SCANDINAVIAN JOURNAL OF
MILITARY STUDIES

A Small State's Cyber Posture: Deterrence by Punishment and Beyond

RESEARCH ARTICLE

TORBJØRN PEDERSEN

SCANDINAVIAN
MILITARY STUDIES

ABSTRACT

This study explores a small-state's offensive cyber capabilities as a deterrent against great-power cyber hostilities. More specifically, it poses the question: Could Norway successfully deter hostile cyber operations of greater powers, notably China and Russia, by signaling a resolve to retaliate within the same domain? The study reviews literature on the small state's prospects of acquiring relevant offensive cyber capabilities; successfully signaling a deterrence-by-punishment posture; and, more generally, on the intricacies of retaliating against a greater power. The study concludes that most small states would enter the cyber battlefield with non-strategic and surreptitious capabilities, be inclined to signal their resolve with considerable ambiguity, and be compelled to respond with deniable means. It finds that such obscure features – the hallmarks of murky clandestine operations rather than a strategic posture – do not provide efficacious deterrence. Hence, to Norway and similar small states, deterrence by punishment may be an elusive, if not altogether vain, cyber posture.

CORRESPONDING AUTHOR:

Torbjørn Pedersen

Nord University, NO

torbjorn.pedersen@nord.no

KEYWORDS:

ambiguity; cyber deterrence; deniable means; Norway; signaling

TO CITE THIS ARTICLE:

Pedersen, T. (2023). A Small State's Cyber Posture: Deterrence by Punishment and Beyond. *Scandinavian Journal of Military Studies*, 6(1), pp. 58–68. DOI: https://doi.org/10.31374/sjms.191

INTRODUCTION

Norway and its computer networks are subject to persistent cyber hostilities. The Norwegian secret services have attributed the most aggressive operations to states such as China and Russia, the great powers boasting the planet's largest army and navy[1] and the world's largest stockpile of nuclear warheads.[2] The Norwegian Intelligence Service (2021, p. 16) declares these powers "likely have the ability to carry out destructive operations of sabotage and deterrence" against Norway inside the cyber domain. The Norwegian Police Security Service (2021, p. 8) asserts that "hostile actors at the international level … are able and willing to manipulate information and sabotage digital systems, and it is only a question of time before such operations are used to attack Norway."

With increasingly destructive attacks apparently looming, this study discusses if a small target state (i.e., Norway) can independently deter hostile cyber operations from state actors considered to be great powers in the traditional domains of land, sea, and air, as well as space (i.e., China and Russia). The small-state posture and perspective are arguably underdeveloped in scholarly literature, which some find "especially daunting when considering how small states can deter larger, militarily more powerful states" (Rivera, 2015, p. 7; see also Jensen, 2020). By using Norway as a point of departure, the study adds new perspectives to a case nation that seems to lack a comprehensive cyber strategy (Wilhelmsen et al., 2021), where public debates on offensive cyber operations are largely absent (Friis, 2020).

This study reviews three essential challenges related to the overall topic of small-state deterrence.

First, it examines a small state's prospects of acquiring a considerable offensive cyber *capability*. Second, it discusses a small state's capacity to *signal* a deterrence-by-punishment posture. Third, it debates the intricacies of small-state *retaliation* against a great power inside the cyber domain. Each of these challenges is subsequently related to the specific case of Norway. The study concludes that the sum of these challenge makes effective small-state cyber deterrence implausible. A small state would enter the cyber battlefield with non-strategic and surreptitious capabilities, be inclined to signal its resolve with considerable ambiguity, and be compelled to respond with deniable means. Such obscure ingredients, the hallmarks of clandestine operations rather than a strategic posture, can hardly provide efficacious deterrence.

While Norway is a member of the North Atlantic Treaty Organization (NATO), which has developed a comprehensive cyber operations structure and provides a historically formidable and extended deterrence to its member states, this study examines Norway's options as an autonomous small-state actor in an international system largely defined by traditional great powers.

DEFINITIONS AND CONCEPTS

A classic definition of deterrence is "the persuasion of one's opponent that the cost and/or risk of a given course of action he might take outweigh its benefits" (George & Smoke, 1974, p. 11). Developed and refined amid the Cold War, traditional deterrence theory emphasized strategic military deterrence and the virtues of second-strike nuclear capabilities. This is not easily adapted to the cyber domain – nor to a small state's perspective.

Classic deterrence suggests that the opponent's cost-benefit calculus can be affected by imposing a cost or by denying the benefits of given actions. The former corresponds with deterrence by punishment, which is discussed in this study, and the latter with deterrence by denial. A broader understanding of the concept may include deterrence by entanglement, alluding to the restraining effects of transnational interdependence, and norms, breaches of which may inflict a cost to a state's reputation and soft power (Nye, 2017).

[1] China has 975,000 active-duty personnel in army combat units and 355 navy ships and submarines, according to U.S. Department of Defense, "Military and Security Development Involving the People's Republic of China 2021."

[2] Russia has 6,255, according to Stockholm International Peace Research Institute (SIPRI), *SIPRI Yearbook 2021*.

The cyber operations discussed in this study include the set of hostile operations that a small target state would wish to deter, on one hand, and the set of latent offensive operations that may provide deterrence (by punishment) on the other. A target state may ideally seek to deter the whole specter of hostile intelligence-gathering, destruction, and/or destabilization operations conducted against its computer networks (Microsoft, 2022; Buchanan, 2022). Such operations do not necessarily amount to the use of force or an armed attack. The deterrent, on the other hand, must promise to inflict some unmistakable warfare-level (but not necessarily strategic-level) harm that can significantly alter the opponent's cost-benefit calculus (Moore, 2022). Offensive cyber operations have been defined by the U.S. Army as "missions intended to project power in and through cyberspace" (U.S. Army, 2021, pp. 2–5). Effect operations, a sub-concept more closely related to the infliction of harm, are defined as operations that "aim to disrupt, deny, degrade, or destroy" (Smeets, 2022, p. 1).

This study begins with Norway's concerns regarding hostile cyber operations carried out, principally, by Russia and China. While the study is tailored to the Norwegian security environment, the analysis is kept generic when feasible and may thus be applied to other small states facing aggression from authoritarian great powers in the cyber domain.

The following analysis, based on a thorough literary review, identifies and debates three fundamental challenges that a small state faces should it choose to pursue an offensive cyber-deterrence posture. The first challenge relates to capabilities – that is, the small state's prospects of acquiring relevant offensive cyber capabilities. The second challenge relates to signaling – the ability to signal a deterrence-by-punishment posture. The third challenge relates to retaliation – the intricacies of retaliating against a greater power.

As the findings and conclusion will demonstrate, the study's attention to deterrence by punishment over other cyber postures or means of deterrence should not be interpreted as any deprecation of these alternative strategy elements.

ANALYSIS

CHALLENGE 1: SMALL-STATE CYBER CAPABILITIES

In the cyber domain, the balance of power among states may take a different shape to that of the traditional domains. More than a decade ago, Joseph Nye Jr. (2010, p. 19) suggested that there is a diffusion of power in this domain, adding that "the low price of entry, anonymity, and asymmetries in vulnerability means that smaller actors have more capacity to exercise hard and soft power in cyberspace than in many more traditional domains of world politics."

Jason Rivera (2015, p. 7) argues that, in the cyber domain, "a nation without a strong military can hold a militarily powerful nation at risk, so long as the former is aware of their strategic advantages as well as the critical vulnerabilities of the latter." Similarly, Alexander Klimburg (2020) asserts that a small state may have a high-ground advantage in a clash with greater powers.

Others contest the notion of a small-state advantage in the cyber domain. Bjørn Svenungsen (2022) finds that cyber warfare favors economic and military great powers, thus consolidating rather than shifting contemporary balances of power and international structures. Similarly, Max Smeets (2022) points to the vast technological, organizational, and policy developments that precede sophisticated offensive cyber operations. He introduces five dimensions which capture a state's ability to conduct cyber effect operations: People, exploits, tools, infrastructure, and organization ("PETIO"). The sum of these is advantageous to greater, rather than smaller, states.

The full – and perhaps unseen – destructive potential of cyber operations remains a matter of speculation and debate. The conceptions of a "modern Pearl Harbor" (Farwell & Rohozinski, 2012, p. 112) and "Cyberwar is Coming!" (Arquilla & Ronfeldt, 1993) have gradually been replaced by the notion that "Cyberwar Will Not Take Place" (Rid, 2012) and the understanding that "cyber attacks are less destructive than we thought they would be" (Buchanan, 2022). Lennart Maschmeyer (2021) contends that cyber operations are doomed to fall short of their strategic promise due to an operational trilemma: Three variables – speed, the intensity of effect, and control – are negatively correlated. Except in rare unicorn cases, "cyber operations will tend to be too slow, too low in intensity, or too unreliable to provide significant utility" (Maschmeyer, 2021, p. 66).

The appreciation that cyber operations may not be a stand-alone strategic-level instrument does not necessarily change the fact that states would like to see others dissuaded from using them, or the fact that they can be a means of deterrence. A variety of effect operations may inflict harm, affect the opponent's cost-benefit calculus, and thus serve as a deterrent. Effect operations range from cheap distributed denial of service (DDoS) attacks that overwhelm the opponent's networks, and data manipulation, such as wipes and encryption of the opponent's data, to sophisticated manipulation of an opponent's systems (Smeets, 2022). The most prominent example of the latter is Stuxnet, the malicious code attributed to Israel and the United States that ultimately destroyed more than 1,000 Iranian centrifuges set to enrich uranium as part of Teheran's nuclear program (Zetter, 2014; Buchanan, 2022).

Arguably, even a small state's sub-strategic and surreptitious capabilities may affect the cost-benefit calculus of an aggressor and thus serve as a deterrent. To do so, the small state would have to signal a resolve to punish aggression, and the threat must be credible.

Capabilities: The Case of Norway

Any assessment of Norway's offensive cyber potential is blurred by the uncertainties discussed above. Very little is publicly known about Norway's offensive cyber capabilities and structures (Wilhelmsen et al., 2021; Liebetrau, 2022). The Norwegian Ministry of Defense (2019, p. 19) acknowledges that the responsibility for network-based intelligence operations and offensive cyber operations lies with the Norwegian Intelligence Service. Evidently, Norway has organized the offensive cyber capability in a way that integrates intelligence and military operations in one centralized structure, rather than establishing a stand-alone cyber command (Liebetrau, 2022). However, specifics remain classified. Most transparency is attached to resilience measures and *defensive* structures, including the Norwegian National Cyber Security Center (NCSC), a part of the National Security Authority, host to the Computer Emergency Response Team (CERT) and described as "Norway's national cyber security hub" (Norwegian National Security Authority, n.d.). However, these structures provide, in effect, deterrence by denial rather than deterrence by punishment.

Size alone should not hamstring Norway's ability to develop potent offensive cyber capabilities. Some of the most sophisticated attacks to date have been, at least in part, attributed to Israel, a state comparable to Norway by most size indicators, including gross domestic product (GDP) and population.[3] Small-state Israel, a cyber power engaged in a continuous exchange of offensive operations with Iran (Baram, 2022), has been partly blamed for the highly destructive Stuxnet worm, and is home to a sizable cyber industry, including the DNO Group, the developer of the notable Pegasus spyware (Bergman & Mazzetti, 2022). Likewise, the Netherlands, with an economy roughly twice the size of Norway's and three times the population, is widely perceived as a significant cyber power. Sitting next to Russia's Kola Peninsula and the world's largest concentration of nuclear capabilities, Norway may even benefit from the transfer of some offensive cyber technology from its closest ally, the United States, a cyber superpower which considers this type of transfer to selected allies.

Norway invests heavily in its intelligence service, which doubles as the nation's cyber command. For the 2023 budget, the Norwegian government proposed to increase the service's "special operating costs" to NOK 3 billion, a nominal increase of NOK 375.2 million from the previous year (Norwegian Ministry of Defense 2022, p. 93). Some of this has the express aim of boosting "operative effect," although no further details were disclosed. Intelligence-service insiders Brigt Harr Vaage and Stig Stenslie argue that the Norwegian service has moved toward "assessments and forecasts of complex problems and trends" (2021, p. 8) and away from clandestine operations. However, Norway's sophisticated capabilities are arguably betrayed by modern assets, which include a state-of-the-art array of signals intelligence (SIGINT) sensors – underwater, surface-based, and airborne alike. Some of Norway's advanced cyber capabilities have been proven through the public attribution of cyberattacks, including Russia's cyberattack on the Norwegian parliament, the Storting, in 2020 (Johansen, 2020).

[3] The Middle Eastern state, often portrayed as a superpower in the cyber domain, reached an estimated GDP of $481.6 billion in 2021, just short of Norway's $482.4 billion the same year, according to the World Bank. Their populations are similarly modest, with Israel's 9.4 million citizens and Norway's 5.4 million in 2021.

Still, the offensive cyber capabilities of Norway are not believed to amount to a *strategic* deterrent. In a joint study, five scholars conclude that Norway's cyber capabilities are primarily an instrument useful for the enhancement of the relevance and effect of other instruments. According to Wilhelmsen and her colleagues (2021, pp. 253–259), the nation's cyber capabilities are unsuitable for obtaining long-term, military-strategic objectives.

Norway's offensive cyber capabilities remain undetermined in nature and may not amount to a stand-alone strategic deterrent. However, they are assumingly capable of inflicting relevant harm – a cost – on Norway's opponents and could thereby potentially produce some degree of deterrence. A posture of retaliation would still have to be communicated to affect any opponent's cost-benefit calculus.

CHALLENGE 2: SMALL-STATE SIGNALING

"You can't have something that's a secret be a deterrent," former director of the United States Strategic Command, James Cartwright, once stated (Healey, 2012). Signaling is an integral part of any deterrence posture. The resolve to punish certain actions through retaliation must somehow be communicated clearly (Borghard & Lonergan, 2017), and the threat must be credible to be efficacious (Schelling, 1960). Hence, the posture of deterrence by punishment is inherently better suited to traditional great powers than small states.

Scholars have defined signaling as "the purposive and strategic revealing of information about intent, resolve, and/or capabilities by an actor A to alter the decisions of another actor B to improve the chances that an outcome desired by A is reached when the desired outcomes of A and B are dissimilar" (Gartzke et al., 2017, p. 5). Signaling involves a sender, a receiver or receivers, and a message. In foreign policy signaling, the message is often non-verbal. In traditional domains, for instance, armed forces may communicate a state's resolve through various physical actions, including the use of firepower, exercises, demonstrations, patrols, and visits (Blechman & Kaplan, 1978; Åtland et al., 2022).

To prevent escalation, and even spill-over to traditional domains (within which a small state is inevitably inferior), clever communication about retaliatory capacities becomes a key issue. In their pre-internet classic *Conflict Among Nations*, Glenn Snyder and Paul Diesing (1977, p. 231) allude to the use of subtle and ambiguous communication and the symbolic displays of force in peacetime; for them, the usefulness of symbolic displays lies in "the ambiguity about what is being threatened in what contingency, which preserves flexibility."

Given that offensive cyber capabilities are not easy to showcase or brandish (Libicki 2013), signaling may be the most testing and subtle art of cyber deterrence (see, for example, Borghard & Lonergan, 2017). Signaling a capability to retaliate against the opponent could easily compromise that very same capability (Gartzke, 2013), a force option diligently and painstakingly developed through the many steps of an offensive cyber-operation chain. One cyber-adapted study, modeling a signaling game between an attacker and a defender, concludes that "it is never in the best interest of the defender to perfectly signal its retaliation capability" within the cyber domain (Welburn et. al., 2019). Verbal signaling, too, has its limitations, as it is less credible. Without physical proof, the communication of cyber capability is open to swagger and bluff (Neuman & Poznansky, 2016; Jensen, 2020) and could backfire (Libicki, 2013).

Communicating red lines is perhaps as challenging as communicating an intent, resolve and/or capability to retaliate against cyber aggression. In the traditional domains, red lines have roughly been established along the thresholds recognized by international law. The United Nations Charter's Article 2(4) prohibits the use of force against other states, whereas Article 51 and customary international law establish that an armed attack against a state triggers the right to exercise individual or collective self-defense. The International Court of Justice (ICJ) defines armed attack as the gravest form of the use of force, a threshold to be determined by its "scale and effects" and the context of its "circumstances and motivations."[4] In addition to the use of force and armed attack thresholds, the UN General Assembly (2017) has recognized

[4] International Court of Justice, *Case Concerning Military and Paramilitary Activity in and Against Nicaragua* (*Nicaragua v. United States of America*), Judgement of 27 June 1986. https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf.

international wrongful acts as a threshold warranting a target state to take “nonforcible countermeasures in order to procure its cessation and to achieve reparation for the injury.”[5]

In the cyber domain, red lines are rendered largely undefined and untested. Legal scholars agree that cyberattacks may amount to the equivalent of the use of force, even an armed attack itself, as referenced by the UN Charter. However, the threshold indicators – scale, effects, circumstances, and motivations – are even more obscure in this domain.

Scholars are divided in how to translate concepts from traditional to cyber domains. Illustratively, some suggest that the destructive Stuxnet attack against Iran, discovered in 2010, should be considered an armed attack, while others argue that it did not meet the threshold that would activate Iran’s right to self-defense (Schmitt, 2017).

The lack of universal cyber norms makes a small state’s deterrence-by-punishment posture inherently adventurous. Hence, dependent on a rules-based international order, the small state would be predisposed to the communication of a posture that is vague and ambiguous rather than clear and predictable. Deliberate ambiguity is a well-established concept within strategic deterrence theory, sometimes praised for adding the certainty of uncertainty to the opponent’s decision-making processes (Baylis, 1995). In the cyber domain, however, ambiguity follows from necessity as much as strategic deliberation.

Signaling: The Case of Norway

Norway and its NATO allies recognize that serious cyber hostilities rising to the equivalent of an armed attack could invoke collective defense (Stoltenberg, 2019). NATO’s General Secretary Jens Stoltenberg does not outline the circumstances that would trigger an all-for-one, one-for-all response under Article 5 of the North Atlantic Treaty. “We will see. The level of cyber-attack that would provoke a response must remain purposefully vague,” he says, adding: “As will the nature of our response” (Stoltenberg, 2018).

Norway’s autonomous signaling and cyber posture are less developed. The government does not appear to brandish its offensive cyber capabilities. In 2019, Frank Bakke-Jensen, defense minister at the time, briefly acknowledged to national media that Norway indeed had offensive cyberweapons but declined to elaborate (Johnsen, 2019). The existence of offensive capacities is also disclosed in a handful of public documents, including a proposition from the Ministry of Defense to the Storting stating that “the responsibility for network-based intelligence operations and offensive cyber operations lays with Norwegian Intelligence Service” (Norwegian Ministry of Defense, 2019, p. 19). In a previous document, the ministry (Norwegian Ministry of Defense, 2018, p. 113) acknowledged that the intelligence service “has the national responsibility to plan and execute offensive cyber operations, including cyberattacks (Computer Network Attack).”

In 2014, the Norwegian government (Norwegian Ministry of Defense, 2014, pp. 13–14) highlighted that the right of self-defense against a cyberattack is regulated by the UN Charter’s Article 51. The threshold was high, and the right would only apply in instances such as the state being exposed to a comprehensive attack aimed at critical infrastructure, or if the cyberattack were to cause significant loss of life or material damage. Below that threshold, Norway could only implement countermeasures that do not involve the use of force (p. 14). In later documents, the Ministry of Defense has argued that it could act if necessary to avert serious threats or challenges (Norwegian Ministry of Defense, 2018). It has indicated that effect operations could indeed be used in various scenarios and above different thresholds:

> The legal basis will vary according to the circumstances, including whether effect operations are carried out within or outside the framework of armed conflict, whether the conditions for self-defense are present or whether the measure is a response to a peacetime act of international law by a foreign state actor. (Ministry of Defense, 2018, p. 113; author’s translation)

Deliberate or not, the ministry’s review leaves an impression of operational flexibility and strategic ambiguity within the cyber domain – which sums up Norway’s modest signaling.

[5] *Responsibility of States for Internationally Wrongful Acts*, Article 75.

CHALLENGE 3: SMALL-STATE RETALIATION

A deterrence-by-punishment posture must, as noted, be credible to be efficacious, and a small state's threat to retaliate against a greater power in the cyber domain is not intuitively cogent. This section discusses small-state constraints related to public attribution, escalation risk, and normative considerations.

First, retaliation requires the aggressor be identified. Complicated by the technical architecture and geography of the internet, attribution has been described as an art (Rid & Buchanan, 2015, p. 7). Still, there is a growing perception (e.g., Egloff, 2020; Rid & Buchanan, 2015) that attribution has become more achievable. If the capacity to attribute is a function of available resources and time, the great and most resourceful nations are at an advantage. Public attribution comes with a risk – and a cost. It does not carry the weight of a ruling by an international court or a resolution the UN Security Council (Hellestveit, 2022), and the wrongdoings can easily be denied by the opponent. Further, it may expose and compromise the small state's own cyber capabilities, which must be weighed against the benefits of exposing the aggressors.

Second, a small state's deterrence-by-punishment posture is only credible if the small state stands a fighting chance if push should come to shove. The defining characteristics of a small state versus a great power are, in this context, that a great power can pose an existential threat to the small state, not the other way around. For decades, the distribution of power has been seen as the constraint confining all states (Waltz, 1979), and a great power is, by one classic definition, "a state which is able to have its will" (Morgenthau, 1948, p. 129). Evidently, a small state runs a disproportionate and – potentially – existential risk in the event of escalation, since escalation in the cyber domain may spill over to domains even more favorable to traditional great powers.

If, however, the exchange may be contained to the cyber domain, some scholars argue that small states enjoy certain advantages. For instance, large nations have "more attack surface to cover," whereas smaller nations "face fewer challenges in coordinating emergency measures":

> All things considered, a number of smaller nations might actually do quite well in a force-to-force conflict with a major cyber power. The ability of many smaller nations to potentially absorb cyber blows is no less significant in a wartime scenario than advantageous defensive geography would be in a ground operation. Yet the "high ground" advantage of smaller states in presenting a smaller attack surface in the cyber domain may not have been adequately factored into analysts' calculations. (Klimburg, 2020, p. 118)

The understanding that a small state has an advantage is usually predicated on the assumption that a conflict will not escalate or spill into other domains.

Third, small-state cyber posturing is also subject to normative constraints. As already discussed, the various response thresholds – including wrongful acts, the use of force, and an armed attack – are blurred in the cyber domain, making any offensive response against a great power highly venturesome. The target state may use force in self-defense only if victim to the equivalent of an armed attack, and its countermeasures should immediately be reported to the UN Security Council[6] – including the great powers that hold permanent seats in the council. As noted, most, if not all, offensive cyber operations fall short of the armed-attack threshold, leaving a response conceptualized as punishment or retaliation disproportionate and legally questionable at best.

The sum of these constraints – the public attribution challenges, the escalation risk, and normative constraints – points in favor of using deniable means of responses to hostile cyber operations, if any at all. Plausible and implausible denials alike imply that a government considers such measures to be conceptually closely linked to covert action (Cormac & Aldrich, 2018). For Cormac and Aldrich, deniability, which can be positioned on a spectrum of comparative plausibility, allows a state to balance its resolve with other considerations, including attribution issues, the risk of escalation, and normative constraints. If the legal framework is indefinite, such "non-acknowledged intervention", they state, will remain a hallmark of offensive cyber operations, even when they are used to inflict a strategy-induced punishment against an aggressor that has been successfully attributed.

[6] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*, Rule 75 (see Schmitt, 2017).

Retaliation: The Case of Norway

In Norway, the Intelligence Service is tasked with correctly attributing cyber operations hostile to Norwegian interests to the foreign actors responsible (Norwegian Ministry of Defense, 2018). According to the Norwegian Ministry of Justice and Public Security:

> Attribution can be an instrument in itself, if the authorities wish to expose that they know who stands behind disinformation and other influence campaigns. Whether it is desirable and appropriate to hold an actor responsible for an intended act depends on the information available and the political context. (Norwegian Ministry of Justice and Public Security, 2020, p. 96; author's translation)

While the process of attribution is demanding, the Norwegian government has publicly exposed China and Russia as principal aggressors against its computer networks. However, according to the director of the Norwegian Intelligence Service, Nils Andreas Stensønes, public attribution has not deterred further attacks (Skei & Tønset, 2021).

Norway has not reported any use of effect operations in response to Chinese or Russian hostilities – neither to the UN Security Council, including permanent members China and Russia, nor to the public. Any overt use of offensive cyber operations, even in response to a cyberattack on its critical infrastructure, would have come with a great risk. Stig Tore Aannø (2018, pp. 53–54), having tested a theoretical game where a small state (Norway) adopts an overt deterrence-by-punishment posture toward a great-power opponent, argues that it is irrational for a small state to openly threaten retaliation against a great power's critical infrastructure. If the weaker state responds to an infiltration with an attack against the stronger state's infrastructure to maintain the credibility of its own deterrence, he writes, the response will soon become an act disproportionate to the act that caused it; this serves to provide conditions allowing the greater state to legitimately escalate the situation and, ultimately, respond with armed force.

The model implies that an overt strategy-by-punishment posture precipitates escalation contrary to the interests of the smaller state.

Notwithstanding this, Norway may still engage *covertly* to prevent escalation. The Norwegian Ministry of Defense (2018, p. 113) has argued that it may indeed execute effect operations in peacetime to avert serious threats or challenges. The ministry defines such operations as a response to an international wrongful act from a foreign state actor in peacetime, alluding to the United Nations resolution concerning the responsibility of states for internationally wrongful acts,[7] rather than any threshold for self-defense.

Norway faces some legal and normative constraints when operating covertly. The small state, ranked among the world's top democracies (European Intelligence Unit 2022), has a strong tradition of transparency and rule of law. These qualities have come under strain in recent times (Falch, 2018). Indeed, Norway's secret services are closely overseen by a Parliamentary Oversight Committee on Intelligence and Security Services. However, the committee has only limited access to "particularly sensitive intelligence operations abroad," which include operations targeting foreign states (EOS Committee, n.d.). Such activity, if it were to take place, would likely remain protected as "particularly sensitive information" and highly classified.

DISCUSSION AND CONCLUSION

NORWEGIAN CYBER DETERRENCE – AND BEYOND

This study has reviewed the literature on a small state's prospects of acquiring retaliatory cyber capabilities, its ability to signal a deterrence-by-punishment posture, and the intricacies of retaliating against a great power.

First, this review suggests that offensive cyber capabilities may not live up to their strategic promise. Even though the cyber domain is radically different from the traditional domains in warfare, such as land, sea, air, and space, a small state's cyber capabilities are likely to be similarly limited there. The most sophisticated and effective cyber capabilities require a vast

[7] United Nations General Assembly (December 6, 2017). Resolution A/RES/62/61 on Report of the Sixth Committee A/62/446: "Responsibility of States for International Wrongful Acts."

resource base, which tends to favor greater powers over small states. Faced with Maschmeyer's (2021) subversive trilemma, small states would be compelled to deprioritize speed and control in pursuit of deterrence, which adds an unacceptable operational risk to its cyber deterrent. Although a few small states (by traditional measures) have risen to the top divisions of cyber powers, Norway and similar states would likely enter the cyber battlefield with non-strategic and inherently surreptitious capabilities. While these cyber capabilities might still have some deterrent effect on the opponent, they are not comparable to strategic retaliatory capabilities in any traditional domain.

Second, the review demonstrates that, even if the small state had the capabilities, a deterrence-by-punishment posture is not easily signaled. The offensive capabilities can hardly be brandished, and the thresholds for responding with effect operations, including retaliation, are near impossible to establish. Relevant legal frameworks and thresholds, such as the use of force and armed attack, are untested in the cyber domain. This prevents small states from drawing red lines and communicating a predictable cyber-deterrence posture. Thus, this study argues that small states like Norway are predisposed toward signaling any deterrence-by-punishment posture with a considerable degree of ambiguity. With muddled thresholds, ambiguity becomes a matter of necessity more than strategic deliberation.

Third, this review suggests that a small-state's capacity to retaliate is highly constrained by various factors. While attribution may be possible, the evidence and methods required to achieve it may not survive daylight. Escalation is always a risk, not least for a small state that runs a disproportionate and existential risk if the crisis escalates and spills into other domains even more favorable, by definition, to traditional great powers. Legal and normative considerations may also prevent a small state from responding with cyber force, as retaliation and punishment are concepts incongrous with international law. Given these limitations, a retaliatory response with offensive cyber capabilities by a small state must be executed through deniable means rather than through overt measures.

These features – surreptitious capabilities, deliberate ambiguity, and deniable means – do not add up to an efficient small-state deterrent-by-punishment posture. They are, rather, the features of peacetime clandestine operations and the increasingly pervasive practice of persistent engagement in the cyber domain (see, for example, Friis, 2020; Buchanan, 2022; Fischerkeller & Harknett, 2017). In such a challenging domain, any endeavor to develop an autonomous and efficacious Norwegian domain-specific deterrence-by-punishment posture seems destined to fail.

FUNDING INFORMATION

Study funded by The Norwegian Ministry of Defense, Grant Number 700906.

COMPETING INTERESTS

The author has no competing interests to declare.

AUTHOR AFFILIATION

Torbjørn Pedersen orcid.org/0000-0002-3324-4752
Nord University, NO

REFERENCES

Aannø, S. (2018). *Strategisk avskrekking i det digitale rom: Finnes det rasjonelle strategier for små stater?* [Master's thesis, Forsvarets høyskole].

Arquilla, J., & **Ronfeldt, D.** (1993). Cyberwar is Coming! *Comparative Strategy*, *12*(2), 141–165. DOI: https://doi.org/10.1080/01495939308402915

Åtland, K., Nilsen, T. & **Pedersen, T.** (2022). Muscle-flexing as interstate communication: Russian NOTAM warnings off the coast of Norway, 2015–2021. *Scandinavian Journal of Military Studies*, *5*(1): 63–78. DOI: https://doi.org/10.31374/sjms.133

Baram, G. (2022, July 25). How the Cyberwar between Iran and Israel has intensified. *The Washington Post*, https://www.washingtonpost.com/politics/2022/07/25/iran-israel-cyber-war/

Baylis, J. (1995). *Ambiguity and deterrence: British nuclear strategy 1945–1964*. Oxford University Press. DOI: https://doi.org/10.1093/acprof:oso/9780198280125.001.0001

Bergman, R., & **Mazzetti, M.** (February, 28, 2022). The battle for the world's most powerful cyberweapon. *The New York Times Magazine*.

Blechman, B., & **Kaplan, S.** (1978). *Force without war: U.S. armed forces as a political instrumen*. The Brookings Institution.

Borghard, E., & **Lonergan, S.** (2017). The Logic of Coercion in Cyberspace. *Security Studies*, *26*(3), 452–481. DOI: https://doi.org/10.1080/09636412.2017.1306396

Buchanan, B. (2022). *The hacker and the state. Cyber attacks and the new normal of geopolitics*. Harvard University Press.

Cormac, R., & **Aldrich, R.** (2018). Grey is the new black: Covert action and implausible deniability. *International Affairs*, *94*(3), 477–494. DOI: https://doi.org/10.1093/ia/iiy067

Egloff, F. (2020). Public attribution of cyber intrusions. *Journal of Cybersecurity*, *6*(1), 1–12. DOI: https://doi.org/10.1093/cybsec/tyaa012

EOS Committee. (n.d.). *Area of oversight*. https://eos-utvalget.no/en/home/about-the-eos-committee/area-of-oversight/

European Intelligence Unit. (2022). *Democracy Index 2021: The China Challenge*. Report. https://www.eiu.com/n/campaigns/democracy-index-2021/

Falch, R. S. (2018). *Er digitalt grenseforsvar mot cyberspionasje forholdsmessig i den norske rettsstaten?* [Master's thesis, University of Oslo].

Farwell, J., & **Rohozinski, R.** (2012). The new reality of cyber war. *Survival*, *54*(4), 107–120. DOI: https://doi.org/10.1080/00396338.2012.709391

Fischerkeller, M., & **Harknett, R.** (2017). "Deterrence is not a credible strategy for cyberspace". *Orbis*, *61*(3), 381–393. DOI: https://doi.org/10.1016/j.orbis.2017.05.003

Friis, K. (2020). Offensive cyberoperasjoner: Den nye normalen? *Økonomi & Politik*, *3*, 30–44. DOI: https://doi.org/10.7146/okonomi-og-politik.v93iOktober.122526

Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security*, *28*(2), 41–73. DOI: https://doi.org/10.1162/ISEC_a_00136

Gartzke, E., Carcelli, S., Gannon, A., & **Zhang, J. J.** (2017). Signaling in foreign policy. In W. R. Thompson (Ed.), *Oxford research encyclopedia of politics*. Oxford University Press. DOI: https://doi.org/10.1093/acrefore/9780190228637.013.481

George, A., & **Smoke, R.** (1974). *Deterrence in American foreign policy: Theory and practice*. Columbia University Press.

Healey, J. (2012, June 4). Stuxnets are not in the U.S. national interest: An arsonist calling for better fire codes. *The New Altanticist*. https://www.atlanticcouncil.org/blogs/natosource/stuxnets-are-not-in-the-us-national-interest-an-arsonist-calling-for-better-fire-codes-1/

Hellestveit, C. (2022). Folkerett i det digitale rom. In H. Bergsjø & K. Friis (Eds.), *Digitalisering og internasjonal politikk*. Oslo Universitetsforlaget.

International Court of Justice. (1986). *Case concerning military and paramilitary activity in and against Nicaragua* (*Nicaragua v. United States of America*), Judgement of June 27. https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

Jensen, M. S. (2020). Småstater og cybervåben – nye muligheder og nye begrænsninger. *Økonomi & Politik*, *3*, 15–29. DOI: https://doi.org/10.7146/okonomi-og-politik.v93iOktober.122525

Johnsen, A. B. (2019, June 27). Forsvarsministeren bekrefter: Norge har offensive cyber-våpen. *Verdens Gang*. https://www.vg.no/nyheter/utenriks/i/4qxmR6/forsvarsministeren-bekrefter-norge-har-offensive-cyber-vaapen

Johansen, P. A. (2020, October 14). Regjeringen: Russland sto bak dataangrep på Stortinget. *Aftenposten*.

Klimburg, A. (2020). Mixed signals: A flawed approach to cyber deterrence. *Survival*, *62*(1), 107–130. DOI: https://doi.org/10.1080/00396338.2020.1715071

Libicki, M. (2013). Brandishing cyberattack capabilities. *RAND Corporation*.

Liebetrau, T. (2022). Organizing cyber capability across military and intelligence entities: Collaboration, separation, or centralization. *Policy Design and Practice*. DOI: https://doi.org/10.1080/25741292.2022.2127551

Maschmeyer, L. (2021). The subversive trilemma: Why operations fall short of expectations. *International Security*, *46*(2), 51–90. DOI: https://doi.org/10.1162/isec_a_00418

Microsoft. (2022, June 22). *Defending Ukraine: Early lessons from the cyber war*. Report.

Moore, D. (2022). *Offensive cyber operations: Understanding intangible warfare*. Hurst & Company. DOI: https://doi.org/10.1093/oso/9780197657553.001.0001

Morgenthau, H. (1948). *Politics among nations: The struggle for peace and power*. Alfred A. Knopf. DOI: https://doi.org/10.2307/2086875

Neuman, C., & **Poznansky, M.** (June 28, 2016). Swaggering in cyberspace: Busting the conventional wisdom on cyber coercion. *Texas National Security Review*.

Norwegian Intelligence Service. (2021). *Focus 2021: The Norwegian Intelligence Service's assessment of current security challenges*. Forsvaret.

Norwegian Ministry of Defense. (March 1, 2014). *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren*. Norwegian Ministry of Defense.

Norwegian Ministry of Defense. (2018). *Høringsnotat: Forslag til ny lov om Etterretningstjenesten* (Oslo: Norwegian Ministery of Defense).

Norwegian Ministry of Defense. (2019). *Prop. 1 S* (2019–2020) Proposition to the Parliament for the fiscal year 2020.

Norwegian Ministry of Defense. (2022). *Prop. 1 S* (2022–2023). Proposition to the Parliament for the fiscal year 2023.

Norwegian Ministry of Police and Public Security. (2020). *Samfunnssikkerhet i en usikker verden*. Report to *Stortinget*, Meld. St. 5 (2020–2021).

Norwegian National Security Authority. (n.d.). *Cyber security*. https://nsm.no/areas-of-expertise/cyber-security/. Accessed 1 February 2022.

Norwegian Police Security Service. (2021). *National threat assessment for 2021*. https://www.pst.no/globalassets/artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/download-the-national-threat-assessment-2021-in-english.pdf

Nye, J., Jr. (2010). *Cyber power*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf

Nye, J., Jr. (2017). Deterrence and dissuasion in cyberspace. *International Security*, *41*(3), 44–71. DOI: https://doi.org/10.1162/ISEC_a_00266

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. DOI: https://doi.org/10.1080/01402390.2011.608939

Rid, T., & **Buchanan, B.** (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37. DOI: https://doi.org/10.1080/01402390.2014.977382

Rivera, J. (2015). Achieving cyberdeterrence and the ability of small states to hold large states at risk. *7th International Conference on Cyber Conflict: Architectures in Cyberspace*. NATO CCD COE Publications. DOI: https://doi.org/10.1109/CYCON.2015.7158465

Schelling, T. (1960). *The strategy of conflict*. Yale University Press.

Schmitt, M. (2017). *Tallinn manual 2.0 on international law applicable to cyber operations*, 8th print. Cambridge University Press. DOI: https://doi.org/10.1017/9781316822524

Skei, L., & **Tønset, T. S.** (2021, December 26). E-sjefen: Russland fortsetter de digitale angrepene. *NRK*. no. https://www.nrk.no/norge/den-norske-etterretningssjefen_-russland-fortsetter-de-digitale-angrepene-1.15782971

Smeets, M. (2022). *No shortcuts: Why states struggle to develop a military cyber-force*. Hurst & Company. DOI: https://doi.org/10.1093/oso/9780197661628.001.0001

Snyder, G. H., & **Diesing, P.** (1977). *Conflict among nations: Bargaining, decision-making and system structure in international crisis*. Princeton University Press.

Stockholm International Peace Research Institute. (2021). *SIPRI Yearbook 2021*. Oxford University Press.

Stoltenberg, J. (2018, May 16). Stoltenberg provides details of NATO's cyber policy. *NATO Source*. https://www.atlanticcouncil.org/blogs/natosource/stoltenberg-provides-details-of-nato-s-cyber-policy/

Stoltenberg, J. (2019, October). NATO will defend itself. *Prospect*. https://www.prospectmagazine.co.uk/content/uploads/2019/08/Cyber_Resilience_October2019.pdf

Svenungsen, B. (2022). Digitalisering av det militære: Militære cyberkapasiteter. In H. Bergsjø & K. Friis (Eds.), *Digitalisering og internasjonal politikk*. Oslo Universitetsforlaget.

United Nations General Assembly. (2017, December 6). Resolution A/RES/62/61 on Report of the Sixth Committee A/62/446. *Responsibility of states for international wrongful acts*.

U.S. Army. (2021, August 24). *Cyberspace operations and electromagnetic warfare*. Field Manual (FM), 3–12.

U.S. Department of Defense. (2021). *Military and security development involving the People's Republic of China 2021*. Annual Report to Congress.

Vaage, B. H., & **Stenslie, S.** (2021, November 10). How good is Norwegian intelligence? *International Journal of Intelligence and Counterintelligence* (pp. 1–12). DOI: https://doi.org/10.1080/08850607.2021.1986792

Waltz, K. (1979). *Theory of international politics*. McGrawl-Hill.

Welburn, J., Grana, J., & **Schwindt, K.** (2019). Cyber deterrence or: How we learned to stop worrying and love the signal (working paper). *RAND Corporation*. DOI: https://doi.org/10.7249/WR1294

Wilhelmsen, V. R., Larsen, T., Soldal Lund, M., Svenungsen, B., & **Aannø, S. T.** (2021). Jakten på Norges militære cyberstrategi. In T. Heier (Ed.), *Militærmakt i nord*. Oslo Universitetsforlaget.

Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown Publisher.

TO CITE THIS ARTICLE:
Pedersen, T. (2023). A Small State's Cyber Posture: Deterrence by Punishment and Beyond. *Scandinavian Journal of Military Studies*, 6(1), pp. 58–68. DOI: https://doi.org/10.31374/sjms.191

Submitted: 06 December 2022
Accepted: 16 May 2023
Published: 06 June 2023