US Allies Offensive Cyber: Entrapment Risk or Entanglement Nuisance

Major Mikkel Storm Jensen, Ph.D.

INTRODUCTION

> "I would now like to say something very important for those who may be tempted to interfere in these developments from the outside. No matter who tries to stand in our way or all the more so create threats for our country and our people, they must know that Russia will respond immediately, and the consequences will be such as you have never seen in your entire history."
>
> *- Vladimir Putin's speech when Russian forces invaded Ukraine February 24, 2022.*

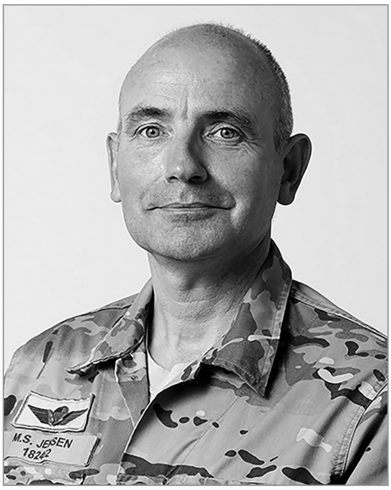
Putin's threat to escalate the war in Ukraine in response to external interference presents a timely reason to reconsider who has the military means to trigger escalation and perhaps draw allies into the conflict. In 1984, Glenn H. Snyder wrote an analysis of states' dilemmas in alliances with this issue at its core that has demonstrably had excellent explanatory and predictive power.[1] In the Cold War's technological strategic context of nuclear and conventional military means, he found that: "In general, entrapment is a more serious concern for the lesser allies than for the superpowers [...] because the superpowers have a much greater capacity for taking initiatives (notably nuclear initiatives)."[2]

In NATO, the US controls much of the alliance's conventional military capabilities and most of its nuclear weapons. Applying Snyder's analysis, this vests the US with a sufficient level of control over NATO's crisis management, to minimize the US' risk of entrapment in conflicts. Emergence of cyberspace[3] as a new venue for military operations changes the US strategic environment.[5] The US was initially NATO's only declared actor in cyberspace, but over the last decade more than half of NATO's members have begun developing offensive cyberspace operations (OCO) capabilities.[6] Based on Snyder's analysis, should the US add proliferation amongst friends and allies to its concerns over OCO proliferation amongst foes?[7]

The theoretical answer is "yes." Any increase in allies' potential for independent initiatives decreases US ability to control escalation, increasing the risk of entrapment. The real-world answer depends on the degree to which OCO has the potential for strategic impact. The counterargument is that OCO's potential military impact even in a crisis would be insignificant, thereby rendering allies' independent deployment of OCO a manageable risk insofar as entangling an otherwise involuntary US.

Hence, the question is the relative magnitude of the entrapment threat from US allies' OCO: Do US allies' growing OCO capabilities constitute a credible risk for entrapment, or are they a mere entanglement nuisance? US' strategies do not provide an answer.[8] Since 2018, they have signaled a more active role for US OCO capabilities to serve as a deterrent, both above and below the threshold of armed conflict. As yet, however, no guidance has been forthcoming as to how allies' OCO capabilities fit this intent.[9] Nor does the academic literature inform this subject, a void this article seeks to begin filling.

Following a brief review of pertinent academic literature, this article presents the theoretical tools deployed. After introducing mainly Snyder's analysis of alliance dilemmas, the theories are applied to the case of the US dominant position in NATO. The analysis then investigates OCO's influence on the outcomes of Snyder's analysis on entrapment by analyzing how the technical and operational attributes of military cyber capabilities effects differ from conventional and



Mikkel Storm Jensen (Ph.D.) is a major in the Danish army with an operational background in intelligence analysis. Since 2016, he has researched national cyber strategies. Initially on the state's role in societal resilience, but now mostly focuses on their use of cyber means for offensive purposes. This article forms part of his dissertation[4] on the influences of offensive cyber capabilities on military alliances, which he defended in May 2023.

nuclear means. It demonstrates how OCO are, in some respects, reasonable to analyze on par with nuclear weapons. The article then reviews the US-published statements and policies on her own and allies' OCO capabilities and compares with US policies during the late 1950s potential proliferation of nuclear weapons amongst NATO members.

The analysis establishes that OCO's potential for destruction is not comparable to nuclear weapons but still convincingly capable of creating strategic effects, e.g., escalation, particularly during a crisis. Thus, in Snyder's terms, OCO convincingly provides allies with new means for "independent strategic initiatives" and constitutes an entrapment risk to the US, particularly during a crisis, albeit less so than nuclear weapons. Furthermore, OCO-proliferation among US allies will be harder to detect and assess than nuclear capabilities. Also, influencing allies' decisions on OCO development will require different efforts than countering allies' nuclear proliferation. Without aspiring to recommend whether the counter proliferation of NATO allies' OCO capabilities should be a US strategy, these findings suggest that the US could consider incentivizing allies by issuing statements on how to best develop OCO capabilities to support US policy objectives.

Two final caveats should be stated before proceeding to the analysis: Firstly, the analysis is based solely on information available to the public. Hence, classified arrangements between the US and allies may exist, rendering the points on the US' lack of shared strategic intents regarding allies' OCO moot. However, the findings on allies' potential as entrapment risk and the challenges with handling that risk still hold. Secondly, this analysis fully recognizes that for most NATO allies, going against the interests of the US, particularly in crisis or war, is something they would likely be highly reluctant to do. Again, this does not change the fact that states may act irrationally or out of desperation. Hence the analysis remains relevant.

Some Literature on Military Use of Cyber and Alliances

The academic literature on OCO as military means has grown significantly over the last decade, particularly from the either explicitly or implicitly assumed great power perspective. Both theoretically, e.g., Libicki, and empirically, e.g., Brandon et al.[10] From the technical perspective, e.g., Schneider has argued why information technology represents a military revolution rather than an evolution.[11] Harknett and Smeets have reviewed the literature extensively and convincingly to discuss in what ways and how significantly offensive cyber operations can affect interstate conflict, but contribute mainly with focal points for further research.[12] Cimbala specifically investigates OCO's potential effects as a means for escalation management in general and the risks of nuclear weapons becoming involved.[13]

However, this literature is from the perspective of individual states. The literature is very limited regarding the use of OCO in or by military alliances: Taillat takes a close look at how some of the special technical and operational characteristics of OCO influence collective security in general, but do not investigate their impact on military alliances.[14] Smeets and

Fasana both discuss the values and risks of integration of offensive cyber in military operations, but neither look into its use in coalitions.[15] Relevant is also Ang's analysis of why and how small states, even if they are part of military alliances find it more difficult than large states to react to hostile activities in the cyber domain below the threshold of armed conflict.[16] Hughes and Colarik touch very briefly upon the theoretical utility of OCO within New Zealand's military cooperation with Australia.[17] However, they do not address challenges arising from the particular attribute that OCO are likely kept secret from allies. Instead, they assume that allies will share information on OCO within the Five Eyes intelligence collaboration network. Thus, Hughes et al neither question the interoperability of OCO in the coalition nor whether Australia or other allies will appreciate New Zealand's acquisition of offensive cyber or may have concerns, entrapment, or otherwise. Their assumption of information sharing is not likely to hold. Allies have strong incentives to keep OCO secret, as demonstrated by NATO's SCEPVA-framework (more on that later) for conducting OCO without sharing information.[18] White has analyzed some aspects of how cooperation in alliances on OCO and capabilities should be organized, but like Hughes et al, White does not address the challenges from classification of offensive cyber means.[19] Another aspect of potential concern over allies' OCO is provided by Jacobsen who highlights the secrecy induced technical risks to US cyber enabled intelligence collection.[20] Smeets has touched upon the threat from entrapment (as defined later in the article) to US allies from US operations conducted in or through the allies' cyberspace and also described NATO's emerging policies in the field.[21] This article aspires to enhance the academic understanding by looking at the entrapment threat from the US perspective.

ENTRAPMENT, ENTANGLEMENT, AND ABANDONMENT

The question posed in this article concerns the effect of emerging military technologies on alliances seen from the perspective of the alliance's senior partner. It is a question primarily directed toward the state's considerations and resulting actions regarding risks from being in alliances. It deals in matters of complex security and actions, perhaps clandestine, for *raison d'état* rather than based on emerging interstate norms, the composition or interpretation of alliance treaties, or strategic culture. These are core analytical parameters of Realism, making that analytical prism a reasonable choice.

Glenn H. Snyder's pioneering *The Security Dilemma In Alliance Politics* provides a standard reference Realist framework for exactly such analysis.[22] In this, Snyder investigates the risk and trade-offs for states seeking security in an anarchic international system through alliances, deploying Mandelbaum's concepts of abandonment and entrapment to depict the negative counterpoints to the states' positive objective of increased security.[23] For more detailed analysis of how the dominant ally and its security dependent allies interact, Lake's Entangling Relations provides valuable perspectives.[24]

From the US perspective, Snyder’s key concept in the present analyses is entrapment: “Entrapment means being dragged into a conflict over an ally's interests that one does not share, or shares only partially. The interests of allies are generally not identical; to the extent they are shared, they may be valued in different degree.”[25] Snyder credits Mandelbaum for the term as he identified entrapment as a strategic risk in Thycodides’ account of the Peloponnesian Wars:

> “When Corcyra seeks an alliance with Athens, the Corinthians, the enemies of Corcyra warn the Athenians that accepting the Corcyrians as allies will lead to entrapment: “You will force us to hold you equally responsible with them, although you took no part in their misdeed.”[26]

Mandelbaum, Snyder and Thucydides are all concerned with entrapment’s worst-case scenario, namely involuntary involvement in a war because of an alliance. To investigate aspects of entrapment risks with less severe consequences, the analysis draws upon Kim’s use of the term entanglement.[27] Kim renames Snyder’s entrapment entanglement and defines it as a process whereby a state is compelled to aid an ally in an unprofitable enterprise because of an alliance. Kim then redefines and reintroduces entrapment as a separate subset of entanglement: “... a form of undesirable entanglement in which the entangling state adopts a risky or offensive policy not specified in the alliance agreement.”[28]

In other words, Kim defines entanglement as a less serious, negative risk than entrapment. It should be noted that Kim’s use deviates from another use of the term “entanglement” to describe the degree to which states are formally and politically bound in an alliance. In this neutral interpretation, entangling is not necessarily harmful and may even be the defining objective of the alliance.[29] The present analysis uses Snyder’s and Mandelbaum’s term *entrapment* for the most serious risks, e.g., those that may lead to war, and Kim’s term *entanglement* for risks that have less serious, although still negative consequences.

Snyder’s other key concept is abandonment. Abandonment is, mainly when there are little or no alternatives to the dominating ally as a security guarantor, primarily a concern for the smaller, dependent allies: “alliances are never absolutely firm, whatever the text of the written agreement; therefore, the fear of being abandoned by one's ally is ever-present. Abandonment, in general, is "defection," but it may take a variety of specific forms: the ally may realign with the opponent; he may merely de-align, abrogating the alliance contract; he may fail to make good on his explicit commitments; or he may fail to provide support in contingencies where support is expected.”[30] Small allies’ fear of abandonment may lead to independent and, from the perspective of the dominating ally, entrapping actions: “Asymmetries in indirect dependence chiefly affect the partners' relative fears of abandonment. Thus, when one state has a stronger strategic interest in its partner than vice versa, the first will worry more about abandonment than the second." Security dependent allies' concerns and the resulting reactions are well demonstrated by De Gaulle's question to Kennedy In 1961: "... whether we [the US] would be ready to trade New York for Paris."[32] Thus France acquired an independent nuclear arsenal against the US wishes to ensure escalation in case of a Soviet invasion.[33]

THE US DOMINANT POSITION IN NATO AND THE RISK OF ENTRAPMENT

NATO is a relevant empirical case study of alliances: It is the US' oldest and largest collective defense arrangement. Furthermore, most NATO members have technologically advanced economies that bring OCO capabilities within their reach without significant additional investments. At least sixteen members already claim to pursue such means.[34] NATO's efforts to integrate OCO since at least 2018 provide empirical evidence to the analysis and have produced academic debate and concrete outcomes, e.g., doctrines and organizational adaptations like the Cyberspace Operations Centre (CyOC).[35] Furthermore, NATO's well-documented history allows investigation of historical analogies of emerging technologies.

Snyder argues that the threat from entrapment to alliance members, in general, is lesser the more they are in control of the alliance's capabilities for initiatives with the potential to have strategic impact.[36] Military capabilities are in this analysis considered to be of strategic value if they have the potential to significantly influence outcomes in military conflict management.[37] According to Snyder, the large US military capabilities relative to her allies, have been a key reducing factor in the risk from entrapment in NATO.[38] The threat from escalation of the war in Ukraine right on the border of NATO accentuates the relevance of assessing allies' emerging OCO-capabilities potential influence on crisis management: if allies' OCO are strategically significant, Snyder suggests they increase US risk from entrapment.

US concerns over entanglement and entrapment were present during the formation of NATO.[39] This may explain why the key Article 5 in the treaty leaves some leeway – "such action as it deems necessary" – for the allies to react in case of an attack.[40] Also, the US has mitigated NATO's nominal anarchic nature, where, in principle, a consensus is needed on every decision, by occupying key nodes and positions, e.g., SACEUR, and thus dominating not only through the US forces in Europe but also by having extensive control over the internal procedures and debates.[41]

It would be a gross mischaracterization to assert that the US has wielded unrestricted hegemonic power over the alliance at any point in NATO's history. NATO allies have often pursued policy objectives that differed from US interests, particularly when external threats were perceived as low.[42] However, the US has always been the senior partner with a decisive influence over the alliance.[43] The advantages provided by this dominant position have played a significant role in keeping the US invested in NATO after the demise of the USSR.[44]

The US position has been reinforced by European reluctance to transform economic growth into military power to the same degree as the US and exacerbated by a significant decline in conventional European capabilities after the Cold War.[45] The crisis between Russia and NATO over Ukraine highlights the European allies' military dependency on the US. Applying Snyder's analysis, the US central role in the alliance's crisis management reduces her risk of entrapment.

Aspects of the management of the war in Ukraine demonstrate the importance of US control over military actions that could lead to escalation – and hence implicitly if allies undertook them without US consent, to entrapment.[46] Military crisis management – including with cyber means - is to a large degree dependent on the opponent's perception.[47] Hence, it is vital to notice that Russia has hitherto perceived US influence in NATO as close to hegemonic, insisting on negotiating solely with the US.[48] Paraphrasing Thucydides' entrapment case, the Russian perception presents a risk that NATO allies' independent actions could lure Russia to hold the US responsible. The analysis will not discuss crisis management models,[49] but simply, recalling Mr. Putin's barely veiled nuclear threats to deter external interference in Ukraine, refer to the intuitive observation that the impact of actions initiated by allies without US knowledge or consent carries a greater risk for entrapping consequences when international tensions are high.

THE CHALLENGES FROM ALLIES' OFFENSIVE CYBER

So how does proliferation of emerging military cyber capabilities influence these dynamics? Defensive cyberspace operations (DCO) do not represent coercive means and are thus irrelevant to the question of alliances' use of military force.[50] The analytical focus should therefore be on OCO. While current NATO doctrine only distinguishes between OCO and DCO,[51] US doctrines distinguish between two different subcategories of OCO, namely cyber-enabled espionage, Cyberspace Exploitation (OCO-CE), and destructive attacks, Cyberspace Attack (OCO-CA).[52] OCO-CE are intrusive but non-destructive operations 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.[53] The US Air Force's doctrine's adds further nuances: they rename OCO-CE "cyberspace ISR" and then straddles the grey zone between exploitation and attack by dividing cyberspace attacks into Cyber Operational Preparation of the Environment (C-OPE) which are non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations, and Cyberspace Effects Operations that are actively destructive or disruptive.[54]

Compared to analog means, OCO-CE constitutes a paradigm shift in small allies' intelligence collection opportunities by widening the scope and lowering the costs and associated risks.[55] However, as espionage is not a new phenomenon, allies' OCO-CE does not per se present a new challenge to the dominant US position in NATO. Even so, OCO-CE cannot be completely discarded as an entrapment risk, as OCO-CE for the purpose of situational awareness, can be difficult to distinguish from OCO-CE conducted as preparations for cyberspace attacks: C-OPE in USAF terms. Hence, any detected intrusion may be considered threatening by the targeted entity.[56]

Cyber enabled destructive attacks, however, arguably constitutes a paradigm shift. OCO-CA's 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.[57] Hitherto, conventional military means with strategic reach or effect, e.g. an intercontinental missile force, a blue water navy or nuclear weapons, have required states to undertake obvious and significant investments and develop large military-industrial bases. Such costs have limited proliferation and the necessary infrastructure is visible from space which enables external observers to assess states' conventional and nuclear strategic capabilities' size and efficacy and may glean information regarding their owner's intent.

The emergence of OCO-CA has changed this situation and hence the strategic context. Small states can acquire the necessary means: the cost of entry into the OCO-CA capable group of states is relatively low. In principle, OCO require commercially available IT equipment and a team of qualified researchers, software developers, and operators optimized by coupling it with national intelligence services' collection capabilities.[58] OCO has unlimited geographical reach if targets are linked to the Internet. As demonstrated by STUXNET, OCO can reach air-gapped targets with some extra effort.[59] Unlike conventional strategic means, OCO do not require large military and industrial investments to develop and deploy, which means that they can be clandestinely developed with little or no recognizable signature.

Why is this important? As demonstrated above, the US dominates the decision process in NATO, reducing the risk of entrapment. Lake provides insights that supplement Snyder's on alliance dynamics based on access to information: In a hegemony, the hegemonic partner dominates the decision process of other allies e.g., whether to attack or how to react to external attacks. However, Lake argues it is difficult to eliminate local decisions, especially in the light of asymmetric information.[60] Hence, the ability to develop OCO-CA clandestinely reduces the hegemon's ability to eliminate the initiatives of other allies.

The relative ease with which OCO-CA can be developed clandestinely reinforces alliance members' inclination to keep them secret even from allies.[61] Involved software is produced by organizations typically within or associated with national intelligence services, whose highly classified and un-sharable intelligence is a prerequisite for the "tailored" part of OCO-CA capabilities with tailored access.[62] Likely even generic OCO-CA means are often kept secret at the national level – perhaps because the cyber domain is still a new and hence immature domain for conflict. Generic OCO-CA means have yet to be transferred from national intelligence organizations to regular military forces to become an everyday part of military operations on a par with other means.[63] The secrecy surrounding OCO, even in alliances, is underlined by the fact that NATO has had to develop the concept of "Sovereign Cyber Effects Provided Voluntarily by Allies," or SCEPVAs to integrate OCO-CA in operations via the Cyber Operational Command, or CyOC.[64] This allows members to offer NATO OCO-effects, without disclosing anything about what means are used and what objectives are targeted.[65] NATO's joint doctrine for cyberspace operations acknowledges that this is a suboptimal way to manage operations.[66] Still, the procedure is a compromise that allows members to support NATO operations with OCO capabilities without disclosing classified information. Historical evidence on multilateral operations involving OCO-CA is currently limited to the 2016 campaign against ISIS: the UK, Australia, and the US all deployed offensive cyber.[67] It suggests that inter-organizational de-confliction just within the US was problematic, and decisions, whether to inform let alone involve allies presented constant dilemmas.[68]

US STATED POSITIONS ON OWN AND ALLIES' OFFENSIVE CYBERSPACE CAPABILITIES

The US is relatively clear regarding the roles of her OCO: in 2018, a new National Cyber Strategy announced increased emphasis on the role of OCO as a means of deterrence by punishment. The unclassified Strategy is kept very general but is a shift towards in-domain deterrence.[69] It came alongside new, classified directions for U.S. Cyber Command (USCYBERCOM) that was allegedly given a broader scope for OCO and higher thresholds before presidential authorization had to be given.[70] In public interviews and official hearings, Mr. John Bolton, the then National Security Advisor, and General Paul Nakasone, commander of USCYBERCOM 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 nation's networks to identify threats as they develop and punish hostile actions.[71] The 2023 National Cybersecurity Strategy retains the former strategy's stated intent to disrupt and dismantle threat actors.[72]

But while US strategies are clear regarding unilateral use of OCO, available information is sparse on the US intent regarding OCO's role in alliances. Regardless of whether or not the US consider allies' OCO-capabilities desirable additions to e.g. NATO's arsenal, the lack of public statements on the subject may leave allies guessing how best to develop their military cyber capabilities. To allies, e.g., Denmark, that depend fully on US security guarantees, it is often more important how military acquisitions, whether F-35 or OCO-capabilities, contribute to strengthening the alliance with the US than how they contribute to national defense.[73]

NATO's recent developments in the field do not provide conclusive answers: In line with the rest of the article's argument that the US has a dominant position in NATO, the introduction of the CyOC and the SCEPVA procedures could be interpreted as implicit US approval of allies' emerging OCO. However, an alternative explanation could be that the US mainly sees the SCEPVA procedure to allow for US OCO in NATO operations without disclosing information on ways and means to allies.

Declassified parts of the US 2006 Strategy and the 2012 Presidential Directive mention international collaboration on defensive cyber issues.[74] DCO, including multinational collaboration, are uncontroversial regarding entrapment and occur in several arenas, including NATO.[75] None of the US strategies apparently place high value on allies' OCO capabilities. Neither does any of them mention NATO regarding OCO. The 2023-strategy mentions NATO (in sect. 5.3), but only with regards to defensive and resilience initiatives.[76] The 2006 Strategy mentions international cooperation as the very last area under the section on partnering, after industry and interagency.[77] The 2017 National Security Strategy mentions allies in just one sentence on threat information sharing and mutual assistance in attribution, defensive and hence uncontroversial tasks.[78] The 2018 National Cyber Strategy hints vaguely at multinational collaborative efforts to punish misbehavior in the cyber domain but does not mention OCO directly:

> The imposition of consequences will be more impactful and send a stronger message if it is carried out in concert with a broader coalition of like-minded states. The United States will launch an international Cyber Deterrence Initiative to build such a coalition and develop tailored strategies to ensure adversaries understand the consequences of their malicious cyber behavior. The United States will work with like-minded states to coordinate and support each other's responses to significant malicious cyber incidents, including through intelligence sharing, buttressing of attribution claims, public statements of support for responsive actions taken, and joint imposition of consequences against malign actors.[79]

This intent is reflected in a paragraph in very broad terms on collaboration in the Defense Department's cyber strategy.[80] The 2023-strategy states a similar objective in sect. 5.4. The new is not more specific than the former, but the wording *"collaborative use of all tools of statecraft"* could include OCO. As of November 2023, nothing concrete regarding this initiative has been disclosed.[81]

NUCLEAR WEAPONS – A SOMEWHAT REASONABLE COMPARISON WHEN CONSIDERING ENTRAPMENT

What justifies seeking an understanding of the emergence of OCO-CA's influence on US alliance policies in the historical case of the emergence of nuclear weapons?

Firstly, high-ranking US politicians and military officers have compared their concern over the emerging threats posed by OCO-CA to the threat from nuclear weapons, and their Russian and Chinese counterparts have expressed similar statements.[82] To the degree these perspectives influence national policy, they are relevant regardless of which degree they are reasonable from a technical perspective. Hence, the fact that some US decision makers' concerns over the emergence and proliferation of OCO-CA are comparable to their concern over nuclear weapons justifies comparison with their predecessors' concerns and policy decisions when these weapons entered the world stage.

Secondly, historical evidence suggests that technological changes in a strategic context have the potential to destabilize international relations and raise the risk of escalation, especially if they, like OCO-CA, are perceived as giving the aggressor an advantage.[83] Nye argues that even though OCO differs in many ways from nuclear weapons, lessons can be drawn from comparisons, e.g., the need to develop strategies without empirical evidence or historical experience.

> Elaborate constructs and prevailing political fashion led to expensive conclusions based on abstract formulas and relatively little evidence. [...] Cyber has the advantage that with widespread attacks by hackers, criminals, and spies, there is more cumulative evidence of a variety of attack mechanisms and of the strengths and weaknesses of various responses to such attacks. [However] no one has yet seen a cyber war, in the strict sense of the word, as defined above. [Historical disclosed attack examples] give some inklings of the auxiliary use of cyber attacks, but they do not test the full set of actions and reactions in a cyber war between states. [...] the problems of unintended consequences and cascading effects have not been experienced.[84]

The Russian full-scale invasion in 2022 of Ukraine has provided some observations regarding the efficacy of OCO in interstate war amongst near-peer opponents. As of November 2023, Russian OCO-CA appears not to have achieved significant results at neither the tactical, operational or strategic level.[85] This is not for lack of trying, though, as Russia has deployed destructive malware against Ukraine throughout the conflict along with less disruptive, but highly profiled attacks against private and government entities in states supporting Ukraine.[86] The reasons for the lack of impact of OCO-CA in the conflict are debated. Likely they are a combination of offensive and defensive factors, e.g., less competent and resourceful Russian cyber forces and better Ukrainian cyber resilience (with external support from both states and private entities) than assessed prior to the conflict.[87] However, the information available for academic analysis is still sparse at this point, and the events of this war still leaves analysts room to theorize over OCO-CA's potential.

Obviously, possession of OCO-CA capabilities does not give a small state the same ability to conduct strategic power projection as a large state's conventional means, let alone nuclear weapons. Also, OCO-CA's usually (although, as demonstrated by, e.g., NotPetya, far from always) limited, temporary, and reversible effects are completely different from nuclear weapons' spectacularly enormous, permanent, and irreversible destructivity.[88]

That said, OCO-CA does provide small states new opportunities to reach out far beyond their borders and inflict serious damage, e.g., on critical infrastructure. US strategies acknowledge the theoretical potential for catastrophic damage from OCO-CA and include them in the threats that the US nuclear arsenal is tasked to hedge against.[89]

Furthermore, as argued by, e.g., Cimbala, OCO-CA's technical and operational attributes make it a destabilizing means with significant potential for crisis escalation.[90] The ambiguities that accompany OCO-CA may further exacerbate the risk of escalation: Commanders have limited situational awareness.[91] Discovering that he is under cyberattack, the victim may be left in doubt whether he has discovered the full extent of the intrusion. Also, the process of intelligence-based attribution may be time-consuming and initially provide insufficient, low-confidence answers.[92] 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 several unfortunate decisions.[93] These include unintended escalation and counter strikes against third parties, especially if the victim is already under pressure, e.g., as an effect of a triggered security dilemma.[94]

As in the classical security dilemma, even non-destructive cyber operations with underlying defensive intent, e.g., OCO-CE intended as routine espionage to maintain normal levels of situational awareness, may be perceived as offensive – or to use the USAF's term: cyberspace operational preparation of the environment – by an opponent and trigger escalation.[95] This is especially pronounced in the cyber domain where a perceived, if debated, dominance of the offensive tends to push towards instability.[96] These properties combined with a likely lack of insight into the situational awareness and threat perceptions of the opponent(s) make OCO-CA or even OCO-CE a potentially de-stabilizing means in a crisis. Particularly if the OCO are directed (or even just perceived as directed) against the most sensitive areas, e.g., nodes in a belligerent's nuclear weapons command and control.[97] The 2018 U.S. Nuclear Posture Review specifically acknowledge the cyber threat to such nodes.[98]

Finally, there is a significant difference between the threshold for using nuclear weapons and OCO. The threshold for using nuclear weapons is arguably the highest for any military means, as it has not been used since 1945, and the means is arguably considered taboo.[99] In contrast, many states have demonstrated a very low threshold for using OCO, often below the threshold of armed conflict.[100]

To round off the discussion in Clausewitzian terms, OCO's potential for achieving positive political ends, e.g., concluding a conflict to one's advantage, is very open for debate.[101] Still, OCO's potential to achieve negative political ends, e.g., escalation of a crisis, appears convincing.[102] OCO as a means for controlling escalation in crisis and war, is largely a question of assumptions and educated guesses. The use of OCO signals in a crisis even more uncertainty than signaling with traditional military means, making escalation even more challenging to control.[103]

US ALLIES, ENTRAPMENT, AND NUCLEAR WEAPONS: A LESSON FROM THE PAST

So, if OCO-capabilities' strategic risks with regards to military crisis management, particularly during a crisis and heightened international tensions, are in some regards comparable to nuclear weapons, how did the US react in the late 1950s when some NATO allies and other friendly nations wanted to acquire their own nuclear arsenals?

A declassified National Intelligence Estimate (NIE) – a high-level strategic assessment collaboration between all the US intelligence services – on the topic from 1958 provides insights on US concerns.[104] The NIE was downgraded from secret to confidential in 1999 and declassified in 2004. Because the NIE was originally intended for internal use in the US government only, it was likely written without consideration for diplomatic signaling or politeness to either friends or foes. Hence, the analyst can arguably have high confidence in their insights into the US decision process. The NIE precedes Snyder's 1984 article on dilemmas in alliances by two decades, but the analysis precisely captures US concerns over entrapment and allies' concerns over abandonment, which is stated as a major driver for the allies' pursuit of nuclear weapons.[105]

In 1958, the UK acquired nuclear weapons in the face of stiff US opposition.[106] France had also overcome the US obstructions and was on the brink of deploying an arsenal. In Europe, West Germany, Italy, and Sweden – the last friendly nation but not a NATO member, were beginning to move towards this goal.

The NIE predicted no change in the basic international [bi-polar] system if the allies and friendly Sweden achieved some nuclear capabilities. However, while the states still regard the US alliance as essential, nuclear capabilities could render them less responsive to US policy. The NIE assessed the reduced US influence as a negative, risk-enhancing outcome and predicted that it would increase the risk for both conventional and nuclear war to an undetermined degree. "Such a development is certain to produce strain and difficulties if nothing worse" if the European allies used them "to achieve deeply felt" national aims or the weapons become available to "almost totally irresponsible governments."[107]

In accordance with Lake's theoretical expectations, the NIE indicates that while the US's dominant position in NATO helped control the political debate, it was insufficient to quell the allies' interest in acquiring nuclear weapons.[108] UK and France partially developed their arsenals out of fear of US abandonment. The French sought to keep their program clandestine until September 1958 but were unsuccessful, as the NIE detailed in July of that year. The US gained some control over the UK's arsenal by supplying its main delivery systems, leaving the UK capability somewhat reliant on US support. France, however, was able to keep its nuclear arsenal completely independent of the US.[109] West Germany was eventually dissuaded by US assurances of commitment, made credible by a massive US military presence within her borders that provided assurance but also ensured Germany's deep security dependence on the US.[110] Italy's interest in nuclear capabilities was more motivated by the pursuit of international prestige rather than immediate security concerns. After a half-hearted effort in the early fifties, Italy latched on to the German initiatives to gain leverage with the US on matters other than the nuclear issue. Hence, they were easy to dissuade.[111] Sweden aproached the US in the late fifties with requests for support for their nuclear program. They were turned down but offered to come under the US nuclear umbrella if Sweden abstained from pursuing nuclear weapons. An independent Swedish program was technically possible but so expensive that it likely undermined her conventional deterrence capabilities. Hence, Sweden gave up its efforts.[112] Instead, Sweden pursued neutrality and defensive autonomy based on extensive investment in conventional forces. However, tacit collusion and US economic and technical support were still necessary to achieve a sufficient quality of conventional forces for defensive autonomy, placing Sweden in partial dependency.[113]

Compared to the current emergence of OCO amongst NATO members, similarities and differences appear. Firstly, in 1958, the US was concerned over the potential nuclear proliferation among allies and friendly states for reasons Snyder would recognize as concerns over entrapment. Nuclear proliferation would increase their scope for strategic initiatives, undermining US control and increasing the risk of international "strain and difficulties if nothing worse" if they used them "to achieve deeply-felt" national aims.[114] Some of the US concern was founded in the recognition that allies' fear of abandonment might lead them to take independent (nuclear) actions counter to US interests. The capacity to do so was recognized as a strong motivating drive for the allies, particularly France and West Germany's pursuit of nuclear weapons. Today OCO, particularly OCO-CA, presents an entrapment risk of a similar nature—both from a technical effects-based perspective and regarding allies' possible motivations to acquire OCO. The counter-argument is that the physical impact of OCO is less catastrophically violent than that of nuclear weapons, and hence only an entanglement risk is valid and relevant. But, as demonstrated above, OCO has significant potential for influencing, e.g., escalation, especially during a crisis.

Secondly, in 1958, nuclear weapons were expensive, scientifically challenging, and required complex means for delivery, which made the allies' nuclear capabilities relatively easy for US intelligence to detect and assess.[115] Today, OCO can be developed by allies with technologically advanced economies, as most NATO members, and it can be done without leaving much in the way of an intelligence footprint. The counter-argument that OCO, unlike nuclear weapons, only constitute a risk of entanglement due to their smaller impact is again arguably less convincing because the much lower entry barrier for the acquisition of OCO makes them much more accessible, as demonstrated by the speed with which they are increasing in NATO.[116]

Finally, in 1958, despite the costs and challenges required by allies to acquire nuclear weapons and delivery means, the normal level of US political and organizational dominance over their allies was insufficient to keep them attentive to US requests. US intelligence had to discover and evaluate the allies' progress. An extraordinary military and diplomatic effort of sticks and carrots was necessary: A mixture of co-option (UK) and threats combined with positive incentives and promises of unflinching commitment (Sweden, West Germany, Italy) eventually brought most of them fully or partially back in line. Only in France's case, the efforts failed.[117] Today, NATO allies can pursue OCO capabilities independent of US scientific or material assistance and realistically with minimal insight from US intelligence in their progress. Hence, involuntary oversight through intelligence collection on allies' OCO capabilities will likely provide a lower level of insight than the US had over the allies' nuclear capabilities in 1958. Also, this means that if the US should wish to incentivize her NATO allies to develop (or refrain from developing) their OCO capabilities in particular ways, several sticks were available in 1958, e.g., withholding scientific support and means of delivery, are less efficient today. Positive and negative incentives for following agreements remain viable, but as mentioned, the verify-part of "trust but verify" on OCO will be difficult compared to nuclear weapons.

CONCLUSION

NATO Allies' OCO Capabilities Constitute an Entrapment Risk to the US

This article poses the question whether US allies' new OCO capabilities risks entrapping the US or are they more likely to merely constitute an entanglement nuisance—a question to which current literature provides little in the way of helpful answers.

The proposed argument was the following: If OCO brings into allies' reach means that can create an international crisis or seriously undermine US control of the management of a crisis, then allies OCO capabilities constitute an entrapment risk. If allies' OCO capabilities only have limited potential for military impact, they only justify minor concern and thus constitute a limited risk of nuisance due to unwanted entanglement.

The analysis explains how OCO's destruction potential of non-U.S. NATO allies falls far short of the threat of nuclear weapons. Yet this same analysis compellingly concludes that these OCO capabilities can deliver strategic effects, to include palpable escalation during an international crisis. They also are much easier to acquire and have an unlimited range, and do not require complex and costly delivery systems. Thus, in Snyder's terms, OCO convincingly provides allies with new means for "independent strategic initiatives."[118] Thus NATO and other US allies with technologically advanced economies may pose more than a minor risk of entanglement.

Recalling the caveat that NATO allies have grave incentives to adhere to US interests, the analysis finds that in extraordinary circumstances, allies' OCO constitutes an entrapment risk to the US, albeit less so than nuclear weapons. Historical evidence that OCO has been deployed by many states and on many occasions below the threshold of armed conflict suggests that states' threshold for using OCO is lower than for nuclear and even conventional means. Again, recalling the caveat, this still suggests a lower threshold for allies' independent initiatives involving OCO.

Furthermore, the acquisition of OCO can realistically be achieved clandestinely and without US scientific support or special raw materials, rendering proliferation harder to detect, and capabilities harder to assess, thus influencing allies' decisions on OCO development requires different efforts than nuclear proliferation. Positive incentives remain viable, as do negative ones if allies (with more difficulty compared to nuclear counter-proliferation) are caught violating agreements. However, the direct 1958-options of disincentives, e.g., withholding scientific support and/or access to delivery means seem less effective in the context of OCO.

The arguments above are not as such an argument for whether or not the US should discourage, condone or encourage allies to acquire OCO-capabilities. They are arguments for considering the potential influence of OCO, particularly OCO-CA, in alliances on the means' own terms as their tactical and technical properties demonstrably differ sufficiently from conventional means for it to be relevant to take these differences into account.

The findings lead to another observation: Whether or not counter-proliferation of NATO allies' OCO capabilities should be a US strategy, a clear statement from the US as to how allies can best develop OCO capabilities to support US policy objectives would provide illumination that is missing in the public discussion today. This is particularly important to allies for whom improving relations with the US is a (or even the) major factor when considering acquiring military capabilities, including for OCO.

NOTES

1. Glenn H. Snyder, "The Security Dilemma in Alliance Politics, *World Politics* 36, no. 4 (July 1984), 461–95, https://doi.org/10.2307/2010183.
2. Snyder, 484.
3. A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. DoD, :DOD Dictionary of Military and Associated Terms" (Department of Defense, 2020), 55.
4. Mikkel Storm Jensen, "Offensive Cyber Capabilities and Alliances: Questionable Assets for Prestige, New Risks of Entrapment" (Copenhagen, University of Southern Denmark, 2023), https://portal.findresearcher.sdu.dk/files/228130107/Phd_thesis_Mikkel_Storm_Jensen_2023_e_publication.pdf.
5. For a discussion of what constitutes the strategic environment, see B. J. Sokol, ed., *The Marine Corps War College Strategy Primer* (Quantico, VA: Marine Corps University Press, 2021), 13-23.
6. Max Smeets, "NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis" International Conference on Cyber Conflict, CYCON 2019-May (2019): 7, https://doi.org/10.23919/CYCON.2019.8756634.
7. Donald Trump, "National Cyber Strategy of the United States of America" (The White House, September 2018), 2-3, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf; ODNI, "ODNI Annual Threat Assessment" (Washington DC: Office of the Director of National Intelligence, 2021), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.
8. Joe Biden, "National Cybersecurity Strategy 2023" (The White House, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf; Trump, "National Cyber Strategy of the United States of America.
9. Jensen, "Offensive Cyber Capabilities and Alliances," 115,119.
10. Brandon Valeriano, Benjamin M. Jensen, and Bryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018); Martin C. Libicki, *Crisis and Escalation in Cyberspace*, RAND Corporation Monograph Series (Santa Monica, CA: Rand Project Air Force, 2012).
11. Jacquelyn Schneider, "The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War," Journal of Strategic Studies 42, no. 6 (September 2019), 884-85, https://doi.org/10.1080/01402390.2019.1627209.
12. Richard J. Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," *Journal of Strategic Studies,* 2020, https://doi.org/10.1080/01402390.2020.1732354."
13. Stephen J. Cimbala, "Nuclear Crisis Management and Deterrence: America, Russia, and the Shadow of Cyber War," The Journal of Slavic Military Studies 30, no. 4 (October 2, 2017), 487-505, https://doi.org/10.1080/13518046.2017.1377007.
14. Stéphane Taillat, "Disrupt and Restraint: The Evolution of Cyber Conflict and the Implications for Collective Security', *Contemporary Security Policy* 40, no. 3 (July 3, 2019): 368-81, https://doi.org/10.1080/13523260.2019.1581458.
15. Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly*, Fall (2018): 90-113; Kenton G Fasana, "Another Manifestation of Cyber Conflict: Attaining Military Objectives through Cyber Avenues of Approach," *Defence Studies* 18, no. 2 (2018), 167-87, https://doi.org/10.1080/14702436.2018.146266lorg/10.1080/14702436.2018.1462661.
16. Benjamin Ang, "Small States Learn Different Survival Lessons," *The Cyber Defense Review*, no. Winter/22 (2021), 92-99.
17. Daniel Hughes and Andrew Colarik, "Small State Acquisition of Offensive Cyberwarfare Capabilities: Towards Building an Analytical Framework," *Intelligence and Security Informatics,* ed. Michael Chau, G. Alan Wang, and Hsinchun Chen (11th Pacific Asia Workshop on Intelligence and Security Informatics, Cham: Springer International Publishing, 2016), 174-75.
18. Mikkel Storm Jensen, "Five Good Reasons for NATO's Pragmatic Approach to Offensive Cyberspace Operations," Defence Studies, May 30, 2022, 1-25, https://doi.org/10.1080/14702436.2022.2080661.
19. White, "Ally or Die: The Unlearned Joint Organizing Lesson and Key to Survival."
20. Jeppe T. Jacobsen, "Europe Is Developing Offensive Cyber Capabilities. The United States Should Pay Attention." Council on Foreign Relations, 2017, https://www.cfr.org/blog/europe-developing-offensive-cyber-capabilities-united-states-should-pay-attention.
21. Max Smeets, "Intelligence and National Security US Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection," 2020, https://doi.org/10.1080/02684527.2020.1729316; Max Smeets, "NATO's Cyber Policy 2002-2019: A Very, Very Brief Overview." Cyber References Project (blog), 2020, http://maxsmeets.com/2019/12/natos-cyber-policy-between-2002-2019-a-very-very-brief-overview/.

NOTES

22. Rosenberger, *Making Cyberspace Safe for Democracy*. Snyder, "The Security Dilemma in Alliance Politics;" Michael Beckley, "The Myth of Entangling Alliances: Reassessing the Security Risks of U.S. Defense Pacts." *International Security* 39, no. 4 (2015), 12.
23. Michael Mandelbaum, *The Nuclear Revolution: International Politics before and after Hiroshima* (New York: Cambridge University Press, 1981), chapter 6; Snyder, "The Security Dilemma in Alliance Politics," 466.
24. David A. Lake, *Entangling Relations* (Princeton, NJ: Princeton University Press, 1999).
25. Snyder, "The Security Dilemma in Alliance Politics," 467.
26. Mandelbaum, *The Nuclear Revolution*, 151.
27. Tongfi Kim, "Why Alliances Entangle But Seldom Entrap States," *Security Studies* 20, no. 3 (July 2011), 350-77, https://doi.org/10.1080/09636412.2011.599201.
28. Kim, 355.
29. R. E. Osgood, NATO, *The Entangling Alliance* (Chicago, 1962).
30. Snyder, "The Security Dilemma in Alliance Politics," 466.
31. Snyder, 473.
32. De Gaulle, "Foreign Relations of the United States, 1961-1963, Volume XIV, Berlin Crisis, 1961-1962 - Office of the Historian," May 31, 1961, https://history.state.gov/historicaldocuments/frus1961-63v14/d30.
33. Alexander Lanoszka, "Protection States Trust?: Major Power Patronage, Nuclear Behavior, and Alliance Dynamics" (2014), 185-88.
34. Smeets, "NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis."
35. NATO, "AJP-3.20, Allied Joint Doctrine for Cyberspace Operations (Edition A)" (NATO Standardization Office, 2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf; L. Brent, "NATO's Role in Cyberspace," *NATO Review*, February 12, 2019, https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html.
36. Snyder, "The Security Dilemma in Alliance Politics," 484.
37. Smeets, "The Strategic Promise of Offensive Cyber Operations," 92.
38. Snyder, "The Security Dilemma in Alliance Politics," 484.
39. Lawrence A. Kaplan, "The United States and the Origins of NATO 1946-1949," *The Review of Politics* 31, no. 2 (1969): 218,221.
40. Lake, Entangling Relations, 170.
41. Lake, 171.
42. C. Layne, "US Hegemony and the Perpetuation of NATO," *The Journal of Strategic Studies* 23, no. 3 (2000), 61.
43. Peter Viggo Jakobsen, "The Indispensable Enabler: NATO's Strategic Value in High-Intensity Operations Is Far Greater Than You Think," *Strategy in NATO: Preparing for an Imperfect World*, ed., L. Odgaard, 2014, 61.
44. Adrian Hyde-Price, "NATO and the European Security System - A Neo-Realist Analysis," *Theorising NATO - New Perspectives on the Atlantic Alliance* (London: Routledge, 2015), 48,50, https://doi.org/10.4324/9781315658001-3.
45. Anthony H Cordesman, "NATO and the Ukraine: Reshaping NATO to Meet the Russian and Chinese Challenge" (Washington, DC: Center for Strategic and International Studies, 2022), 5-6, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220216_Cordesman_NATO_Ukraine.pdf?cS8vKRNOdoYvg3t_y6QMZMSCpadAo90a.
46. Jack Detsch Gramer Robbie, "Biden Administration Debates Legality of Arming Ukrainian Resistance," *Foreign Policy*, February 24, 2022, https://foreignpolicy.com/2022/02/24/biden-legal-ukraine-russia-resistance/.
47. Martti J Kari, "Russian Strategic Culture in Cyberspace Theory of Strategic Culture – a Tool to Explain Russia's Cyber Threat Perception and Response to Cyber Threat Russian Strategic Culture in Cyberspace Theory of Strategic Culture – a Tool to Explain" (Ph.D. Thesis, University of Jyväskylä, 2019).
48. Fiona Hill, "Russia's Assault on Ukraine and the International Order: Assessing and Bolstering the Western Response," Brookings (blog), February 2, 2022, https://www.brookings.edu/testimonies/russias-assault-on-ukraine-and-the-international-order-assessing-and-bolstering-the-western-response/; Michael Crowley and David E. Sanger, "U.S. and NATO Respond to Putin's Demands as Ukraine Tensions Mount," *The New York Times*, January 27, 2022, sec. U.S., https://www.nytimes.com/2022/01/26/us/politics/russia-demands-us-ukraine.html.

NOTES

49. See e.g., C. Peoples, "Chapter 18: Strategic Studies and Its Critics," in S*trategy in the Contemporary World: An Introduction to Strategic Studies*, ed., John Baylis, James J. Wirtz, and Colin S. Gray, 5th edition (Oxford: Oxford University Press, 2016).
50. Robert J. Art and Robert Jervis, eds., *International Politics: Enduring Concepts and Contemporary Issues*, 12. ed (Boston: Pearson, 2015), 151-65.
51.NATO, "AJP-3.20, Allied Joint Doctrine for Cyberspace Operations (Edition A)," 16.
52. Joint Chiefs of Staff, "JP 3-12 Cyberspace Operations" (2018), U.S. Joint Chiefs of Staff, June 8, 2018), II-6, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.
53. Department of the Army, Field Manual No. 3-13 Information Operations: Doctrine, Tactics, Techniques, and Procedures, 2003, 2-11, 2-9, https://irp.fas.org/doddir/army/fm3-13-2003.pdf.
54. U.S. Air Force, Air Force Doctrine Publication 3-12, Cyberspace Operations, U.S. Air Force, February 1, 2023, 7, https://www.google.com/search?rlz=1C1GCEA_en&sxsrf=APwXEddlIDebLCjKu6M0E5rKYa0W-IB-WNA:1687337290580&q=jp+3-12+cyberspace+operations&sa=X&ved=2ahUKEwiTnMie_dP_AhXEYPEDHeFP-C8QQ1QJ6BAhHEAE.
55. Klaus Solberg Søilen, ‘Economic and Industrial Espionage at the Start of the 21st Century – Status Quaestionis’, *Journal of Intelligence Studies in Business* 6, no. 3, December 30, 2016, https://doi.org/10.37380/jisib.v6i3.196.
56. Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations* (New York: Oxford University Press, 2017), 76, https://doi.org/10.1093/acprof:oso/9780190665012.001.0001.
57. *Micheal Handel, Weak States in the International System*, 2nd ed. (Frank Cass & Co. ltd., 1990), 83.
58. Adam P Liff, ‘Cyberwar: A New “Absolute Weapon”? The Proliferation of Cyberwarfare Capabilities and Interstate War’, *The Journal of Strategic Studies* 35, no. 3 (2012), 418, https://doi.org/10.1080/01402390.2012.663252; "An Interview with Paul M. Nakasone," *Joint Force Quarterly*, no. 92 (2019): 4-9.
59. James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," Survival 53, no. 1 (2011), 23-40, https://doi.org/10.1080/00396338.2011.555586.
60. Lake, *Entangling Relations*, 55.
61. Jensen, "Five Good Reasons for NATO’s Pragmatic Approach to Offensive Cyberspace Operations."
62. Fred M. Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon & Schuster, 2016), chap. 8.
63. Pablo Breuer, Interview via Skype October 23, 2020 with Dr. Pablo Breuer, interview by Mikkel Storm Jensen; Gen. Michael V. Hayden, USAF, Ret, "The Future of Things 'Cyber,'" *Strategic Studies Quarterly* 5, no. 1, Spring 2011, 5.
64. Bernard E. Harcourt, E*xposed: Desire and Disobedience in the Digital Age* (Cambridge: Harvard University Press, 2015), 8-10. Wiesław Goździewicz, "Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)," *Cyber Defense Magazine*, November 11, 2019, https://www.cyberdefensemagazine.com/sovereign-cyber/.
65. NATO, "AJP-3.20, Allied Joint Doctrine for Cyberspace Operations (Edition A)," 11, 21.
66. NATO, 26.
67. J. Flemming, Director’s Speech at Cyber UK 2018 - GCHQ.GOV.UK, GCHQ, April 12, 2018, https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018; Mike Burgess, Director-General ASD Speech to the Lowy Institute | ASD Australian Signals Directorate, Australian Signals Directorate, March 27, 2019, https://www.asd.gov.au/publications/director-general-asd-speech-lowy-institute; Sanger and Schmitt, "U.S. Cyberweapons, Used Against Iran and North Korea, Are a Disappointment Against ISIS," *The New York Times*, June 12, 2017, https://www.nytimes.com/2017/06/12/world/middleeast/isis-cyber.html?rref=collection%2Fsectioncollection%2Ftechnology&action=click&contentCollection=technology&region=rank&module=package&version=highlights&contentPlacement=1&pgtype=sectionfront&_r=0.
68. USCYBERCOM, "USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY" (National Security Archive, November 22, 2016), https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony; Steven Loleski, "From Cold to Cyber Warriors: The Origins and Expansion of NSA’s Tailored Access Operations (TAO) to Shadow Brokers," *Intelligence and National Security* 34, no. 1 (2019), 123, https://doi.org/10.1080/02684527.2018.1532627; Nakashima, "U.S. Military Cyber Operation to Attack ISIS Last Year Sparked Heated Debate over Alerting Allies," *The Washington Post*, May 9, 2017, https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html.
69. Trump, "National Cyber Strategy of the United States of America;" Smeets, "Intelligence and National Security US Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection."

NOTES

70. Sanger, "Trump Loosens Secretive Restraints on Ordering Cyberattacks," *The New York Times*, 2018, https://www.nytimes.com/2018/09/20/us/politics/trump-cyberattacks-orders.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer.

71. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly,* 2019, 10–14; Nakasone, Statement of General Paul M. Nakasone Commander USCYBERCOM before the Senate Committee on Armed Services (Senate Committee on Armed Services, February 14, 2019), https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf; Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace," *Foreign Affairs,* August 25, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity; JFQ, "An Interview with Paul M. Nakasone;" Nakashima, "White House Authorizes 'Offensive Cyber Operations' to Deter Foreign Adversaries," *The Washington Post*, September 20, 2018, 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; Nakashima, "Trump Gives the Military More Latitude to Use Offensive Cyber Tools against Adversaries," *The Washington Post*, 2018, 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?noredirect=on&utm_term=.89e4be3895b0.

72.Biden, "National Cybersecurity Strategy 2023," 14.

73. Mikkel Storm Jensen, "Denmark's Offensive Cyber Capabilities: Questionable Assets for Prestige, New Risks of Entrapment," *Scandinavian Journal of Military Studies* 5, no. 1 (September 9, 2022), 111-128, https://doi.org/10.31374/sjms.139.

74. D. Rumsfeld, "National Military Strategy for Cyberspace Operations 2006: (Washington, DC: US DOD, 2006), 17; B. Obama, "Presidential Policy Directive/PPD-20," Presidential Policy Directive, 2012, https://fas.org/irp/offdocs/ppd/ppd-20.pdf.

75. NATO Cyber Defence Factsheet, NATO, 2021, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf.

76. Biden, "National Cybersecurity Strategy 2023," 31.

77. Rumsfeld, "National Military Strategy for Cyberspace Operations 2006," 17.

78. Trump, "National Security Strategy of the United States of America' (The White House, 2017), 20, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

79. Trump, "National Cyber Strategy of the United States of America," 21.

80. DoD, "2018 DoD Cyber Strategy and Cyber Posture Review Sharpening Our Competitive Edge in Cyberspace" (U.S. Department of Defense, 2018), 5, https://media.defense.gov/2018/Sep/18/2002041659/-1/-1/1/Factsheet_for_Strategy_and_CPR_FINAL.pdf.

81. Biden, "National Cybersecurity Strategy 2023," 32.

82. P. Cirenza, "The Flawed Analogy between Nuclear and Cyber Deterrence," *Bulletin of the Atomic Scientists* (blog), February 22, 2016, https://thebulletin.org/2016/02/the-flawed-analogy-between-nuclear-and-cyber-deterrence/.

83. Todd S. Sechser, Neil Narang, and Caitlin Talmadge, "Emerging Technologies and Strategic Stability in Peacetime, Crisis, and War," *Journal of Strategic Studies* 42, no. 6 (2019), 883, https://doi.org/10.1080/01402390.2019.1626725; Rebecca Slayton, "What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment," *International Security* 41 (2016), 72-109.

84. Joseph S Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, no. Winter 2011, 25.

85. See e.g., Jon Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications" (Washington, DC: Carnegie Endowment for International Peace, December 2022), https://carnegieendowment.org/files/Bateman_Cyber-FINAL21.pdf; J. Reddick, "Finland, Now a NATO Member, Sees an Uptick in Cyberattacks," The Record, April 21, 2023, https://therecord.media/finland-reports-uptick-in-cyberattacks-after-nato-membership; "Ministries Hit by Cyber-Attacks," Pressemelding, Government.no (regjeringen.no, July 24, 2023), https://www.regjeringen.no/en/aktuelt/ministries-hit-by-cyber-attacks/id2990098/; FMI, 'DDoS-angreb på offentlige hjemmesider under Forsvarsministeriet i december," Forsvarsministeriets Materiel- og Indkøbsstyrelse, January 4, 2023, https://www.fmi.dk/da/nyheder/2023/pm-DDoS-angreb-paa-offentlige-hjemmesider-under-Forsvarsministeriet-i-december-2022/.

86. Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," 11.

87. Bateman, 33.

88. Liff, "Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War," 416; Bryan R. Early and Victor Asal, "Nuclear Weapons and Existential Threats: Insights from a Comparative Analysis of Nuclear-Armed States," Comparative Strategy 33, no. 4 (August 8, 2014), 281, https://doi.org/10.1080/01495933.2014.941720; Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

NOTES

89. Schneider, ‘The Capability/Vulnerability Paradox and Military Revolutions: Implications for Computing, Cyber, and the Onset of War’, 856; Rumsfeld, ‘National Military Strategy for Cyberspace Operations 2006’, C–1; DOD, ‘2018 Nuclear Posture Review’ (Department of Defense, 2018), 38, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.
90. Cimbala, ‘Nuclear Crisis Management and Deterrence’.
91. Carl von Clausewitz, *On War, Vol. 1.*, trans. J.J. Graham (Kegan Paul, Trench, Trubner & Co Ltd, 1918), 34, https://oll-resources.s3.us-east-2.amazonaws.com/oll3/store/titles/2050/Clausewitz_1380-01_EBk_v6.0.pdf.
92. Jon R Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack," *Journal of Cybersecurity* 1, no. 1 (2015), 56, https://doi.org/10.1093/cybsec/tyv003.
93. Libicki, *Crisis and Escalation in Cyberspace,* 93-97.
94. Libicki, 45-49.
95. Buchanan, *The Cybersecurity Dilemma,* chap. 4.
96. Slayton, "What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment."
97. Wan Wilfred, Kastelic Andraz, and Krabill Eleanor, "The Cyber-Nuclear Nexus: Interactions and Risks" (UNIDIR, November 2021), 19, https://doi.org/10.37559/WMD/21/NRR/03.
98. 2018 Nuclear Posture Review, viii, 57.
99. Nina Tannenwald, "How Strong Is the Nuclear Taboo Today?" The Washington Quarterly 41, no. 3 (July 3, 2018): 89-109, https://doi.org/10.1080/0163660X.2018.1520553.
100. Valeriano, Jensen, and Maness, *Cyber Strategy.*
101. For a conceptual discussion on how to assess states’ “cyber power,” see Jelle J. Van Haaster, "Assessing Cyber Power," 8th International Conference on Cyber Conflict, Tallinn, 2016).
102. Clausewitz, *On War, Vol. 1.*, 42.
103. Lawrence J. Cavaiola, David C. Gompert, and Martin Libicki, "Cyber House Rules: On War, Retaliation and Escalation," Survival 57, no. 1, January 2, 2015, 81-104, https://doi.org/10.1080/00396338.2015.1008300; David C. Gompert and Martin Libicki, "Waging Cyber War the American Way," Survival 57, no. 4, July 4, 2015, 10,12, https://doi.org/10.1080/00396338.2015.1068551; Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," International Security 41, no. 3 (2016): 49.
104. CIA et al., "Development of Nuclear Capabilities by Fourth Countries: Likelihood and Consequences" (National Intelligence Estimate (NIE) No. 100-2-58 (Washington, DC: Director of Central Intelligence, 1958), https://www.cia.gov/library/readingroom/docs/DOC_0001108555.pdf.
105. CIA et al., 11.
106. Lanoszka, "Protection States Trust?: Major Power Patronage, Nuclear Behavior, and Alliance Dynamics." 176.
107. CIA et al., "Development of Nuclear Capabilities by Fourth Countries: Likelihood and Consequences" (NIE No. 100-2-58, 3, 14, 16, 18, 19.
108. CIA et al., 17; Lake, *Entangling Relations,* 55.
109. Lanoszka, "Protection States Trust?: Major Power Patronage, Nuclear Behavior, and Alliance Dynamics," 177-83, 187-89.
110. Lanoszka, 112–38.
111. L. Nuti, "Italy’s Nuclear Choices," UNISCI Discussion Papers 25, no. January (2011), 171-73.
112. Wilhelm Agrell, *Svenska Forintelsesvapen* (Falun: Historiska Media, 2002), 298-348.
113. Thomas Jonter, *The Key to Nuclear Restraint* (London: Palgrave and Macmillan, 2016), 93-124, 255-69.
114. CIA et al., "Development of Nuclear Capabilities by Fourth Countries: Likelihood and Consequences" (NIE No. 100-2-58, 18).
115. CIA et al., 11.
116. Smeets, "NATO Members’ Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," 7.
117. Lanoszka, "Protection States Trust?: Major Power Patronage, Nuclear Behavior, and Alliance Dynamics."
118. Snyder, "The Security Dilemma in Alliance Politics," 484.