challenges and opportunities, and it requires technical, policy, and social aspects to support it. Therefore, as CA is the primary component of OCO, it also requires support from its secondary component: Cyberspace Exploitation.

4.4 Cyberspace Exploitation – A Secondary Component of Offensive Cyberspace Operations

This section discusses Cyberspace Exploitation. Figure 5 presents a conceptualisation of Cyber Exploitation. This is level 2, a more detailed conceptualisation than Level 1 in Figure 1.

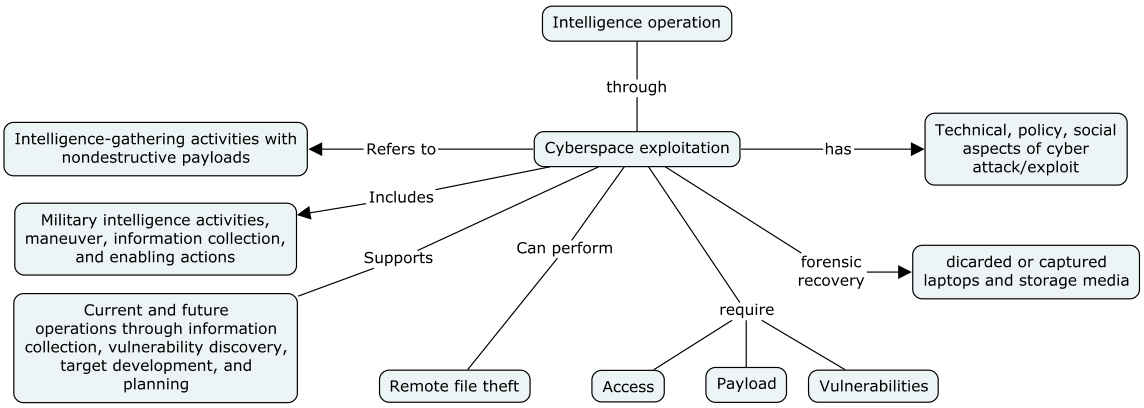

Figure 5: Conceptualisation of Cyberspace Exploitation.

Cyberspace Intelligence operations in cyberspace are executed through cyberspace exploitation (CE). CE are intelligence gathering activities with non-destructive payloads. This exploitation includes a range of activities, including military intelligence activities, manoeuvre through information collection, and enabling actions. It is essential to state that while at a first impression CE may appear "inferior" and "less complex" than CA, they are fundamentally identical in operation. The primary distinction lies in the objectives: CE aims to remain undetected over extended periods of time, emphasising the use of non-destructive payloads, ensuring a persistence in the target system. These efforts directly support current and future operations by the collection of information, discovering vulnerabilities, target development, and planning. Once an operator is inside a target, they have the capability to exfiltrate and conduct remote file theft. However, CE, just like its counterpart, Cyberspace Attack (CA), requires a base of Access, Payload and Vulnerabilities. Additionally, CE plays a role in the support of the forensic recovery of information from discarded or captured laptops and storage media. Just like CA, CE has implications for the technical, policy, and social dimensions of cyber attack and exploitation.

5. Discussion - The Theory's Policy and Strategy Implications

The comprehensive theory of offensive cyberspace operations, as described in Section 4, that accounts for their technical, policy, and social dimensions, is developed through *conceptualisation*. This represents one of the five phases in the theory-building methodology in applied disciplines. The theory describes a high level conceptualisation of offensive cyberspace operations. Additionally, it describes detailed conceptualisations of the importance of policy, the triad of access, vulnerabilities and payloads, cyberspace attack, and cyberspace exploitation.

We acknowledge the challenges in ensuring the exhaustiveness and accuracy of the conceptual framework. Continuous research and peer review are essential for validation. This conceptualisation serves as a base for academics, strategists, and policymakers to understand the complexities of OCO. It benefits those involved in the development and implementation of cyber strategies and policies, providing a structured approach to OCO. The deniability of cyber attacks does raise concerns about circumventing international laws. It is imperative for policymakers to ensure that operations are conducted within legal boundaries and for military leaders to enforce adherence among cyber operators. While there are inherent challenges in monitoring and enforcing compliance, especially with decentralised units, command structures and clear rules of engagement can mitigate risks.

Policymakers have early understood the opportunities provided using OCO as a tool of national power. Therefore, from a policy perspective, it is important to ensure that all OCO adhere to international law, are conducted under oversight and under the threshold of an armed attack, and do not risk generating significant consequences, such as human death. Presidential Policy Directive 20 is an example of a first policy for OCO, providing a framework for decision-makers and the actions that could be taken for the conduct of OCO. It is likely that as policymakers asked USCYBERCOM for courses of action to support U.S. policymakers in their policy-response options, USCYBERCOM in turn were tasked to conduct OCO. Over the years, as USCYBERCOM conducted OCO, it is very likely that the organisation become more mature through the experience generated by the conduct of OCO. This in turn is also likely to have led to policymakers becoming more confident in how to conduct OCO as a tool of national power. The evolution of U.S. policy from PPD20 to NSPM13 and the Defend Forward Strategy is an indicator of the maturity that US policymakers generated by what is believed to continuously asking USCYBERCOM for courses of actions to support U.S. policymakers in their policy-response options, and through OCO, generated enough experience and maturity.

The theory underscores the importance of policymakers comprehending the risks and technological aspects of cyberspace operations to make informed decisions. Figure 1 shows that OCO require access, vulnerabilities and payload, and that OCO are cyberspace attack (CA) and cyberspace exploitation (CE), while at the same time CA is not the same as CE. Using CA raises policy issues, and because CA require access, vulnerabilities and payload, this implies that policymakers must also have some understanding of technology. Furthermore, it suggests that they need to understand the ethical and legal implications of OCO in the context of the international law. With this understanding, policymakers can then develop policy that balances operational freedom and flexibility for organisations such as USCYBERCOM to conduct OCO, under oversight. NSPM13 is an example of a policy that offers more operational freedom to conduct OCO without risking significant consequences. The implication is that policymakers need to continuously monitor the technological development, adapt, and refine their policies that direct the use of OCO.

The theory emphasises that conducting OCO require an understanding of the technology dimension. Primarily, an understanding of the triad of access, vulnerabilities, and payloads, and the complexities and uncertainties inherent in these operations. Additionally, the theory describes the importance of computer professionals in developing, deploying, and maintaining OCO capabilities. While it may seem obvious that engineers are needed to develop capabilities, the theory aims to highlight the specific types of engineering expertise required for sophisticated cyberspace operations. Furthermore, the theory describes the importance of research, cyber exercises, and the participation of the same professionals in cyber groups and conferences. The theory does not state that the computer professionals must hold any form of university degrees, however, they need to have a high level of expertise, creativity, and innovation, as well as a sense of responsibility and ethics so the conduct of OCO fall within the developed policy as mentioned above.

The theory also distinguishes between two important components of OCO: cyberspace attack and cyberspace exploitation. While cyberspace attack is crucial for OCO to generate, for example, destructive effects on an adversarial target, cyberspace exploitation seeks instead to collect intelligence. Therefore, both components (CA and CE) are identical in operation but the effects and objectives of the operations differ. Thus, military commanders and their policymakers need to have a clear understanding of the target, the target's cyberspace and cyber environment, the mission, and the desired end state, or outcome. Additionally, it is crucial to understand the likelihood of collateral damage (secondary, tertiary effects), potential escalation, and attribution, in order to conduct OCO responsibly, within international law (= under the threshold of an armed attack), and proportionally.

The theory has implications for the social dimension. Although the targets are technological in nature, such as interconnected networked information systems, these systems are generally a node in a bigger system. These systems, critical infrastructure, can be the political, military, economic, social, and electoral systems.

Therefore, through the conduct of OCO, it is possible to influence public perception and awareness through disinformation by exploiting vulnerabilities inherent in living in a highly digitalised society. It is also possible to undermine societal trust in government institutions and impact the integrity of democratic processes. This in turn can lead to societal divisions and weakening national cohesion. Additionally, through OCO, it is possible to impact private companies, industry, academia and more. Examples include corporate espionage and theft of intellectual property by targeting vulnerabilities in supply chains, leading to reputational risks, shifts in market dynamics and competition, impacting not only the security of the companies, industry and academia, but also the economic and national security of a State.

In summary, the theory suggests that OCO stakeholders need to have a holistic and systems multidisciplinary and multilevel approach on OCO. From the technical, policy, and societal dimensions to the national, global and organisational levels. It is imperative that stakeholders collaborate and communicate on all domains and levels, vertically and horizontally, in order to conduct OCO as a tool of national power.

6. Conclusions & Future Research

The paper presents a comprehensive theory of offensive cyberspace operations, which are military missions that employ cyberspace capabilities to project power in and through foreign cyberspace. The theory was developed through conceptualisation, one of five the five phases in the theory-building methodology in applied disciplines, by reviewing previous research based on the works of Lin (2009), Denning & Denning (2010), and JCS (2018). The paper also discusses the policy and strategy implications of OCO by focusing on the role of U.S. government policies and strategies, which have shaped the conduct of OCO. Furthermore, the paper also examines the importance of a technical understanding, requirements and challenges, of OCO, specifically of cyberspace attack, cyberspace exploitation, and the triad of access, vulnerabilities and payloads.

The paper contributes to theory and practice by providing understanding and how OCO are conducted, as well as offering practical insights into the role of policymakers for policy development. Furthermore, it contributes to the scientific literature by offering a unified and comprehensive theory of OCO. Finally, the paper also bridges the gap between academics and practitioners, and technology and policy, by interpreting the empirical evidence.

Future areas of research can explore different contexts, such as regions, actors, and domains, employ other methodologies like simulations, experiments, and surveys, or address additional unanswered questions within deterrence, escalation, and conflict resolution. Future research can also support policy by informing policy development, and strategy development, through the collection of empirical evidence from human sources.

References

Caton, J. L., & Bartholomees, J. B. (2012). ON THE THEORY OF CYBERSPACE (VOLUME I:, pp. 325–344). Strategic Studies Institute, US Army War College; JSTOR. http://www.jstor.org/stable/resrep12116.26

Denning, D. E. (1999). Information Warfare. https://is.theorizeit.org/wiki/Information_warfare

Denning, P. J., & Denning, D. E. (2010). The profession of it discussing cyber attack. Communications of the ACM, 53(9), 29–31. https://doi.org/10.1145/1810891.1810904

Dictionary.com. (2019). The Origin Of Cyber Monday's Name Is From The 1940s. https://www.dictionary.com/e/cyber-monday-cyberspace/

Fischerkeller, M. (2017). Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies. Survival, 59(1), 103–134. https://doi.org/10.1080/00396338.2017.1282679

Hardesty, L. (2011). Norbert Wiener's earlier work may prove more important. https://phys.org/news/2011-01-norbert-wiener-earlier-important.html

Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. Journal of Cybersecurity, 5(1), 1–15. https://doi.org/10.1093/cybsec/tyz008

Jensen, E. T., & Watts, S. (2023). Pressing questions: Offensive cyber operations and NATO strategy. Modern War Institute. Retrieved from: https://mwi.westpoint.edu/pressing-questions-offensive-cyber-operations-and-nato-strategy/.

Joint Chiefs of Staff. (2018). Joint Publication 3-12 Cyberspace Operations (Issue June 2018, pp. 1–104).

Leyden, J. (2022). NSA general confirms US offensive cyber ops in Ukraine war. The Register. Retrieved from: https://www.theregister.com/2022/06/02/nakasone_us_hacking_russia/.

Lin, H. (2009). Lifting the veil on cyber offense. IEEE Security and Privacy, 7(4), 15–21. https://doi.org/10.1109/MSP.2009.96.

Nakasone, P. M. (2022). The evolution of cyber defense and deterrence. Joint Force Quarterly, 92, 6-113.

Nakasone, P. M. (2023). 2023 posture statement of General Paul M. Nakasone. U.S. Cyber Command. Retrieved from: https://www.cybercom.mil/Media/News/Article/3320195/2023-posture-statement-of-general-paul-m-nakasone/.

Oates, B. J. (2005). Researching Information Systems and Computing (First). Sage Publications, Inc.

RAND Corporation. (n.d.) Cyber Warfare. Retrieved from: https://www.rand.org/topics/cyber-warfare.html.
Sky News. (2024). US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command. Retrieved from: https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139.
Swanson, R. A., & Chermack, T. J. (2013). Theory Building in Applied Disciplines. Berrett-Koehler Publishers, Inc.
USAF to create cyber-warfare command. (2006). Jane's Defence Weekly. www.scopus.com