National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Conceptualising Cyber Warfare: Warfare Theory, Contemporary Examples, and Future Concepts

Major Justin D. Tomlinson, ADF

JCSP 50

Exercise Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI n° 50

Exercice Solo Flight

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 50 - PCEMI n° 50
2023 - 2024

Exercise Solo Flight – Exercice Solo Flight

Conceptualising Cyber Warfare: Warfare Theory, Contemporary Examples, and Future Concepts

Major Justin D. Tomlinson, ADF

INTRODUCTION

Clausewitz describes war as a duel on a large scale, akin to a pair of wrestlers attempting to compel the other to their will through physical force.[1] This wrestling match is occurring today in numerous theatres of war, from the trenches of the Russia-Ukraine conflict to urban fighting amongst the civil populace in the Gaza Strip. The struggle between various state and non-state actors in the cyber domain is less visible but similarly vigorous. Cyberspace's rising importance has necessitated its new status as the fifth warfighting domain, complementing land, sea, air, and space.[2] Operations in the cyber domain are proving critical in modern operations and will form a crucial part of the future battlespace. They must be integrated with actions in the other four domains in a multi-domain sense to maximise success and win wars. Understanding the parallels between cyber warfare and the ideas set out by the foundational military theorists and inherent within the Principles of War is essential in designing offensive cyber operations and defending friendly cyberspace. In demonstrating this, this paper will first describe classical theory and theorists to provide a foundation for analysis and comparison. Secondly, the cyber domain will be broadly outlined. Next, an analysis of offensive cyberspace operation case studies focused on Russian cyber attacks against Estonia, Georgia, and Ukraine, Chinese cyber capabilities, and the Stuxnet virus will highlight commonalities and linkages to military theory. Lastly, cyber defence, legal considerations, and deterrence will be discussed, along with a consideration of the cyber domain's role in multi-domain operations.

WARFARE

Critical lessons from the most prominent traditional warfare theorists will be distilled and used as a framework to aid the analysis of cyber warfare. In *On War*, Clausewitz focuses on the violent clash of opposing forces as an extension of politics by other means.[3] He taught that war must be fought with a clear objective and that objective must shape all military actions. Sun Tzu's theory of warfare is much broader, with diplomacy and war as part of a spectrum of political competition.[4] Jomini's theory of warfare is more specific and tactical. He offers a principle of war in four parts. To simplify, this theory suggests that to be successful in warfare, an Army should be massed at a decisive point, at the right time, to deal a decisive blow against the enemy.[5] Douhet's air power theories were formulated during the First World War. He suggested that nations needed an "offensive-minded air force, constructed in peacetime and available at the outset of conflict to win wars quickly and decisively."[6] His theories were challenged in the Second World War, primarily due to the development of air defence capabilities,

---

[1] Carl von Clausewitz et al., *On War*, Unabridg ed. (Ashland, Or.: Blackstone Audio, 2008). p75

[2] Sean Brandes, "The Newest Warfighting Domain: Cyberspace," *Synesis: A J.Sci., Technol., Ethics, Policy* 4 (2013), p90.

[3] Clausewitz, *On War* p75-76.

[4] Robert E. Neilson and National Defense University. Institute for National Strategic Studies, *Sun Tzu and the Art of War in Information Warfare* (Washington, DC: National Defence University, 1997).

[5] de Jomini Baron, *The Art of War* (New York: Start Publishing LLC, 2013).

[6] Phil Haun, "Winged Victory: How the Great War Ended: The Evolution of Giulio Douhet's Theory of Strategic Bombing," *War in History* 29, no. 3 (2022), p584.

including the radar. With the arrival of the nuclear bomb, the air domain became a critical component of deterrence. Mahan and Corbett are sea power theorists. Mahan discusses the importance of sea power at the strategic and political levels, noting the importance of a free and open sea for trade and the implications for a nation politically and militarily.[7] Corbett focuses on sea power as a means to maintain command of the sea. He notes the object of naval warfare is to gain command of the sea directly or indirectly, or to prevent the enemy from securing it. Importantly, he also notes that, for the most part, the sea remains uncommanded.[8]

These theorists shaped modern understanding of warfare and will be a valuable tool for analysing the concept of cyber warfare. The Principles of War listed below will also be applied to assist in understanding cyber warfare.

Table 1 – ADF Principles of War

Selection and Maintenance of the Aim	Offensive Action
Concentration of Force	Surprise
Cooperation	Flexibility
Economy of Effort	Sustainment
Security	Maintenance of Morale

Australian Army, "Land Warfare Doctrine 3-0-3, Formation Tactics," (14 Nov 2016), p15.

Alternate theoretical warfare frameworks relevant to cyber operations include irregular warfare and special operations.[9] The ideas inherent in these two frameworks, of complexity, covert and clandestine operations, and relative superiority, are also good comparisons to cyber warfare.

THE CYBER DOMAIN

A domain is a "major part of the operational environment" with its own specific characteristics in which or through which military activity takes place.[10] The cyber domain comprises the "Internet of networked computers, but also intranets, cellular technologies, fiber optic cables, and space-based communications.". [11] Unlike traditional

---

[7] A. T. Mahan et al., *Mahan on Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan*, 1st Naval Institute Press pbk.; 1 ed. (Annapolis, Md: Naval Institute Press, 2015).
[8] Julian Stafford Corbett Sir, Inc OverDrive and OverDrive ebook, *Principles of Maritime Strategy*, 1st ed. (Mineola, NY: Dover Publications, 2004).
[9] Frank C. Sanchez, Weilun Lin and Kent Korunka, "Applying Irregular Warfare Principles to Cyber Warfare," *Joint Force Quarterly*, no. 92 (2019a), p15.
[10] Canada. Department of National Defence, "Pan-Domain Force Employment Concept: Prevailing in an Uncertain World," *Cjoc* (2023).
[11] R. Nicholas Burns et al., *Securing Cyberspace: A New Domain for National Security* (Washington, D.C: Aspen Institute, 2012) p22.

domains, the cyber domain is entirely human-made.[12] The advent of the cyber domain is comparable to that of air and space, with each domain rising out of new technologies (planes, satellites). Cyber warfare is "an extension of policy by actions taken in cyberspace by state actors (or non-state actors with state support) that constitutes a serious threat to another state's security, or an action of the same nature taken in response to a serious threat."[13] This definition aligns with Clausewitz's concept of war as an extension of politics by other means. Cyber capabilities can be offensive or defensive. These capabilities are crucial to modern warfare as part of the 'multi-domain operations' (MDO) concept. MDO seek to converge operations across all five domains to mass effects and generate dilemmas for enemy commanders.[14] Operations in the cyber domain occur across the spectrum of competition and conflict. An example of the spectrum of conflict is in Figure 1.

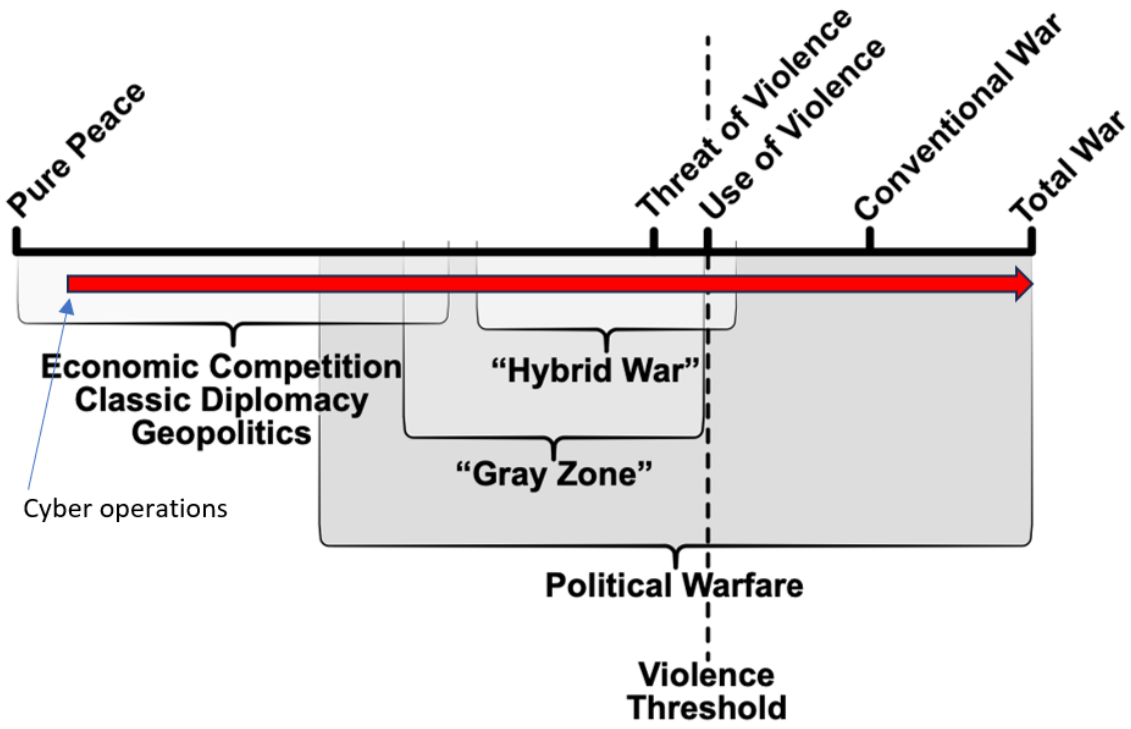

Figure 1: The conduct of cyber operations across the 'Spectrum of Competition'[15]

[12] Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Force Quarterly: JFQ*, no. 77 (2015), p8.
[13] James A. Green, *Cyber Warfare: A Multidisciplinary Analysis*, ed. James A. Green, 1st ed. (Abingdon, Oxon; New York, NY: Routledge, 2015) p8.
[14] Gen David G. Perkins, "Multi-Domain Battle," *Military Review* (2017) p7.
[15] United States Marine Corps, "MCDP 1-4 Competing," (2020).

OFFENSIVE CYBERSPACE OPERATIONS

Offensive Cyberspace Operations (OCO) involve "digitally affecting adversary systems and networks for a military goal or objective; affecting data by using data."[16] These operations are often split into computer network attack (CNA) and computer network exploitation (CNE).[17] This definition aligns with the Principle of War 'Offensive Action' and the Clausewitzian idea that military operations should have a clear objective. Like Douhet's description of Air Power, a nation with strong OCO capabilities will enter a new conflict with a considerable advantage over an adversary who has not yet developed that capability due to the time it takes to cultivate, like an offensive air platform. This has contributed to four out of the five Five Eyes intelligence community nations publicly acknowledging that their national communications intelligence organisations hold OCO capabilities.[18]

Russian activities against Estonia in 2007, Georgia in 2008, and Ukraine from 2014, and during and after the February 2022 invasion, have provided several lessons regarding the use of OCO by a state actor. Russia's OCO capabilities nest within its overarching strategic-level information operations.[19] During a two-week period in 2007, Estonia was subjected to a protracted and intense attack in the cyber domain, targeted at Estonia's information infrastructure. This is considered the first cyber attack against a country's national security.[20] The attack occurred in the context of historical tensions between ethnic Estonians and the country's Russian minority population. The trigger for the attack was the movement of a statue which commemorated the Russian liberation of Estonia from Nazi occupation. The statue was moved from a prominent location to a less prominent location.[21] In addition to rioting, this act triggered a cyber attack against Estonia. DDoS[22] cyber attacks targeting the country's critical national infrastructure "shut down the websites of all government ministries, two major banks, and several political parties. At one point, hackers even disabled the parliamentary email server."[23] This attack occurred below the threshold of traditional conflict. However, it did take full advantage of the Principle of War – Surprise. Since this type of attack had not been seen against a

---

[16] Herbert Lin et al., *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, ed. Herbert Lin and others , 1st ed. (Washington, D.C: Brookings Institution Press, 2019). p807-808.
[17] Kraig Hanson and ARMY WAR COLL CARLISLE BARRACKS PA, *Organization of DoD Computer Network Defense, Exploitation, and Attack Forces* US Army War College, 2009). p9.
[18] Josh Gold, "The Five Eyes and Offensive Cyber Capabilities: Building a 'cyber Deterrence Initiative'," *Tallinn, Estonia: NATO CCDCOE* (2020) p4.
[19] Marcus Willett, "The Cyber Dimension of the Russia–Ukraine War," in *Survival: October-November 2022*Routledge, 2023), p8.
[20] William C. Ashmore, "Impact of Alleged Russian Cyber Attacks," *Baltic Security & Defence Review* 11, no. 1 (2009), p1.
[21] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011), p50.
[22] "Distributed denial of service (DDoS) is a cyber attack that employs a series of computers to overwhelm the target with large amounts of traffic, suspending its ability to respond and effectively shutting it down." Eneken Tikk-Ringas and International Institute for Strategic Studies, *Evolution of the Cyber Domain: The Implications for National and Global Security*, ed. Eneken Tikk-Ringas, 1st ed. (Abingdon, Oxon; New York, NY: Routledge, for the International Institute for Strategic Studies, 2016) p8.
[23] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011), p51.

nation-state before, Estonia and the wider world were taken off guard, which increased the attack's effect on Estonia. This effect was made worse by Estonia's lack of 'Security' in the cyber domain, as well as Estonia's heavily digitised society.[24] Although these attacks were not coordinated with other domain effects in a formal MDO sense, the alignment with protests in the physical domain saw an increase in the dilemma posed to the Estonian government. A final observation to make about this particular attack is one of attribution, which will be further explored throughout this paper. Despite supportive evidence, this attack could not be formally attributed to Russia.[25] Given the open and complex nature of the internet and cyberspace, attributing attacks to a specific actor, especially a nation-state, is difficult.[26] This attribution complexity further exacerbates the inherent uncertainty in war and warfare.[27]

During the 2008 Russia-Georgia conflict, Russia coordinated offensive cyber effects with actions in other domains, including land, sea, and air. DDoS attacks took down Georgian infrastructure, affecting government communications. This included the "defacing (of) government websites."[28] "Banks, transportation companies, and private telecommunications providers were also attacked, disrupting services".[29] This coordinated attack demonstrated an ability and willingness for Russia to fully integrate its elements of national power in war with Georgia. Here, OCO contributed effectively to the principles of 'Offensive Action' and 'Cooperation'. This was considered the first attack in history to see OCO integrated with actions in the physical domains, an early example of MDO.[30] At the operational level, the conflict between Russia and Georgia was a victory for Russia as the manner in which Russia was able to integrate effects across the domains, including cyber, was highly effective. At a strategic level, the outcome of the conflict is considered to have favoured Russia, given they gained control of South Ossetia and Abkhazia.[31] In this conflict, Russia aligned its military strategy with its political goals. It massed its effects in a synchronised manner against decisive points, as Jomini taught. These acts in 2008 demonstrated how critical integrated cyber effects can be in the modern battlespace.

Russia commenced OCO against Ukraine almost a decade before its large-scale invasion in February 2022. In 2015, Russia used malware against Ukrainian electricity distribution companies to disrupt the supply of electricity to the Ukrainian population.[32]

---

[24] William C. Ashmore, "Impact of Alleged Russian Cyber Attacks," *Baltic Security & Defence Review* 11, no. 1 (2009), p5.
[25] Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective" p164.
[26] Frank C. Sanchez, Weilun Lin and Kent Korunka, "Applying Irregular Warfare Principles to Cyber Warfare," *Joint Force Quarterly*, no. 92 (2019b), p15.
[27] Clausewitz, *On War*
[28] Michael Connell, Sarah Vogler and CENTER FOR NAVAL ANALYSES ALEXANDRIA VA ALEXANDRIA United States, *Russia's Approach to Cyber Warfare*, 2016) p12.
[29] Michael Connell, Sarah Vogler and CENTER FOR NAVAL ANALYSES ALEXANDRIA VA ALEXANDRIA United States, *Russia's Approach to Cyber Warfare*, 2016), p12.
[30] David Hollis, "Cyberwar Case Study: Georgia 2008," (2011) p2.
[31] Lionel Beehner et al., "Analyzing the Russian Way of War: Evidence from the 2008 Conflict with Georgia," *Analyzing the Russian War of War: Evidence from the 2008 Conflict with Georgia* (2018) p32.
[32] Willett, "The Cyber Dimension of the Russia–Ukraine War," p9-10.

The cyber-attack targeted three separate power distribution centres and effectively shut down power to 220,000 Ukrainians.[33] This blend of political coercion fell in the grey zone at the threshold of conflict. It was a form of political pressure using OCO as a strategic effect. These attacks were akin to the special forces tactic of 'sabotage'; this form of cyber operation is a common tactic used by the Russian military.[34] Similar to Sun Tzu's teachings, Russia's actions blurred the lines between politics and military operations, with cyber and information operations central to this method.

The expectations of Russia's cyber operations capability before the country's special military operation incursion into Ukraine in February 2022 were very high. Bolstered by relative successes in Estonia, Georgia, and Ukraine before 2022, as well as Russia's own messaging. One prominent columnist wrote that the cyber component of Russia's anticipated invasion of Ukraine would "take down the power grid, turn the heat off in the middle of winter and shut down Ukrainian command centers."[35] The reality of the cyber component of Russia's military operation in 2022 was that it was not as catastrophic or damaging as the operations in the traditional domains. However, Russia did coordinate certain types of attacks. As an example, concurrent to the physical invasion, Russia conducted DDoS attacks against the Ukrainian government and business websites, which also involved the attempted planting of malware on Ukrainian computer systems.[36] These cyber operations were less effective than similar attacks in 2014-2015 because Ukraine learned from the earlier attacks and increased its cyber security and defensive measures.[37] Other OCO included attacks on tens of thousands of Ukrainian-based satellite modems, targeting civilian internet service providers, attempted targeting of StarLink terminals supporting Ukrainian operations, and cyber support for the broad Russian information operation campaign on social media and elsewhere.[38] This was a significant cyber operation in support of the overall Russian military operation. However, these operations did not prove decisive. There have been several reasons given for this relative lack of success. One is that their most successful cyber actions have been reserved for espionage and that those intrusions are not publicly known.[39] This is difficult to comment on, especially at an unclassified level. Another clearer reason is the increase in Ukraine's cyber resilience through increased cyber security and defence and learning from previous Russian attacks.[40] A further reason is a failure at the highest levels of the Russian military to fully integrate cyber operations successes with actions in the other domain.[41] Had the Russian military demonstrated a greater application of the Principles of War through more coordinated, 'massed' effects that maximised 'Offensive Action', used 'Economy of Effort', and aligned all domain effects towards a single aim in a MDO approach, they may have had more success. Like the advancement of air power in the

---

[33] Connell, *Russia's Approach to Cyber Warfare* p15.
[34] Connell, *Russia's Approach to Cyber Warfare*, p17.
[35] Herbert Lin, "Russian Cyber Operations in the Invasion of Ukraine," *The Cyber Defense Review* 7, no. 4 (2022), p31.
[36] Willett, "The Cyber Dimension of the Russia–Ukraine War," p9.
[37] ibid, p10
[38] Lin, "Russian Cyber Operations in the Invasion of Ukraine," p33.
[39] James Lewis. *Cyber War and Ukraine* JSTOR, 2022, p2.
[40] Willett, "The Cyber Dimension of the Russia–Ukraine War," p11.
[41] Lin, "Russian Cyber Operations in the Invasion of Ukraine," p37.

Second World War, and true of all military technology advancements, Ukraine's defensive cyberspace operations (DCO) developed to counter Russia's OCO. Ukraine has been fighting back in the Clausewitzian wrestling match in the virtual world. The perceived lack of Russian success in its cyber campaign in 2022 should not be taken as a lesson on the lack of relevance of offensive cyber operations. Instead, it is a lesson in the importance of effective synchronisation across all domains and the positive effect of DCO.

China invests heavily in its offensive cyber capabilities, one aspect of the People's Liberation Army (PLA) where capabilities may be at parity with those of the United States of America (USA). China's cyber warfare doctrine "incorporates all three levels of warfare – strategic, operational, and tactical."[42] China's assessed strength in the cyber domain results from its two-decades-long modernisation of the PLA towards a more high-tech force capable of operations in and around Taiwan and, more broadly, across the South China Sea and the region.[43] Given the size and scale of the PLA, there are some different terminologies and tactics described across the organisation, but essentially, the PLA cyber operations are divided into three overlapping groups of activities: Computer Network Operations (CNO), Information Operations (IO), and Net-Centric Warfare (NCW).[44] Like Russia and Western doctrine, the PLA seeks to integrate these activities with other components of its military and government agencies. Within the CNO grouping, the PLA has developed capabilities to conduct CNA, CNE, and computer network defence (CND). Within CNA, the PLA has developed capabilities such as "DDoS, trojans, viruses, worms" designed to 'deceive, degrade, deny, destroy, or disrupt" adversary computers and networks.[45] These are serious capabilities, and like Russia before 2022, the PLA's ability to use these instruments can only be speculated on, especially at the unclassified level. Experts in the US, such as Paul Springer, assess that these CNO capabilities are being developed to target internet-facing US Department of Defense (DoD) networks such as the 'Non-classified Internet Protocol Router Network (NIPRNET) as well as civilian networks that support the DoD.[46] The disruption of these networks in isolation would have significant but not catastrophic operational impacts. The disruption of these networks in a coordinated fashion, integrated with effects across the other domains, can be more devastating. China routinely conducts CNE now as an extension of its politics and strategy. China's CNE activities include theft, intelligence collection, and network reconnaissance.[47] An excellent example of this type of PLA OCO was the activity named 'Titan Rain' by the US. Titan Rain involved Chinese cyber intrusions into DoD laboratories, NASA networks, and aerospace companies from 2003

---

[42] Jason R. Fritz, Inc Overdrive and Overdrive ebook, *China's Cyber Warfare: The Evolution of Strategic Doctrine*, 1st ed. (Lanham: Lexington Books, 2017) pxviii.
[43] Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation", *The US-China Economic and Security Review Commission*, 2020), p87.
[44] Fritz, *China's Cyber Warfare: The Evolution of Strategic Doctrine*, pxix.
[45] A trojan horse is code disguised as a legitimate program, operating as a backdoor to a system that allows an attack to spread; a worm is code that spreads without outside assistance. Steve Winterfeld and Jason Andress, *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*, 1st ed. (Amsterdam; Boston: Syngress/Elsevier, 2012) p6.
[46] Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation", *The US-China Economic and Security Review Commission*, 2020), p88.
[47] Fritz, *China's Cyber Warfare: The Evolution of Strategic Doctrine*, p2.

to 2005.[48] This is just one example of nefarious Chinese CNE activities; there were 37 cases of CNE similar to Titan Rain reported from 2003 to 2011 alone.[49] These 37 are the detected and reported cases, with likely many more undetected. It is clear China has a sophisticated approach and a deep interest in cyber operations. The PLA has proven to study the teachings of Sun Tzu deeply.[50] Chinese investment in and use of cyber operations to aid political and strategic goals has become integral to their modern appreciation of his theories.

Stuxnet is arguably the most well-known and significant instance of an OCO used on an international scale. It is an example of a cyberspace action with a physical, destructive outcome. It is also an example of a cyber attack that was not integrated with effects in the other domains. Stuxnet was "one of the most sophisticated and unusual pieces of software ever created."[51] Stuxnet was malware[52] designed to target a specific type of equipment[53] in Iran's nuclear enrichment program, which was suspected to be supporting a weapons program.[54] Stuxnet spread for several months before it identified and prosecuted its target.[55] During this time, it spread to over 60,000 computers, over half of which were in Iran.[56] Once it reached its target, the malware caused enrichment centrifuges in the Iranian nuclear facility to malfunction and break due to the delivery of false instructions.[57] Though this destruction was ultimately recovered from, it represented a level of disruption wholly attributable to an OCO capability but ultimately not attributable (publicly) to a particular nation or actor. Interestingly, from an 'Economy of Effort' point of view, this malware capability is assessed to have taken approximately three years to develop.[58] Once it reached its target and was deployed, it expired as a capability (though its code is available on the Internet to potentially be repurposed). This is a characteristic common across sophisticated offensive cyber capabilities. The key deduction from this fact is that OCO should be held for decisive moments. As described by Jomini, if victory can be achieved through massing effects at a decisive point in space and time, then in a modern context, these massed effects must be sourced from all domains, including the cyber domain, to be most effective.

If, as Clausewitz stated, war is an extension of politics by other means and is inherently violent, then Stuxnet came very close to meeting that definition. Ultimately, it

---

[48] Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security* 39, no. 3 (2015), p21.
[49] ibid, p21.
[50] Fumio Ota, "Sun Tzu in Contemporary Chinese Strategy," *Joint Forces Quarterly* 73, no. 2 (2014), p76.
[51] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival (London)* 53, no. 1 (2011), p23.
[52] "Malware is a "program or file that alters a computer's normal functions for malicious purposes or is otherwise harmful to the computer's user." Tikk-Ringas, *Evolution of the Cyber Domain: The Implications for National and Global Security*, p8.
[53] The specific equipment within the Iranian nuclear plant were the supervisory control and data acquisition (SCADA) and programmable logic controllers (PLC). Deonna Neal, *Stuxnet*, 2019), 95-98.
[54] Deonna Neal, *Stuxnet*, 2019), p97.
[55] T. M. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," *Computer (Long Beach, Calif.)* 44, no. 4 (2011), p91-93.
[56] Farwell, "Stuxnet and the Future of Cyber War," p23.
[57] Neal, *Stuxnet*, p97.
[58] Chen, "Lessons from Stuxnet," p91-93.

was not an act of war in the Western sense, as the act did not trigger effects in the other domains, nor did it see any attribution or retaliation. It was, however, violent if you consider the meaning of the original German word 'Gewalt', meaning force or power.[59] This act used cyberspace to exert a destructive force on the Iranian nuclear industry. The lack of retaliation or reaction may be related to the fact the act was never attributable to a specific nation, which is always a difficulty in the conduct of OCO against or between nation-states.[60] However, it likely was a nation, given the assessment of malware experts regarding the sophistication of the malware.[61] This fact elevates the act from an act of terrorism to what was likely an act of a government seeking a strategic or political outcome. It was an 'offensive action' but not synchronised or orchestrated with actions in the other domains. It produced 'strategic surprise' upon Iran (and the rest of the world) through deception, but that surprise was not exploited. A conclusion based on these observations is that the meticulously planned Stuxnet malware had the potential to be an act of war if it had been synchronised across domains with a clear end state.

Contrasting with the historical evidence, which demonstrates that OCO is most effective when integrated correctly into a holistic, multi-domain operation or strategy, is the argument, or sensationalist idea, that actions in the cyber domain alone will decide future wars. The concept that the next Pearl Harbour will be an attack in the cyber domain.[62] This is sensationalist and undermines the actual utility that well-developed cyber operations can bring a nation's military and government. There has never been a cyber incident of the magnitude of the destructive, strategic nature of the Japanese attack on Pearl Harbour. There is no evidence of a capability of that magnitude existing.[63] A pure cyber attack is unlikely to compel an opponent accept defeat.[64] What there is evidence of is that adversaries and potential adversaries such as Russia and China are devoting significant resources to developing cyber capabilities across the spectrum. These capabilities could help these nations win the information fight as part of broader operational, strategic, and grand strategic fights. As seen in the Russia-Ukraine conflict, OCO can disrupt and degrade a nation's critical infrastructure to create dilemmas for the adversary and advantages across the domains for the antagonist. This links well with modern consideration of theories of military defeat (defeat mechanisms). Contemporary theorists such as Frank Hoffman suggest that cyber effects can be a crucial or central contributor to 'Degradation' or 'Disorientation' methods of defeat.[65] Note these are separate and different from traditional defeat mechanisms such as 'Destruction' or 'Dislocation', which are more aligned with the Pearl Harbour analogy and more physical and related to conventional kinetic firepower. The discussion of a cyber Pearl Harbour

---

[59] Andreas Herberg-Rothe, "Clausewitz's "Wondrous Trinity" as a Coordinate System of War and Violent Conflict," *International Journal of Conflict and Violence (IJCV)* 3, no. 2 (2009), p206.
[60] Sanchez, "Applying Irregular Warfare Principles to Cyber Warfare," , p15
[61] Neal, *Stuxnet*, p97.
[62] James F. Dunnigan, *The Next War Zone: Confronting the Global Threat of Cyberterrorism* (New York: Citadel Press, 2003) p4-5.
[63] Thomas Rid, *Cyber War Will Not Take Place*, 1st ed. (New York; Oxford: Oxford University Press, 2013) pxiv-xv.
[64] James Lewis. *Cyber War and Ukraine* JSTOR, 2022, p2.
[65] Frank Hoffman, "Defeat Mechanisms in Modern Warfare," *Parameters (Carlisle, Pa.)* 51, no. 4 (2021), p53.

does have some tertiary merit, though. The merit lies in a 'call for action' across government institutions to invest in defensive cyber and cyber security. Investment in these pillars of cyber operations is essential to build resilience against possibly disruptive adversary cyber activities in future conflict. An informed discussion about the real cyber threats is necessary to ensure practical cyber defences can be built.

DEFENSIVE CYBERSPACE OPERATIONS

After the Second World War, Douhet's theory of air power had been challenged by the establishment of robust integrated air defence to counter the effects of the air domain. Similarly, over the last twenty years, militaries have invested in building their DCO capabilities and cyber security alongside OCO capabilities. These functions are vital in securing cyber key terrain, as demonstrated by Ukraine in its increasing cyber resilience from 2014-2022. Like sea power, securing key cyber terrain is essential to the continued prosperity of a nation in terms of finance, trade, and critical infrastructure. Also, like sea power, DCO extends from commercial interests, such as defending bank information, to tactical engagements in cyberspace (vice at sea). Focusing on the military and warfare aspects, DCO parallels the 'Security' Principle of War. It involves defending friendly networks to preserve the ability to use cyberspace and protect the resident data. These operations can be passive or active.[66] Western nations, as those most likely to be adversely affected by insecurity in cyberspace, are obligated to their citizens and each other to generate 'cyber power' by increasing cyber security and defence across military and civilian networks.[67]

Securing cyber terrain requires a whole of government approach, integrated with a nation's military. There are distinct parallels here with the whole of government approach to shipbuilding, generating a navy, and creating sea power. Like developing a credible Defence Force, the starting point for this approach is to organise a national strategy. Over the last 10-20 years, many nations across the globe have created a cyber strategy, including the Five Eyes nations, as well as countries such as the Czech Republic, Estonia, France, Germany, India, Japan, Lithuania, Luxembourg, Romania, The Netherlands, South Africa, Spain, and Uganda.[68] The Australian Government recently released the 2023-2030 Australia Cyber Security Strategy.[69] This strategy introduces that "the stakes in protecting our people and businesses have never been higher" and "cyber security is not just about defending ourselves against threats – it's critical to support the rapid adoption of new technologies, boosting productivity and growing the digital economy."[70] There are strong similarities here with the theories of Mahan on sea power protecting trade and commercial interests. Another observation on this strategy, and similar strategies from Canada, the US, the UK, and other like-minded nations, is that cyber security affects a nation's civil population as much or more than a nation's military. This

---

[66] Tikk-Ringas, *Evolution of the Cyber Domain: The Implications for National and Global Security*, p170.
[67] Burns, *Securing Cyberspace: A New Domain for National Security*, p60-61
[68] Eric Luiijf, Kim Besseling and Patrick De Graaf, "Nineteen National Cyber Security Strategies," *International Journal of Critical Infrastructures 6* 9, no. 1-2 (2013), p3.
[69] Department of Home Affairs Australian Government, "2023-2030 Australian Cyber Security Strategy," (2023). https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf
[70] ibid, p8.

is concerning, given the lessons from the Russia-Ukraine conflict and the assessments of Chinese cyber operations and their recent CNE operations. The targets of our adversaries' cyber capabilities are often 'soft' civilian targets. Nations are adapting to this new tool, which allows the application of political will in a new arena. Additionally, modern nations and their governments must adjust to nefarious cyber-based activities by non-state actors (like crime and terrorism in the physical domain).

The development of the air domain saw significant legal issues and considerations, noting the ability of air power to bring effects and violence to the civilian population, far removed from the battlefield.[71] The advent of OCO and DCO has also had significant legal ramifications. Understanding these legal issues is a matter of broad international debate. Looking at international law, "Article 2(4) of the United Nations (UN) charter stipulates that nations should refrain from the threat or use of force against other sovereign nations."[72] Any nation that conducts OCO can avoid attribution or use the ambiguity in international law to claim that any action carried out did not constitute 'force'. This legal loophole speaks broadly to the theme of this paper – what are the actions in cyberspace if they do not constitute some level of force? Regarding DCO, specifically 'active' defence, UN Charter Article 51 "provides a loophole in which nations are given the right of individual or collective self-defence in the face of armed attack."[73] These legal issues are observed differently in Chinese academic literature. The US position on cyber warfare is that the law of armed conflict (LOAC) would apply to cyber actions from a "distinction, necessity, and proportionality" point of view.[74] China and Russia have indicated they do not support this position. Using their strong position on the UN Security Council, China and Russia influenced the 2015 Group of Government Experts (GGE) report on information and telecommunications. The report notes that "the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction", might be applied but avoids specifically referencing international humanitarian law.[75] These legal complications are complexities that require collaboration across the international community. However, they are not unique to cyberspace. The advent of airpower and the overlap of the military and civilian use of the air has ultimately been deconflicted to the point where sovereign airspace is primarily respected, or if not, an incursion may be considered an escalatory act that may lead to war. Similar comparisons can be made about the rules of the sea.

Counter to the idea of DCO as a subset of cyber warfare is that these cyber security efforts are just good government business and 'cyber hygiene', which is the responsibility of all pillars of society.[76] The question posed here is one of the primacy of

---

[71] Karl P. Mueller, "Air Power," in *Oxford Research Encyclopedia of International Studies*, 2010) p6.
[72] Julian Richards Dr, *Cyber-War: The Anatomy of the Global Security Threat*, 1st ed. (Houndmills, Basingstoke, Hampshire; New York, NY: Palgrave Pivot, 2014) p7.
[73] ibid, p7.
[74] Chaoyi Jiang, "Decoding China's Perspectives on Cyber Warfare," *Chinese Journal of International Law (Boulder, Colo.)* 20, no. 2 (2021), p270.
[75] Chaoyi Jiang, "Decoding China's Perspectives on Cyber Warfare," *Chinese Journal of International Law (Boulder, Colo.)* 20, no. 2 (2021), p270.
[76] Martin C. Libicki, "Cyberspace is Not a Warfighting Domain," *Isjlp* 8 (2012), p321.

jurisdiction between civil organisations and civil policing versus military control.[77] A cautious review of the evidence discussed in this paper demonstrates that adversary nation-states who wish to 'push politics through other means' can significantly disrupt civilian access to cyberspace. One example of this is the Russian disruption of Ukrainian power networks in 2015. Western nations' governments understand this overlap. The previously mentioned 2023-2030 Australian Cyber Security Strategy overlaps and nests with the Australian 'Defence Strategic Review' (DSR) released in the same year (2023). The DSR's section addressing the cyber domain, notes that "Australia's cyber and information capabilities must be scaled up and optimised."[78] It also notes that the Australian Defence Department must develop a framework for "managing operations in the cyber domain that is consistent with the other domains."[79] Like the sea and air domains overlap with civilian use of the air and sea, civilian use of cyberspace overlaps with the widespread civilian use of that same terrain. A nation's military's ability to operate in that terrain is vital for protecting its people.

The concept of deterrence in military strategy is linked to the advent of a different type of new technology – nuclear weapons. Though definitions vary, most will resemble that provided in United States Joint Publication 1-02: "the prevention from action by fear of the consequences… a state of mind brought about by the existence of a credible threat of unacceptable counteraction."[80] This is a concept well aligned with the capability and threat of nuclear weapons. However, the language of deterrence has become more critical in recent years due to rising geopolitical tensions and associated changing strategic circumstances. Notably, in the Australian 'National Defence Strategy' released in April 2024, deterrence through denial was listed as a critical capability requirement of the ADF: "deter through denial any potential adversary's attempt to project power against Australia through our northern approaches."[81] Cyber operations are a component of national power that supports deterrence. However, the evolution of cyber technology and theory has meant cyber deterrence theory has often been outpaced by cyber deterrence in practice.[82] Deterrence in the cyber domain is further complicated by issues attributing actions to specific actors and the open nature of modern internet-facing networks.[83] Additionally, unlike nuclear deterrence, which focuses on a single type of weapon, many weapons are available in the cyber domain.[84] These issues contribute to the theory of

---

[77] Mary Ellen O'Connell, "Cyber Security without Cyber War," *Journal of Conflict & Security Law* 17, no. 2 (2012), p188.
[78] "National Defence - Defence Strategic Review," Australian Government, 2023 https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review p64.
[79] "National Defence - Defence Strategic Review," Australian Government, 2023 https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review p54.
[80] James Blackwell, "Deterrence at the Operational Level of War," *Strategic Studies Quarterly* 5, no. 2 (2011), p31.
[81] "2024 National Defence Strategy," last modified 17 April 2024, https://www.minister.defence.gov.au/media-releases/2024-04-17/2024-national-defence-strategy
[82] Alex S. Wilner, "US Cyber Deterrence: Practice Guiding Theory," *Journal of Strategic Studies* 43, no. 2 (2020), p247.
[83] Alex S. Wilner, "US Cyber Deterrence: Practice Guiding Theory," *Journal of Strategic Studies* 43, no. 2 (2020), p252.
[84] Denning, "Rethinking the Cyber Domain and Deterrence," p12.

cyber deterrence, which is still in its infancy. A nation without a credible cyber capability risks having a non-credible deterrence effect in a multi-domain sense.

MULTI-DOMAIN OPERATIONS

Australian General Sir John Monash was one of the pioneering forces of combined arms warfare in the First World War. He described this innovative form of warfare as allowing the infantry to "advance under the maximum possible protection of the maximum possible array of mechanical resources in the form of guns, machine-guns, tanks, mortars and aeroplanes; to advance with as little impediment as possible."[85] MDO are the combined arms warfare of the 21st century.[86] Modern technologies such as long-range strike and uncrewed aerial systems have changed the character of war to be larger and more complex. Integrating cyber effects as part of MDO is essential to maximise military outcomes and success in warfare. In future warfare, cyber operations must be integrated with other military and whole of government effects to match and exceed adversary capabilities and actions. The relationship between the nation's government and the projection of cyber power has been demonstrated by studying Russian and Chinese high-level capabilities. However, integration across the domains, including the cyber domain, will also need to occur at the operational and tactical levels for effective MDO. To access OCO capabilities, habitual relationships with government agencies such as the Australian Signals Directorate (ASD) in Australia are necessary. These collaborations will be required to deliver appropriate technical capabilities and ensure complex legal and ethical considerations are accounted for.[87] These challenges are similar to the challenge of integrating strategic-level air and sea effects with land-based tactical actions—a common challenge of joint and multi-domain warfare. The focus of cyber activities at the tactical and operational level should be on protecting the operational function of Command. Cyberspace and the electromagnetic spectrum (EMS) are decisive terrain that must be secured to maintain decision superiority against an adversary commander and to facilitate effective command and control of deployed forces. This focus will allow commanders to focus on new theories of victory based on making "faster and better decisions than adversaries, rather than attrition."[88] This is an important focus, as it is one that potential adversaries such as the PLA also hold. Chinese military writings note that "command speed enabled by information dominance determines the outcome of a battle in a modern conflict."[89] At its most fundamental, securing this cyber and EMS terrain involves good communications security, information security, and force-wide education.

---

[85] James W. Reed, "Combined Arms Warfare in the 21st Century: Maximizing the Capability of US Army Future Combat System Equipped Brigade Combat Teams to Conduct Combined Arms Operations*", US Army Command and General Staff Course*, (2008), p33.
[86] US Army Training and Doctrine Command, "Multi-Domain Battle: Combined Arms for the 21st Century," *White Paper, US Army, February* 24 (2017), p1.
[87] Marcus Thompson, "The ADF and Cyber Warfare," *Australian Defence Force Journal*, no. 200 (2016), p45-46.
[88] Hoffman, "Defeat Mechanisms in Modern Warfare," p56.
[89] Edmund J. Burke et al., *People's Liberation Army Operational Concepts* RAND Santa Monica, CA, 2020), p10.

CONCLUSION

Recent examples, such as those from the Russia-Ukraine conflict, show that cyber warfare is crucial to the current battlespace. Estonia and Georgia were not prepared for operations in the cyber domain and suffered as a result. Ukraine learnt from its experiences in 2014 and was more prepared in 2022, contributing to successful early defensive outcomes. Sophisticated cyber attacks such as those demonstrated by Stuxnet and the types of capabilities being developed by the PLA indicate the importance of these capabilities in future conflicts. However, cyber capabilities are unlikely to win a war on their own. OCO and DCO must be synchronised with effects across the other domains in coherent MDO design to succeed and be effective. Understanding how cyber warfare functions align with classical military theory is critical. Cyber warfare can be seen as violent in the Clausewitzian sense if one considers the nature of the effects that can be generated in this domain. The force that cyber can generate must be employed decisively, at decisive points, as Jomini described in his principles. The PLA is blurring the lines of cyber diplomacy and cyber warfare, a concept as old as the teachings of Sun Tzu. An important point for modern military planners is that the advent of the cyber domain holds significant parallels with that of the air and sea domains. The teachings of Douhet can guide modern nation-states to ensure that not only is their Air Force ready and capable for future fights, but also their cyber force. Similar to Mahan's descriptions of 'control of the sea', the defence of cyberspace will be vital to the continued prosperity of all nations, with trade at sea paralleling e-commerce. However, akin to Corbett's observations of sea power, the open nature of cyberspace will mean the Clausewitzian wrestling match will continue for decades to come.

BIBLIOGRAPHY

Ashmore, William C. "Impact of Alleged Russian Cyber Attacks." *Baltic Security & Defence Review* 11, no. 1 (2009): 4-40.

Australian Army. "Land Warfare Doctrine 3-0-3, Formation Tactics.", 14 Nov, 2016

Australian Government. "National Defence - Defence Strategic Review." Australian Government. https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review.

Australian Government Department of Defence. "2024 National Defence Strategy." . https://www.minister.defence.gov.au/media-releases/2024-04-17/2024-national-defence-strategy.

Australian Government, Department of Home Affairs. "2023-2030 Australian Cyber Security Strategy.", 2023. https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

Beehner, Lionel, Liam Collins, Steve Ferenzi, Robert Person, and Aaron F. Brantly. "Analyzing the Russian Way of War: Evidence from the 2008 Conflict with Georgia." *Analysing the Russian War of War: Evidence from the 2008 Conflict with Georgia* (2018).

Blackwell, James. "Deterrence at the Operational Level of War." *Strategic Studies Quarterly* 5, no. 2 (2011): 30-51.

Brandes, Sean. "The Newest Warfighting Domain: Cyberspace." *Synesis: A J.Sci., Technol., Ethics, Policy* 4, (2013): 90.

Burke, Edmund J., Kristen A. Gunness, Cortez A. Cooper, and Mark R. Cozad. *People's Liberation Army Operational Concepts* RAND Santa Monica, CA, 2020.

Burns, R. Nicholas, Jonathon Price, Joseph S. Nye, Brent Scowcroft, Aspen Institute, and (U S.). Aspen Strategy Group. *Securing Cyberspace: A New Domain for National Security*. Washington, D.C: Aspen Institute, 2012.

Canada. Department of National Defence. "Pan-Domain Force Employment Concept: Prevailing in an Uncertain World." *Cjoc* (2023).

Chen, T. M. and S. Abu-Nimeh. "Lessons from Stuxnet." *Computer (Long Beach, Calif.)* 44, no. 4 (2011): 91-93. doi:10.1109/MC.2011.115.

Clausewitz, Carl von, Wanda McCaddon, OverDrive audiobook, and Inc OverDrive. *On War*. Unabridged ed. Ashland, Or.: Blackstone Audio, 2008.

Connell, Michael, Sarah Vogler, and CENTER FOR NAVAL ANALYSES ALEXANDRIA VA ALEXANDRIA United States. *Russia's Approach to Cyber Warfare* 2016.

Corbett, Julian Stafford, Sir, Inc OverDrive, and OverDrive ebook. *Principles of Maritime Strategy*. 1st ed. Mineola, NY: Dover Publications, 2004.

Denning, Dorothy E. "Rethinking the Cyber Domain and Deterrence." *Joint Force Quarterly: JFQ* no. 77 (2015): 8.

Dunnigan, James F. *The Next War Zone: Confronting the Global Threat of Cyberterrorism*. New York: Citadel Press, 2003.

Farwell, James P. and Rafal Rohozinski. "Stuxnet and the Future of Cyber War." *Survival (London)* 53, no. 1 (2011): 23-40.

Fritz, Jason R., Inc Overdrive, and Overdrive ebook. *China's Cyber Warfare: The Evolution of Strategic Doctrine*. 1st ed. Lanham: Lexington Books, 2017.

Gold, Josh. "The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'." *Tallinn, Estonia: NATO CCDCOE* (2020).

Green, James A. *Cyber Warfare: A Multidisciplinary Analysis*, edited by Green, James A. 1st ed. Abingdon, Oxon; New York, NY: Routledge, 2015.

Hanson, Kraig and ARMY WAR COLL CARLISLE BARRACKS PA. *Organization of DoD Computer Network Defense, Exploitation, and Attack Forces* US Army War College, 2009.

Haun, Phil. "Winged Victory: How the Great War Ended: The Evolution of Giulio Douhet's Theory of Strategic Bombing." *War in History* 29, no. 3 (2022): 584-601. doi:10.1177/09683445211027596.

Herberg-Rothe, Andreas. "Clausewitz's "Wondrous Trinity" as a Coordinate System of War and Violent Conflict." *International Journal of Conflict and Violence (IJCV)* 3, no. 2 (2009): 204-219.

Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49-60.

Hoffman, Frank. "Defeat Mechanisms in Modern Warfare." *Parameters (Carlisle, Pa.)* 51, no. 4 (2021): 49-66.

Hollis, David. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*, *https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf* (2011).

Jiang, Chaoyi. "Decoding China's Perspectives on Cyber Warfare." *Chinese Journal of International Law (Boulder, Colo.)* 20, no. 2 (2021): 257-312.

Jomini, de, Baron, Inc Overdrive, and Overdrive ebook. *The Art of War*. New York: Start Publishing LLC, 2013.

Krekel, Bryan *"*Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*", The US-China Economic and Security Review Commission,* 2020.

Lewis, James A. *Cyber War and Ukraine* JSTOR, 2022

Libicki, Martin C. "Cyberspace is Not a Warfighting Domain." *Isjlp* 8, (2012): 321.

Lin, Herbert. "Russian Cyber Operations in the Invasion of Ukraine." *The Cyber Defense Review* 7, no. 4 (2022): 31-46.

Lin, Herbert, David Aucsmith, Steven M. Bellovin, Daphna Canetti, Henry Farrell, Erik Gartzke, Charles L. Glaser, et al. *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*,

edited by Lin, Herbert, Herbert Lin, Amy B. Zegart and Amy Zegart. 1st ed. Washington, D.C: Brookings Institution Press, 2019.

Lindsay, Jon R. "The Impact of China on Cybersecurity: Fiction and Friction." *International Security* 39, no. 3 (2015): 7-47.

Luiijf, Eric, Kim Besseling, and Patrick De Graaf. "Nineteen National Cyber Security Strategies." *International Journal of Critical Infrastructures 6* 9, no. 1-2 (2013): 3-31.

Mahan, A. T., John B. Hattendorf, Inc OverDrive, and OverDrive ebook. *Mahan on Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan*. 1st Naval Institute Press pbk.; 1 ed. Annapolis, Md: Naval Institute Press, 2015.

Mueller, Karl P. "Air Power." In *Oxford Research Encyclopedia of International Studies*, 2010.

Neal, Deonna. *Stuxnet, "Conflict in the 21st Century: The Impact of Cyber Warfare, Social Media, and Technology"*, 2019.

Neilson, Robert E. and National Defense University. Institute for National Strategic Studies. *Sun Tzu and the Art of War in Information Warfare*. Washington, DC: National Defence University, 1997.

O'Connell, Mary Ellen. "Cyber Security without Cyber War." *Journal of Conflict & Security Law* 17, no. 2 (2012): 187-209.

Ota, Fumio. "Sun Tzu in Contemporary Chinese Strategy." *Joint Forces Quarterly* 73, no. 2 (2014): 76-80.

Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective."Academic Publishing Limited Reading, MA, 2008.

Perkins, Gen David G. "Multi-Domain Battle." *Military Review* (2017).

Reed, James W. "Combined Arms Warfare in the 21st Century: Maximizing the Capability of US Army Future Combat System Equipped Brigade Combat Teams to Conduct Combined Arms Operations" US Army Command and General Staff Course (2008).

Richards, Julian, Dr. *Cyber-War: The Anatomy of the Global Security Threat*. 1st ed. Houndmills, Basingstoke, Hampshire; New York, NY: Palgrave Pivot, 2014.

Rid, Thomas. *Cyber War Will Not Take Place*. 1st ed. New York; Oxford: Oxford University Press, 2013.

Sanchez, Frank C., Weilun Lin, and Kent Korunka. "Applying Irregular Warfare Principles to Cyber Warfare." *Joint Force Quarterly* no. 92 (2019a): 15.

Thompson, Marcus. "The ADF and Cyber Warfare." *Australian Defence Force Journal* no. 200 (2016): 43-48.

Tikk-Ringas, Eneken and International Institute for Strategic Studies. *Evolution of the Cyber Domain: The Implications for National and Global Security*, edited by Tikk-Ringas, Eneken. 1st ed. Abingdon, Oxon; New York, NY: Routledge, for the International Institute for Strategic Studies, 2016.

Training, US Army and Doctrine Command. "Multi-Domain Battle: Combined Arms for the 21st Century." *White Paper, US Army, February* 24, (2017).

United States Marine Corps. "MCDP 1-4 Competing." (2020).

Willett, Marcus. "The Cyber Dimension of the Russia–Ukraine War." In *Survival: October-November 2022*, 7-26: Routledge, 2023.

Wilner, Alex S. "US Cyber Deterrence: Practice Guiding Theory." *Journal of Strategic Studies* 43, no. 2 (2020): 245-280.

Winterfeld, Steve and Jason Andress. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. 1st ed. Amsterdam; Boston: Syngress/Elsevier, 2012.