Chapter 14

Cyberspace Operations, Grey zone conflict and Small States

Mikkel S. JENSEN

Abstract

Cyber-attacks are a growing component of grey zone operations. Even small and weak states can develop offensive cyber capabilities, but there may be disadvantages to doing so. How does offensive cyber, both acknowledged and unacknowledged, affect the ability of a small state to deploy other means of pursuing security, including conventional alliance or alignment, and use of international organizations? This chapter explores offensive cyberspace operations in the context of small states, contemporary geopolitics, and its implications for the management of national security.

Cyber weapons and strategy in Grey Zone conflicts

Offensive cyberspace operations capabilities (OCOC) – “cyber weapons” – have attributes that make them well suited as means for states to deploy in Grey Zone conflicts. The different categories of offensive cyberspace operations (OCO) will be explained below, but initially it must be noted that OCO can be stealthy, difficult and time consuming to attribute, have potential for severe impact either directly or as second-order effects, and their digital traces are more accommodating for “credible deniability” than the more tangible evidence left by kinetic means. OCOC are often less suited for achieving very specific effects in time and space, but such disadvantages are more than balanced by the fact that states can use OCOC to conduct espionage, subversion and sabotage from the comfort of home through cyberspace at lower risks and on exponentially larger scales than in the analogue Grey Zone-operations of yesteryear. Modern critical infrastructure and governance depend on IT-systems, which can be targeted. Disinformation-dissemination can utilize the algorithms of social media to optimize impact. Espionage benefits from the digitalisation of data by measuring successful operations in extracted terabytes of information rather than a few documents exfiltrated in a micro dot. OCOC allow all these Grey Zone operations to be conducted from the safety and comfort of home without having to send vulnerable and, if caught, potentially embarrassing agents abroad. Furthermore, some OCOC are relatively cheap to acquire. This make them available even to states with limited resources, allowing them to conduct operations against neighbouring states as well as against opponents on the other side of the globe.

That said, in spite of how potent cyber attacks are often represented in popular culture, they are rarely a miracle weapon. The purpose of this chapter is to provide a first impression, introducing the potential and limitations of OCOC in Grey Zone operations within a very limited space. Other chapters in this book discuss important and cyber-relevant aspects such as information operations, society wide cyber resilience and the role of non-state actors. Therefor this chapter will focus on states' use of OCOC as an offensive means in Grey Zone conflicts, with only a brief discussion of defensive aspects of OCOC's applicability, e.g. as a deterrence against hostile Grey Zone cyberspace activities. The ambition is to, based on current literature, provide the reader with an initial understanding of OCOC's basic attributes and their influence on the means use in and defending against, Grey Zone operations and perhaps inspire to further studies.

The chapter initially presents its analytical framework for Grey Zone operations: Kilcullen's model of Liminal Warfare. It moves on to present different subtypes of cyberspace operations and their roles in Grey Zone conflict. Then follows a brief discussion to present OCOC's offensive and defensive potential and establish why OCOC present more serious threats than the most sceptical analysts profess but are less of a doomsday means than the most hyperbolical claim. It rounds of with a discussion of OCOC's use by military alliances or by individual states who depend mainly on alliances for their security.

The chapter concludes that from an offensive perspective, OCOC are very well suited for Grey Zone Conflict. There are severe limitations to their use for defence or deterrence, especially by alliances or by states dependent on alliances – as many small states are. To such states, societal resilience against cyberattacks and cyber-enhanced disinformation are more immediately useful strategies to diminish the effect of hostile Grey Zone operations and deter their use.

For clarity, the chapter will mainly refer to definitions used in US or NATO doctrines. The analysis will be limited to the strategic use of OCOC by states – that is, OCOC used as a means by way of Grey Zone Conflict to achieve national security ends, e.g. the weakening of an advesary by subversion[1]. This includes states' use of non-state actors, e.g. Russia's tacit collaboration with cyber criminals, but excludes non-state actors that engage in offensive cyberspace operations for criminal or ideological purposes. The chapter acknowledges that some criminals are very capable threats, that states must be prepared to defend against – but their attacks are for criminal purposes, not raison d'état, and hence not a part of Grey Zone Conflict. Ideologically motivated cyber activists could arguably be included, e.g. if the attacker through insurgency aspires to become a state actor. However, ideologically motivated attackers have hitherto remained rather ineffective and without significant impact even when they have been most extensively engaged as after the Russian invasion of Ukraine. At the time of writing (October 2022) neither Russian criminals swearing support for the Motherland nor Ukraine's IT Army have apparently been able to cause significant effects (Schechner, 2022; Vu *et al.*, 2022). Also the Ukraine IT Army, an entirely new concept of national and foreign volunteers pledging to attack Russia in support of Ukraine, but only loosely affiliated with the state and often anonymous, is a too big, recent and underexamined topic from both strategic and legal perspectives for this chapter to address.[2]

[1] For a conceptual understanding of strategy, see e.g.(Yarger and Bartholomees, 2012; Jakobsen, 2022).

[2] For studies of the Ukraine IT-Army, see e.g. (Soesanto, 2022, 2023; Vu *et al.*, 2022)

Kilcullen’s model of liminal warfare

To provide an analytical framework of the discussion, Kilcullen’s model of liminal warfare (see Figure 1) identifies some very useful concepts in the shape of the three thresholds; detection, attribution and response: Grey Zone Conflict is conducted mainly above the threshold of detection. While some operations, e.g. espionage, are intended to remain under the threshold of detection, they may also be considered as aspects of Grey Zone Conflict due to their objectives or accumulative effects, e.g. the consistent Chinese cyber enabled espionage campaigns to transfer intellectual property from other nations to her own industries (NCSC, 2018). Some Grey Zone operations may be designed to be difficult to attribute, while others may be indifferent to this aspect, as in the case of many Russian offensive cyber campaigns or even seek attribution as an objective as in North Korea’s Sony attack (Sharp, 2017, pp. 911–913). Above the level of response, Grey Zone conflict becomes armed conflict.

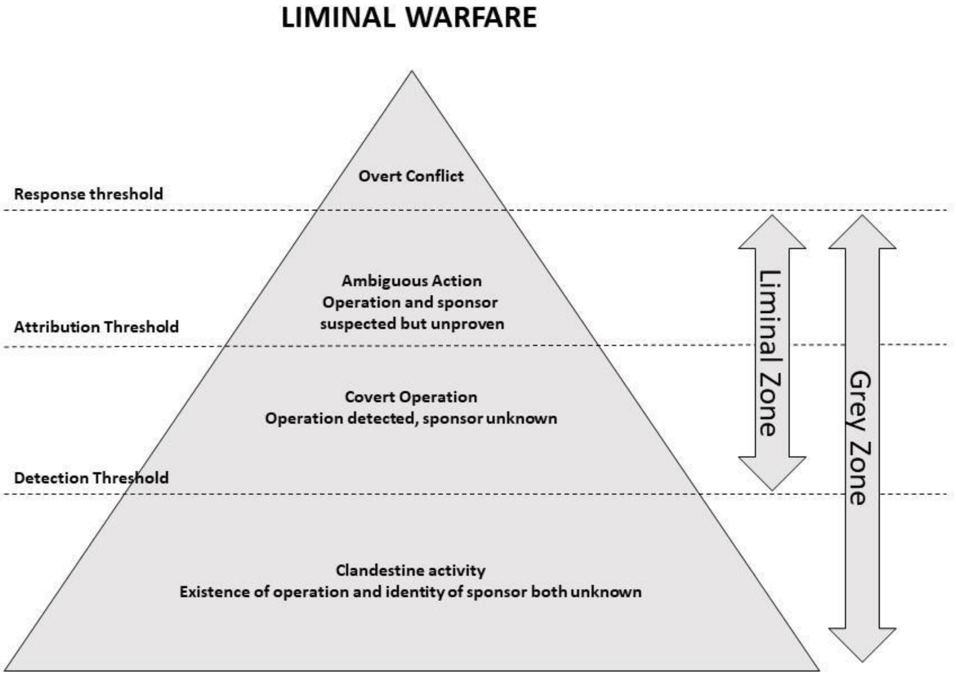

Figure 1: Grey Zone operations imposed on Kilcullen's Liminal Warfare model. Source: Kilcullen, ‘The Evolution of Unconventional Warfare’, 69.

Grey Zone cyber-enabled means: Espionage, disinformation and destructive attacks through cyberspace

While the term “cyber domain” is sometimes used in NATO communications, the term used in NATO-doctrines is “cyberspace”. NATO defines cyberspace as “The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data.”. Cyberspace operations (CO) are actions in or through cyberspace intended to preserve friendly freedom of action in cyberspace and/or to create effects to achieve commanders’ objectives (NATO, 2020, pp. 4, 18). CO can be devided into defensive cyberspace operations (DCO) and offensive cyberspace operations (OCO).

DCO and the associated capabilities do, by their very nature, not represent coercive means. DCO-capabilities and other means of cyber-resilience are not considered controversial or threatening in international relations and are indeed necessary to protect a nation's citizens and corporations against the proliferate and talented criminals in cyberspace. Most states with a level of digital infrastructure have acquired means and set up organizations for DCO. These play important roles in societal resilience in cyberspace against hostile state actions, criminal attacks and cyber-related accidents. Thus, states' DCO-capabilities are essential to strategies of deterrence by denial as they are key to resilience (Janczewski and Caelli, 2016; Jensen, 2018, p. 4). In general, resilience is the main component in the strategies of the EU and the European NATO allies to deter Grey Zone operations conducted through cyberspace (Smeets, 2020b, 2021).

When looking at inter-state relations, the analytical focus should therefore be on offensive cyberspace operations (OCO). Current NATO doctrine only distinguishes between DCO and OCO, but US doctrines helpfully distinguish between two different subcategories of OCO: cyber enabled espionage (Cyberspace Exploitation) and destructive attacks (Cyberspace Attacks). Cyberspace exploitation are intrusive, but non-destructive operations in order to collect intelligence, while cyberspace attacks are operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves (Joint Chiefs of Staff, 2018, p. II–6, II–7; NATO, 2020, pp. 16–17).

Espionage is not a new tool for states operating in the Grey Zone, but compared to analogue means, cyberspace exploitation provide a paradigm shift in states' intelligence collection opportunities by widening the scope and lowering the costs and associated risks (Søilen, 2016). Thus, Chinese theft of intellectual property, a lot of which has been conducted through cyberspace exploitation, has risen from the level of nuisance to being considered a strategic threat by the US after 2010 (Harold, Libicki and Stuth Cevallos, 2016). The EU is also becoming more concerned over the threat from China's espionage, that to a large degree is conducted through cyberspace. So far though, the EU has been reluctant to call out the Chinese state on the activities and mainly restrained reactions to recommending higher resilience against espionage (PricewaterhouseCoopers, 2018). Furthermore, cyberspace exploitation can support hostile states' disinformation campaigns, which themselves can be conducted utilizing cyber means, e.g. social media and the associated optimizing algorithms to target and reach the most advantageous audience. Again, propaganda and disinformation are old tools for Grey Zone-operations, but cyber means increase their scale exponentially, blurs the source, obfuscate attribution and facilitate targeting the most receptive audiences. Probably the most famous and successful example of such OCO-enhanced disinformation operations was the Russian hack of the Democrats during the US 2016 presidential elections. Russia used some of the extracted material, e.g. disseminated through WikiLeaks, to support and substantiate parallel efforts to undermine national US coherence and widen ideological fault lines. Operations were conducted from fake accounts run from troll farms such as the Internet Research Agency located in Skt. Petersburg, where Russians impersonated American citizens on both sides of ideological divides and fanned the flames by calling for radical action and disseminating propaganda aimed at radicalising both sides (U.S. Senate Intelligence Committee, 2016, p. 199; Diresta *et al.*, 2019). The effects of the espionage and disinformation campaigns resonated throughout the Trump administration and beyond (Calamur, 2019). Thus, cyberspace exploitation and disinformation are potentially powerful tools for states in Grey Zone operations.

Characteristics of offensive cyberspace operations fit Grey Zone operations

OCO provide states with a genuinely new tool for sabotage and coercion around or below Kilcullen's attribution threshold, and sometimes even below the detection threshold. OCO will be explained in more detail below, but note initially that they normally proceeds along a so called "kill chain". Once a target system is identified, recconaisance for weaknesses becomes the next step. Once found, an OCOC is chosen, or, in the case of "tailored access operations", specifically developed to take advantage of this weakness, either by facilitating the installation of other OCOC inside the system under attack or deliver an effect, e.i. extract information (OCO/cyberspace exploitation) or destroy data or hardware run by the system (OCO/cyberspace attack) (Yadav and Rao, 2015; Loleski, 2019). While the effect is instantaneous once you press "enter" (providing the intelligence on the opponent's system your OCOC's development was based on was sufficiently detailed and updated), the time from deciding to effect an opponent through OCO to being able to actually conduct the attack may take several months. As demonstrated by the current lack of success for Russia's OCO against Ukraine, conducting succesfull attacks is a difficult undertaking against a vigilant opponent (Bateman, 2022).

Unlike Grey Zone-operations with analogue means, OCO, whether cyberspace attacks or cyberspace exploitation, will often leave the victim of attacks in some level of uncertainty regarding attribution. Furthermore, even when realizing he is under attack, the victim will be left in doubt whether he has realized all the ways in which he has been attacked (Libicki, 2009, p. 92; Rid and Buchanan, 2015, p. 11). The US initial reactions to the Solar Winds attack, attributed tentatively to Russian intelligence, provide ample evidence of the insecurity that follows the discovery of a deep penetration of critical systems (Fireye, 2020; Sanger and Perlroth, 2020; Jensen, 2022b, p. 15).

The technical and operational attributes of OCO are thus conducive to the ambiguities that accompanies Grey Zone operations. Successful cyberspace exploitation will remain under the detection threshold. Detected cyberspace exploitation or successful cyberspace attacks move from the lowest, undetected level in Kilcullen's figure and into the liminal zone: They may remain unattributed for a while and even when attributed, will most likely remain below the threshold of response. To give three examples, the 2017-NotPetya attack cost Western companies several billion dollars in losses and damage. It was attributed to Russia by the US, UK and Danish governments (Greenberg, 2018; Demberger, 2022). In 2020, the director of FBI stated that "The greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China, […] the people of the United States who are the victims of what amounts to Chinese theft on a scale so massive that it represents one of the largest transfers of wealth in human history," (Flannery, 2020). Yet arguably, neither Russia nor China have suffered consequences comparable to their actions. The STUXNET cyberspace attacks could be seen as a third, Western example of use of OCO in a Grey Zone operation: The US and Israel has never recognized the attack but the cyber-enabled sabotage of the Iranian nuclear program is generally attributed to them (Falco, 2012, p. 20). In Kilcullen's terms, the STUXNET cyberspace attacks remained below the detection threshold from 2009 to 2010. Following its discovery and substantial analysis, the attack now hovers around the attribution threshold where the attackers are suspected but not proven. Even so, the attack has remained below the response threshold, something that would have been less likely if the Israelis had opted for e.g. an airstrike instead of cyberspace attacks to delay the Iranian program (Steele, 2008).

While OCO will leave digital trails, the process of intelligence based attribution may be time consuming and initially provide insufficient, low-confidence answers (Lindsay, 2015, p. 56). Furthermore, a victim may be reluctant to disclose detailed evidence as it may reveal counterintelligence capabilities and methods. In any case, a screenshot or a printout from a log file is less likely to arouse public emotions, particularly with third parties, and more easily dismissed as fabrications by the perpetrator than e.g. bomb fragments or CCTV-images of intelligence agents entering the area where an attack has taken place.

Offensive cyberspace operations: Less than a revolution, more than a nuisance

Cyberspace attacks' technical and tactical properties challenge the traditional realist understanding of what is possible for large states but impossible for small states based on their available resources (Handel, 1990, p. 83). Hitherto, conventional military means with strategic reach and/or effect, e.g. a capable intercontinental missile force, a blue water navy and/or nuclear weapons, have required a very obvious and significant investment from a state and a large military-industrial base to develop. Their costs have limited proliferation and the necessary infrastructure has literally made preparations visible from space to external observers. Based on observable intelligence, allies and foes alike are able to make assessments of states' conventional and nuclear strategic capabilities' size and efficacy and may glean information regarding their owner's intent.
The emergence of cyberspace attacks has changed this situation and hence the strategic context. Small states can acquire them: The cost of entry into the cyberspace attack-capable group of states is relatively low. Basic capabilities requires only commercially available IT-equipment and a team of qualified researchers, software developers and operators (Liff, 2012, p. 418; JFQ, 2019). This setup can be optimized by coupling it with national intelligence services' collection capabilities. Cyberspace attacks have unlimited geographical reach as long as the targets are linked to the Internet, and as demonstrated by STUXNET, with some extra effort they may even reach air gapped targets (Farwell and Rohozinski, 2011). Unlike conventional means, cyberspace attacks does not require large military and industrial investments to develop and deploy. This means that cyberspace attacks can be developed with little or no recognizable signature, preparations staying below the detection threshold, which adds to the means usefulness for Grey Zone operations.

Prior to the Russian invasion of Ukraine, Russia had conducted nearly a decade of Grey Zone-style coercive cyber campaigns against Ukraine. Many attacks lay above the detection and even attribution threshold, but the attacks remained below the response threshold (Demberger, 2022). Following the invasion in February 2022, some analysts, including the author of this chapter, expected Russian OCO to significantly impact the Ukrainians' communications, logistics, air defences and perhaps also civilian critical infrastructure. While information from the cyber aspects of the war is still sparse at the time of writing (June 2023), it is apparent that Russia has conducted a significant amount of potentially destructive attacks against both military targets, e.g. air defence and communications, and civilian infrastructure, e.g. governance and financial infrastructure (Sanger and Barnes, 2022). However, Ukraine has been sufficiently resilient to remain functional (Bronk, Collins and Wallach, 2022; Kostyuk and Gartzke, Erik, 2022). There are several credible explanations why this is so: 1) Western analysts may have overestimated Russian competence and ability to conduct and coordinate cyber warfare, in the same way as the Russian conventional operations have surprised analysts by their lack of coordination and skill even at the tactical level. 2) Russia may have saved their OCOC for other missions: If you are unconcerned with attribution and collateral damage, then why temporarily disable a piece of Ukrainian infrastructure with an advanced, specially tailored cyberspace attacks, if you can level the target with an artillery barrage? 3) Ukraine has, with some support from friendly states and private companies like Microsoft and STARLINK, skilfully mitigated the Russian attacks sufficiently (Nakasone, 2022). In doing so, Ukraine has demonstrated a whole-of-society resilience strategy involving extensive public-private-partnerships. The answer is for future historians to provide, but likely, all three explanations have played a role (Bateman, 2022; Wilde, 2022; Hüsch and Jarnecki, 2023; Lonergan and Poznansky, 2023).

While the war in Ukraine is far above the response threshold in the overt conflict-zone and hence outside the realm of Grey Zone operations, it does to a degree demonstrate how cyberspace attack-capabilities, even when freed from the reins of remaining within the Grey Zone, are not miracle means. OCOC do not provide the same ability to conduct power projection as conventional means, let alone nuclear weapons. Cyberspace attacks' usually (though, as demonstrated by NotPetya and STUXNET, not always) limited, temporary and reversible effects are different from conventional weapons' permanent and irreversible destructivity.

Also, unlike conventional weapons, advanced cyberspace attacks are not able to breach defences and deliver their effect by brute force, but are dependent on identified weaknesses in the target systems (Jensen, 2022b, p. 10). Although some systems can be attacked immediately and temporarily be disabled by simple attacks, e.g. by overwhelming them with incoming signals, advanced systems require "tailored access" by OCOC designed specifically for that purpose. Such OCOCs depend on secrecy to achieve their effect: they can only penetrate an opponent's defence if it has a flaw of which he is unaware (Libicki, 2009, pp. xiii, 18). To slip through an opponent's defences OCOCs need a technical, organizational, or procedural vulnerability that the opponent is unaware of, for example, zero-day vulnerabilities in his software or an item with internet access installed on the opponents' system with a low security setting. It could also be physical access to his system that allows electronic or physical tampering or simply an employee in the opponent's organization that has been identified as liable to click on phishing mails of a particular design (Taillat, 2019, p. 370). Once such weaknesses have been identified, e.g. by intelligence collection, tailored development of cyberspace attacks takes further time: hence weeks or months may pass between identifying a target and developing a means to take it down. Throughout this entire time, any change to the target system may render the cyberspace attack-means impotent.

Even so, cyberspace attacks does provide states new opportunities to reach out far beyond their borders and inflict very serious damage, e.g. on critical infrastructure. US' strategies acknowledge the theoretical potential for catastrophic damage from cyberspace attacks and include cyberspace attacks in the threats that the US nuclear arsenal is tasked to hedge against (Rumsfeldt, 2006, p. C–1; DOD, 2018, p. 38; Schneider, 2019, p. 856). In itself, the inherent ambiguity of OCO make it a destabilizing means with significant potential for crisis escalation (Cimbala, 2017). Decision makers have limited situational awareness (Clausewitz, 1918, p. 34). Discovering that he is under cyberattack, the victim may be left in doubt whether he has discovered the full extent of the intrusion. Lack of information on what has happened, who did it and what will happen next, combined with a lack of international norms and historical experience from empirical precedence to draw on can lead to a number of unfortunate decisions (Libicki, 2012, pp. 93–97). These include unintended escalation and/or counter strikes against third parties, especially if the victim is already under pressure, e.g., as an effect of a triggered security dilemma (Libicki, 2012, pp. 45–49).

OCOC and deterrence

Having established that OCOC's attributes are very conducive to grey zone operations, let us for a moment discuss the means' efficacy if a state should consider crossing the response threshold and respond to hostile grey zone cyberspace operations with cyberspace attacks, or declare such a policy in order to deter such attacks. Since the topic of this book is grey zone operations, it is assumed that the cyberspace attacks in question are intended to deter further attacks, but to not escalate the conflict above the threshold of armed conflict. In 2018, the US announced increased emphasis on the role of OCOC as a means for deterrence by punishment. The unclassified version of the 2018 National Cyber Strategy is kept in very general terms but is a shift towards in-domain deterrence (Trump, 2018; Smeets, 2020a)[3]. This came along with new, still classified directions for US Cyber Command, that was allegedly given a wider scope for OCO and a higher threshold before presidential authorization had to be given (Sanger, 2018). In public interviews and official hearings, Mr. Bolton, the then National Security Advisor and General Nakasone, commander of Cyber Command and NSA since 2018, have stressed the importance of the US doctrine of "persistent engagement". The persistent engagement doctrine requires the ability to be constantly present in other nations networks in order to identify threats as they develop and punish hostile actions (E. Nakashima, 2018; Nakashima, 2018; JFQ, 2019; Nakasone, 2019a, 2019b; Nakasone and Sulmeyer, 2020; Jensen, 2023b).

While it is impossible to counterfactually assess how many state sponsored cyber attacks the US would have suffered without the declared strategy based on deterrence by punishment, it is relatively clear that Russia and China apparently remain undeterred with regards to cyberspace operations. Theorists on cyber strategy have provided excellent arguments why in-domain deterrence is fraught with difficulties when it comes to OCO in the grey zone. One of the first significant contributions to cyber specific deterrence is Libicki, who dedicates several chapters to the challenges of response to OCO below the threshold of armed conflict. He states, that "attribution, predictable response, the ability to continue attack, and the lack of a counterforce option are all significant barriers." (Libicki, 2009, p. xix). Fischerkeller and Harknet further explore a number of arguments in depth why in-domain deterrence by punishment is difficult to apply by Western powers that simultaneously seek to establish norms for inter-state behavior in a rules based cyberspace (Fischerkeller and Harknett, 2017). At the same time, their article was published, Nye explained why this is so: "The United Nations Charter prohibits the use or threat of force but permits self defense in the case of armed attack (a higher threshold). As Michael Schmitt observes, "Cyber operations do not fit neatly into this paradigm because although they are 'non-forceful' (that is, non-kinetic), their consequences can range from mere annoyance to death." (Nye, 2017, p. 47). However, while Nye acknowledges these difficulties and argues for resilience, norm-building and cross-domain deterrence to be key components in deterrence strategies, he does not rule out some value of OCOC as a means for deterrence by punishment when combined with

[3] For a thorough discussion of US Cyber Deterrence, see e.g. (Wilner, 2019).

the other means. "As has been shown, retaliatory threats of punishment are less likely to be effective in the cybersphere, where the identity of the attacker is uncertain; there are many unknown adversaries; and knowing what assets can be held at risk and for how long is unclear. In that narrow use of the concept, deterrence based on threats of punishment will not play as large a role in strategies for cyberweapons as it does for nuclear weapons. Nonetheless, even though deterrence by punishment has difficulties, it remains a crucial part of the dissuasion equation in cyberspace." (Nye, 2017, p. 55).

OCOC, Small states and alliances – particular impacts

Since many of this book's potential readers are likely citizens of relatively small states whose national security strategies rest on alliances rather than independent military action, it may be useful to conclude with a note on OCOC's potential as deterrent below the threshold of armed conflict for such states. Most literature on OCOC's roles in cyber strategy and deterrence is directly or implicitly written from a great power-perspective as it analyses the direct cause-and-effect relations between a state and its opponents. Very little deals with the subject from an alliance-dependent state's perspective (Jensen, 2023a, p. 39). Over the last decade the number of alliance-dependent states that have declared that they are acquiring OCOC has risen significantly: Today this group includes more than half of NATO's members (Smeets, 2019, p. 7). Hence, OCOC are apparently seen as attractive assets by other than the major powers. However, small states should consider OCOC's limited usefulness as a stand-alone deterrence when balancing their investments in OCOC against other cyber defence means, e.g. DCO-capabilities, national CERTs and other assets supporting public-private-partnerships to attain cyber resilience across critical infrastructure. Compared to conventional means, OCOC's special characteristics, particularly their extraordinarily high dependence on operational security presents some obstacles for their use alongside allies. This is demonstrated by how NATO, unlike with any other military means, even nuclear weapons, has refrained from attempts to coordinate her members' acquisition and planning based on shared knowledge of their OCOC. Instead, NATO has developed a doctrine that merely allow OCO to be integrated in operations on an ad hoc basis without the allies sharing information of the deployed means [4].

Major powers such as the US, China and Russia, along with states that include independent military action in their national security strategies, e.g. Israel, Iran and North Korea, thus may find the threat of OCO below the threshold of armed conflict – that is; in the Grey Zone – a useful tool to support deterrence.

However, to states such as Denmark, who are demonstrably willing to use military force, but only with allies whether in the framework of UN-operations, NATO or coalitions of the willing, independent use of OCO as punishment for grey zone attacks would require a major and probably unlikely deviation from traditional national security strategies. To such states, independent use of military force, including OCO, would require higher levels of risk appetite among decision makers, than they historically have demonstrated[5]. At the same time, secrecy associated with OCO is, as demonstrated by NATO's approach to the new means, an impediment to their coordinated use in

[4] For a discussion in depth of this topic, see (Jensen, 2022b).

[5] For a thorough discussion of OCOC's effects on national security strategies and alliances from a small state-perspective, see (Jensen, 2022a)

coalitions. This may explain why while the US emphase the role of OCO, e.g. in the "persistent engagement strategy", the majority on NATO members appear to be more focusued on mitigating the threat from OCO by other means, e.g. through strategies that contribute to deterrence through resilience (Smeets, 2021).

Conclusion

This very brief discussion of OCOC's potential value as a means to conduct or defend against grey zone operations has demonstrated that the technical and tactical attributes of OCO are highly conducive to grey zone operations but less well suited to deter them.

While OCO are demonstrably not wonder weapons that on short notice can be developed and deployed to sabotage any desired critical infrastructure connected to the Internet, their stealthy nature, deployability from the safety of home and lack of physical, tangible evidence make them ideal for grey zone operations. OCO can be designed to remain below the attribution, sometimes even the detection threshold. Even when attributable, OCO are often difficult to retaliate against for states attempting to uphold a rules based international order, thus keeping them below the response threshold. From a defensive perspective, states that are expected by adversaries to include independent use of military force may convincingly include OCOC in their assets to deter said adversaries from grey zone operations. However, states that normally only use military force in the framework of alliances may include OCOC as a military means, but should be aware of the impediments to their coordinated use by alliances, and probably rely mainly on resilience and other forms of cross-domain deterrence against grey zone operations conducted through the cyber domain.

References

Bateman, J. (2022) *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications*. Washington DC: Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/files/Bateman_Cyber-FINAL21.pdf (Accessed: 5 January 2023).

Bronk, C., Collins, G. and Wallach, D. (2022) *Cyber and Information Warfare in Ukraine: What Do We Know Seven Months In?*, *Baker Institute*. Available at: https://www.bakerinstitute.org/research/cyber-and-information-warfare-ukraine-what-do-we-know-seven-months (Accessed: 16 September 2022).

Calamur, K. (2019) 'Trump Still Hasn't Condemned Russia for Meddling in the 2016 Election', *The Atlantic*, 18 April. Available at: https://www.theatlantic.com/international/archive/2019/04/trump-russia-meddling-2016-election/587518/ (Accessed: 20 October 2022).

Cimbala, S.J. (2017) 'Nuclear Crisis Management and Deterrence: America, Russia, and the Shadow of Cyber War', *The Journal of Slavic Military Studies*, 30(4), pp. 487–505. Available at: https://doi.org/10.1080/13518046.2017.1377007.

Clausewitz, C. von (1918) *On War, Vol. 1*. Translated by J.J. Graham. Kegan Paul, Trench, Trubner & C. Available at: https://oll-resources.s3.us-east-

2.amazonaws.com/oll3/store/titles/2050/Clausewitz_1380-01_EBk_v6.0.pdf (Accessed: 10 March 2021).

Demberger, A. (2022) *Merck Awarded $1.4 Billion for NotPetya After 5 Years of Legal Battle*, *Risk & Insurance*. Available at: https://riskandinsurance.com/merck-awarded-1-4-billion-for-notpetya-after-5-years-of-legal-battle/ (Accessed: 22 October 2022).

Diresta, R. *et al.* (2019) *The Tactics and Tropes of the Internet Research Agency*. United States Senate Select Committee on Intelligence (SSCI). Available at: https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf.

DOD (2018) '2018 Nuclear Posture Review'. Department of Defense. Available at: https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF (Accessed: 27 February 2022).

Falco, M.D. (2012) *STUXNET Facts Report*. Tallinn: CCDCOE. Available at: https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf.

Farwell, J.P. and Rohozinski, R. (2011) 'Stuxnet and the Future of Cyber War', *Survival*, 53(1), pp. 23–40. Available at: https://doi.org/10.1080/00396338.2011.555586.

Fireye (2020) *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor*, *FireEye*. Available at: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html (Accessed: 4 January 2021).

Fischerkeller, M.P. and Harknett, R.J. (2017) 'Deterrence is Not a Credible Strategy for Cyberspace', *Orbis*, 61(3), pp. 381–393. Available at: https://doi.org/10.1016/j.orbis.2017.05.003.

Flannery, R. (2020) *China Theft Of U.S. Information, IP One Of Largest Wealth Transfers In History: FBI Chief*, *Forbes*. Available at: https://www.forbes.com/sites/russellflannery/2020/07/07/china-theft-of-us-information-ip-one-of-largest-wealth-transfers-in-history-fbi-chief/ (Accessed: 22 October 2022).

Greenberg, A. (2018) *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, *Wired*. Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (Accessed: 26 September 2018).

Handel, M. (1990) *Weak States in the International System*. 2nd edn. Frank Cass & Co. ltd.

Harold, S.W., Libicki, M.C. and Stuth Cevallos, A. (2016) *Getting to Yes with China in Cyberspace*. Santa Monica: RAND. Available at: www.rand.org/t/rr1335.

Hüsch, P. and Jarnecki, J. (2023) *All Quiet on the Cyber Front? Explaining Russia's Limited Cyber Effects*, *RUSI*. Available at: https://www.rusi.orghttps://www.rusi.org (Accessed: 4 June 2023).

Jakobsen, P.V. (2022) ‘Understanding and teaching military strategy as theories of success at the Royal Danish Defence College (Forthcoming)’, *Scandinavian Journal of Military Studies* [Preprint], (Special Issue).

Janczewski, L.J. and Caelli, W. (2016) ‘Security of Small Countries: Summary and Model’, in L.J. Janczewski and W. Caelli (eds) *Cyber Conflicts and Small States*. 1st edn. London: Routledge. Available at: https://www-dawsonera-com.ezproxy.fak.dk/readonline/9781315575650.

Jensen, M.S. (2018) ‘Sector Responsibility or Sector Task? New Cyber Strategy Occasion for Rethinking the Danish Sector Responsibility Principle’, *Scandinavian Journal of Military Studies*, 1(1), pp. 1–18. Available at: https://doi.org/10.31374/sjms.3.

Jensen, M.S. (2022a) ‘Denmark’s Offensive Cyber Capabilities: Questionable Assets for Prestige, New Risks of Entrapment.’, *Scandinavian Journal of Military Studies*, 5(1), pp. 111–128. Available at: https://doi.org/10.31374/sjms.139.

Jensen, M.S. (2022b) ‘Five good reasons for NATO’s pragmatic approach to offensive cyberspace operations’, *Defence Studies*, pp. 1–25. Available at: https://doi.org/10.1080/14702436.2022.2080661.

Jensen, M.S. (2023a) *Offensive Cyber Capabilities and Alliances: Questionable Assets for Prestige, New Risks of Entrapment*. University of Southern Denmark. Available at: https://portal.findresearcher.sdu.dk/files/228130107/Phd_thesis_Mikkel_Storm_Jensen_2023_e_publication.pdf.

Jensen, M.S. (2023b) ‘U.S.’ Allies’ Offensive Cyber: Entrapment Risk or Entanglement Nuisance (Forthcoming)’, *The Cyber Defense Review* [Preprint].

JFQ (2019) ‘An Interview with Paul M. Nakasone’, *Joint Force Quarterly*, (92), pp. 4–9.

Joint Chiefs of Staff (2018) ‘JP 3-12 Cyberspace Operations (2018)’. US Joint Chiefs of Staff. Available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

Kostyuk, N. and Gartzke, Erik (2022) *Why Cyber Dogs Have Yet to Bark Loudly in Russia’s Invasion of Ukraine*, *Texas National Security Review*. Available at: https://tnsr.org/2022/06/why-cyber-dogs-have-yet-to-bark-loudly-in-russias-invasion-of-ukraine/ (Accessed: 27 June 2022).

Libicki, M.C. (2009) *Cyberdeterrence and cyberwar*. Santa Monica, CA: RAND. Available at: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

Libicki, M.C. (2012) *Crisis and escalation in cyberspace*. Santa Monika, Calif.: Rand Project Air Force (RAND Corporation monograph series).

Liff, A.P. (2012) ‘Cyberwar: A New “Absolute Weapon”? The Proliferation of Cyberwarfare Capabilities and Interstate War’, *The Journal of Strategic Studies*, 35(3), pp. 401–428. Available at: https://doi.org/10.1080/01402390.2012.663252.

Lindsay, J.R. (2015) ‘Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack’, *Journal of Cybersecurity*, 1(1), pp. 53–67. Available at: https://doi.org/10.1093/cybsec/tyv003.

Loleski, S. (2019) ‘From cold to cyber warriors: the origins and expansion of NSA’s Tailored Access Operations (TAO) to Shadow Brokers’, *Intelligence and National Security*, 34(1), pp. 112–128. Available at: https://doi.org/10.1080/02684527.2018.1532627.

Lonergan, E. and Poznansky, M. (2023) *Are We Asking Too Much of Cyber?*, *War on the Rocks*. Available at: https://warontherocks.com/2023/05/are-we-asking-too-much-of-cyber/ (Accessed: 4 June 2023).

Nakashima (2018) ‘White House authorizes “offensive cyber operations” to deter foreign adversaries’, *Washington Post*, 20 September. Available at: https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html (Accessed: 30 October 2020).

Nakashima, E. (2018) ‘Trump gives the military more latitude to use offensive cyber tools against adversaries’, *Washington Post*, 17 August. Available at: https://www.washingtonpost.com/world/national-security/trump-gives-the-military-more-latitude-to-use-offensive-cyber-tools-against-adversaries/2018/08/16/75f7a100-a160-11e8-8e87-c869fe70a721_story.html (Accessed: 11 March 2021).

Nakasone (2019a) ‘A Cyber Force for Persistant Operations’, *Joint Force Quarterly*, pp. 10–14.

Nakasone (2019b) ‘Statement of General Paul M. Nakasone Commander USCYBERCOM before the Senate Committee on Armed Services’. Senate Committee on Armed Services. Available at: https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf (Accessed: 30 October 2020).

Nakasone, P.M. (2022) *Posture statement of Gen. Paul M. Nakasone, commander, U.S. Cyber Command before the 117th Congress > U.S. Cyber Command > News*, *US Cyber Command*. Available at: https://www.cybercom.mil/Media/News/Article/2989087/posture-statement-of-gen-paul-m-nakasone-commander-us-cyber-command-before-the/ (Accessed: 15 September 2022).

Nakasone and Sulmeyer, M. (2020) ‘How to Compete in Cyberspace’, *Foreign Affairs* [Preprint]. Available at: https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity (Accessed: 23 October 2020).

NATO (2020) ‘AJP-3.20, Allied Joint Doctrine for Cyberspace Operations (Edition A)’. NATO Standardization Office. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.

NCSC (2018) ‘Foreign Economic Espionage in Cyberspace’. NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER. Available at: https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

Nye, J.S. (2017) ‘Deterrence and Dissuasion in Cyberspace’, *International Security*, 41(3), pp. 44–71. Available at: https://doi.org/10.1162/ISEC_a_00266.

PricewaterhouseCoopers (2018) *The scale and impact of industrial espionage and theft of trade secrets through cyber*. LU: EU Commision. Available at: https://data.europa.eu/doi/10.2873/48055 (Accessed: 14 September 2021).

Rid, T. and Buchanan, B. (2015) ‘Attributing Cyber Attacks’, *Journal of Strategic Studies*, 38(1–2), pp. 4–37. Available at: https://doi.org/10.1080/01402390.2014.977382.

Rumsfeldt, D. (2006) ‘The National Military Strategy For Cyberspace Operations’. Department of Defense. Available at: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf (Accessed: 20 August 2020).

Sanger (2018) ‘Trump Loosens Secretive Restraints on Ordering Cyberattacks’, *New York Times*. Available at: https://www.nytimes.com/2018/09/20/us/politics/trump-cyberattacks-orders.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer (Accessed: 5 October 2018).

Sanger, D.E. and Barnes, J.E. (2022) ‘Many Russian Cyberattacks Failed in First Months of Ukraine War, Study Says’, *The New York Times*, 22 June. Available at: https://www.nytimes.com/2022/06/22/us/politics/russia-ukraine-cyberattacks.html (Accessed: 23 June 2022).

Sanger, D.E. and Perlroth, N. (2020) ‘More Hacking Attacks Found as Officials Warn of “Grave Risk” to U.S. Government’, *The New York Times*, 17 December. Available at: https://www.nytimes.com/2020/12/17/us/politics/russia-cyber-hack-trump.html (Accessed: 18 December 2020).

Schechner, S. (2022) ‘Ukraine’s “IT Army” Has Hundreds of Thousands of Hackers, Kyiv Says’, *The Wall Street Journal*, 4 March. Available at: https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-04/card/ukraine-s-it-army-has-hundreds-of-thousands-of-hackers-kyiv-says-RfpGa5zmLtavrot27OWX (Accessed: 18 June 2022).

Schneider, J. (2019) ‘The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war’, *Journal of Strategic Studies*, 42(6), pp. 841–863. Available at: https://doi.org/10.1080/01402390.2019.1627209.

Sharp, T. (2017) ‘Theorizing cyber coercion: The 2014 North Korean operation against Sony’, *Journal of Strategic Studies*, 40(7), pp. 898–926. Available at: https://doi.org/10.1080/01402390.2017.1307741.

Smeets, M. (2019) ‘NATO Members’ Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis’, in. *2019 11th International Conference on Cyber Conflict:*, Tallinn: NATO CCD COE Publications, p. 15. Available at: https://ccdcoe.org/uploads/2019/06/Art_09_NATO-Members-Organizational-Path.pdf.

Smeets, M. (2020a) ‘Intelligence and National Security US cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection’. Available at: https://doi.org/10.1080/02684527.2020.1729316.

Smeets, M. (2020b) ‘NATO’s Cyber Policy 2002-2019: A very, very brief overview -’, *Cyber References Project*. Available at: http://maxsmeets.com/2019/12/natos-cyber-policy-between-2002-2019-a-very-very-brief-overview/ (Accessed: 18 August 2020).

Smeets, M. (2021) *NATO allies’ offensive cyber policy: A growing divide?*, *The Hague Centre for Strategic Studies*. Available at: https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide/ (Accessed: 24 March 2022).

Soesanto, S. (2022) ‘The IT Army of Ukraine: Structure, Tasking, and Eco-System’, p. 32 p. Available at: https://doi.org/10.3929/ETHZ-B-000552293.

Soesanto, S. (2023) ‘Ukraine’s IT Army’, *Survival*, 65(3), pp. 93–106. Available at: https://doi.org/10.1080/00396338.2023.2218701.

Søilen, K.S. (2016) ‘Economic and industrial espionage at the start of the 21st century – Status quaestionis’, *Journal of Intelligence Studies in Business*, 6(3). Available at: https://doi.org/10.37380/jisib.v6i3.196.

Steele, J. (2008) ‘Israel asked US for green light to bomb nuclear sites in Iran’, *The Guardian*, 25 September. Available at: https://www.theguardian.com/world/2008/sep/25/iran.israelandthepalestinians1 (Accessed: 22 October 2022).

Taillat, S. (2019) ‘Disrupt and restraint: The evolution of cyber conflict and the implications for collective security’, *Contemporary Security Policy*, 40(3), pp. 368–381. Available at: https://doi.org/10.1080/13523260.2019.1581458.

Trump, D. (2018) ‘National Cyber Strategy of the United States of America’. The White House. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (Accessed: 1 October 2018).

U.S. Senate Intelligence Committee (2016) *Report Of The Select Committee On Intelligence United States Senate on Russian active measures campaigns and interference in the 2016 U.S. election Volume 2: Russia’s use of social media with additional views*. Washington, D.C.: THE SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE. Available at: https://www.newknowledge.com/articles/the-disinformation-report/;

Vu, A.V. *et al.* (2022) ‘Getting Bored of Cyberwar: Exploring the Role of the Cybercrime Underground in the Russia-Ukraine Conflict’. arXiv. Available at: http://arxiv.org/abs/2208.10629 (Accessed: 6 September 2022).

Wilde, G. (2022) *Cyber Operations in Ukraine: Russia’s Unmet Expectations*. Washington D.C.: Carnegie Endowment for International Peace. Available at:

https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607 (Accessed: 14 March 2023).

Wilner, A.S. (2019) ‘US cyber deterrence: Practice guiding theory’, *Journal of Strategic Studies* [Preprint]. Available at: https://doi.org/10.1080/01402390.2018.1563779.

Yadav, T. and Rao, A. (2015) ‘Technical Aspects of Cyber Kill Chain’, in J.H. Abawaji (ed.) *SSCC 2015*. Switzerland 2015: Springer International Publishing, pp. 438–452. Available at: https://doi.org/10.1007/978-3-319-22915-7_40.

Yarger, H.R. and Bartholomees, J.B. (2012) *Toward a Theory of Strategy: Art Lykke and the U.S. Army War College Strategy Model*. Strategic Studies Institute, US Army War College, pp. 45–52. Available at: https://www.jstor.org/stable/resrep12116.6 (Accessed: 13 January 2021).