2019 11th International Conference on Cyber Conflict:
Silent Battle
T. Minárik, S. Alatalu, S. Biondi,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

What are Military Cyberspace Operations Other Than War?

Brad Bigelow[1]
Principal Technical Advisor
Deputy Chief of Staff Cyberspace
SHAPE
Mons, Belgium
brad.bigelow@shape.nato.int

Abstract: NATO has recognized cyberspace as a domain of military operations, with the Cyberspace Operations Centre as the focal point for coordinating and directing effects in cyberspace in the context of Alliance operations and missions. Yet many of the threats nations face in cyberspace deliver their effects below the level of conventional armed conflict, involve systems and capabilities outside the span of military control, and do not lend themselves to traditional military response options. As concerns over the defense of critical national infrastructures and other non-military targets such as election systems and social media increase, however, many are calling for the military to take on a greater role in cyberspace outside the context of armed conflicts. This paper looks at calls for greater military involvement in cyberspace below the level of conventional armed conflict, in the context of previous doctrinal work on military operations other than war. It attempts to derive a set of equivalent principles that could be applied to military cyberspace operations performed below the level of armed conflict; it then assesses these functions in terms of whether the military should take a leading or supporting role, and what kinds of tasks, relationships, and authorities might be involved. The aims of this paper are to identify the appropriate roles for the military in cyberspace operations below the level of conflict and to highlight the importance of cross-functional coordination with civil authorities in performing these roles.

Keywords: *Cyberspace, Cyberspace Operations, Military Operations Other Than War*

[1] The views and opinions expressed in this article are those of the author alone and do not necessarily reflect those of NATO.

1. INTRODUCTION

Cyberspace is now broadly recognized as an essential element of national security. As a consequence, many nations are developing the role the military plays as an instrument of national defense. And in the case of the North Atlantic Treaty Organisation, cyberspace has been recognized as an instrument of collective defense, a domain of military operations "… in which NATO must defend itself as effectively as it does in the air, on land, and at sea" (NATO, 2016).

Much of the effort involved in developing military capabilities in cyberspace is focused on those aspects mentioned in the Warsaw Summit declaration quoted above: the "ability to protect and conduct operations across these domains" and to integrate these capabilities "into operational planning and Alliance operations and missions" (NATO, 2016). This is, in part, analogous to the recognition of airspace as a domain of military operations and the development of military air power capabilities that began in the early 20th century (Bigelow, 2002). For many nations, including the members of NATO, there has also been an explicit commitment to the employment of such capabilities in compliance with *jus in bello*, the law of armed conflict or the law of war.

Traditionally, much of military doctrine has focused on large-scale, sustained combat operations aimed at achieving national objectives or protecting national interests. Yet many of the threats that nations face in cyberspace deliver their effects below the level of conventional armed conflict, affect systems and capabilities outside the span of military control, and do not lend themselves to military response options involving combat operations. As concerns increase over the defense of critical national infrastructures and other non-military targets such as election systems and social media, many are calling for the military to take on a greater role in cyberspace outside the context of armed conflicts.

These problems are less related to large-scale combat operations than they are to what U.S. military doctrine once referred to as "Military Operations Other than War" (MOOTW): "deterring war, resolving conflict, promoting peace, and supporting civil authorities in response to domestic crises" (Joint Chiefs of Staff, 1995). Although this term is no longer used in U.S. doctrine, the concept of military operations other than war offers a useful framework within which the development of military cyberspace capabilities can be assessed.

This paper looks at calls for greater military involvement in cyberspace below the level of armed conflict in the context of previous doctrinal work on military operations other than war, including civil-military cooperation, peace support operations, and special operations. It attempts to derive a set of equivalent principles for military cyberspace operations performed below the level of armed conflict in physical domains. It then assesses these functions in terms of whether the military should take a leading or supporting role and what kinds of tasks, relationships, and authorities might be involved. The aims are to identify the appropriate roles for the military in cyberspace operations below the level of conflict and to highlight the importance of cross-functional coordination with civil authorities in performing these roles.

2. CALLS FOR A GREATER MILITARY ROLE

The security challenges now being seen in cyberspace have two fundamental and very different consequences for those implementing cyberspace as a domain of military operations. One is that of establishing cyberspace effectively as an operational domain in the context of what one might call traditional military combat operations and missions—situations in which an Area of Responsibility is defined, forces assigned, objectives set and Rules of Engagement provided, together enabling a military commander to achieve Alliance objectives while complying with the Laws of Armed Conflict. The second consequence, however, is the much more difficult problem of defining the military role in cyberspace outside this context: in other words, the nature of military cyberspace operations other than war.

Some have argued that military operations in cyberspace outside the context of armed conflict should be limited to the protection of military networks and information systems. Miriam Dunn Cavelty has flatly stated that "Militaries cannot defend the cyberspace of their country – it is no space where troops and tanks can be deployed because the logic of national boundaries does not apply" (Dunn Cavelty, 2012). Stephen J. Anderson agrees, writing that traditional concepts of national defense cannot be applied in cyberspace: "The US Navy defends the littoral territorial boundaries; air defenses, either through missile defense initiatives or alert aircraft, define airspace boundaries. Those lines are not readily identifiable in cyberspace" (Anderson, 2016). Some go even further, arguing that an active military role in peacetime cyber security undermines investment in alternative mechanisms. In a 2013 post for the Lowy Institute, Ian Wallace wrote that such efforts disincentivized "other longer-term and more sustainable efforts to address the new challenges that cyber brings to security systems" (Wallace, 2013).

Yet this debate has evolved significantly in recent years, in large part thanks to increasing evidence of state-sponsored attacks on civilian cyberspace infrastructure. In a recent paper entitled *Rethinking Cyber Security*, James Lewis has stated that "The primary source of risk in cybersecurity comes from conflict between states"

(Lewis, 2018). This assessment is echoed by the Netherlands' National Cyber Security Centrum, which concluded in its 2018 assessment that "The most significant threats are sabotage and disruption by nation-states" (National Cyber Security Centrum, 2018). As consensus on the state actor threat in cyberspace has grown, so have calls for the military to take a more active role in the defense of cyberspace.

In the 2017 U.S. Senate deliberations on increasing the Secretary of Defense's authority to conduct clandestine military cyberspace operations, Senator John McCain asserted that the need for a strong military role in peacetime was self-explanatory: "It's the Department of Defense's job to defend this nation: that's why it's called the Department of Defense" (Pomerleau, 2017). This more active role— sometimes referred to as defending forward—is reflected in recent updates to military cyber strategies. The *2018 U.S. Defense Department Cyber Strategy*, for example, states explicitly: "We are engaged in a long-term strategic competition with China and Russia" and declares that this requires (and justifies) "action in cyberspace during day-to-day competition to preserve U.S. military advantages and to defend U.S. interests" (U.S. Department of Defense, 2018). Similarly, the Netherlands' *Defence Cyber Strategy 2018*, subtitled *Investing in cyber striking power for the Netherlands*, concludes that the current security environment demonstrates that "a more active contribution from Defence within the existing structures is required" (Netherlands Ministry of Defence, 2018). Jan Kallberg and Thomas S. Cook have gone even further, stating that nations should be prepared not only to use military cyberspace forces in peacetime but to actively foster these capabilities as an alternative to armed conflict: "Cyber is no longer a mere enabler of joint operations, but instead a viable strategic option for confronting adversarial societies" (Kallberg & Cook, 2017).

3. MILITARY OPERATIONS OTHER THAN WAR: DOCTRINE

It is useful to consider these calls for a more active military role in cyberspace outside of war in the context of doctrinal work on the role of military operations other than war in general. Although early discussion of the use of military force outside large-scale conflicts stems from counterinsurgency operations and the use of Special Forces in the early days of the Vietnam conflict, the term "Military Operations Other Than War" first appeared in U.S. military training publications in the early 1980s and was formally incorporated into U.S. doctrine in 1995 with *Joint Publication 3-07, Joint Doctrine for Military Operations Other Than War* (now deleted from the official library of U.S. joint military doctrine).

JP 3-07 divided military operations into two categories: combat and non-combat, the latter constituting military operations other than war. It identified fifteen types of non-combat operations, ranging from arms control and combatting terrorism to providing support to civil authorities and humanitarian assistance, and divided these operations into two categories based on whether the operation involved the use or threat of military force. In operations involving the use or threat of force, *jus ad bellum*, the international law governing use of force as an instrument of national policy, would apply. According to *JP 3-07*, in such operations, "force or threat of its use may be required to demonstrate U.S. resolve and capability, support the other instruments of national power, or terminate the situation on favorable terms" (Joint Chiefs of Staff, 1995).

In operations not involving the use of force, the military is often acting in support of, or in close coordination with, a civilian authority—for example, in response to a natural disaster or humanitarian crisis. Even operations such as a show of force or blockades are carried out in a larger context of diplomatic objectives. In support of disaster relief or a humanitarian crisis, the military's role involves providing the organic capabilities that it maintains for the primary purpose of supporting combat operations. Army field hospitals and kitchens, for example, can provide care and comfort to civilian populations injured and displaced by a hurricane, and Navy and Air Force sealift and airlift capabilities can deliver heavy equipment to locations devastated by an earthquake. However, the military can also take the lead, as in providing capacity-building support to the military forces of another nation. As *JP 3-07* notes, such peacetime uses of military forces "helps keep the day-to-day tensions between nations below the threshold of armed conflict or war and maintains U.S. influence in foreign lands". At the time when *JP 3-07* was written, it was assumed that such operations were "usually, but not always, conducted outside of the United States" (Joint Chiefs of Staff, 1995).

In hindsight, *JP 3-07* can be seen to suffer from covering too broad a spectrum of operations. Differences in legal authorities rooted in U.S. federal laws made military operations conducted on U.S. territory in support of civil authorities very different from, for example, humanitarian assistance operations conducted in support of the Department of State outside the U.S. Similarly, arms control operations, which are normally conducted overtly and under the conditions of treaties or other international agreements, are fundamentally different from "strikes and raids", which have usually involved the use of special operations forces working through covert means under Presidential authority in the U.S. and are termed "clandestine traditional military activities".

To better address the range of military operations other than war, the U.S. has replaced the 1995 *JP 3-07* with a number of discrete doctrine publications. Activities such as peace operations, which some nations such as the United Kingdom and Australia refer to as peace support operations, are now covered by *JP 3-07, Stability* (2016). *JP 3-24* (2018) covers counterinsurgency, *JP 3-26* (2014) counterterrorism, and *JP 3-28* (2018) support to civil authorities. These clarifications greatly aid in the application of doctrinal principles to real-world problems.

For the purposes of this paper, however, the most important lesson to be drawn from *JP 3-07* is that it may no longer be useful, for cyberspace operations doctrine at least, to draw a line between military operations in war and those "other than war". This seems to be particularly true for military operations in the cyberspace domain. Michael Sulmeyer echoes the sentiment of many commentators when he states, "Today's fight in cyberspace occurs in the gray zone between war and peace" (Sulmeyer, 2018). Indeed, argues Michael Fischerkeller, an offensive military cyberspace capability "would offer many opportunities, both when used on its own and in combination with other military capabilities, to influence an adversary's decision making in pre-crisis and crisis environments" (Fischerkeller, 2017). The more important distinction, particularly when it comes to military cyberspace capabilities, is whether or not a military operation involves the use or threat of force.

To illustrate, consider the latest update of U.S. Department of Defense (DOD) doctrine on cyberspace, *JP 3-12, Cyberspace Operations*, issued in June 2018. *JP 3-12* states that there are three cyberspace missions: operations of DOD networks (DODIN Ops); Defensive Cyberspace Operations (DCO); and Offensive Cyberspace Operations (OCO). It further divides DCO into three categories: Internal Defensive Measures (DCO-IDM), "where authorized defense actions occur within the defended network or portion of cyberspace"; Response Actions (DCO-RA), "where actions are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system"; and Defense of Non-DOD Cyberspace, in which the military carries out DCO-IDM and DCO-RA missions on "any U.S. or other blue cyberspace when ordered" (Joint Chiefs of Staff, 2018).

If one accepts the premise that the most important distinction between military operations is whether they involve the threat or use of force, however, *JP 3-12* adds, rather than reduces, confusion. It is hard to understand how DCO-RA actions taken external to the defended network and without the permission of the owner of the affected system do not constitute the use of force in cyberspace. Furthermore, the explanation of the Defense of Non-DOD Cyberspace is contradictory: if, by definition, Defense of Non-DOD Cyberspace missions are carried out in "blue"—friendly, willing, cooperative—cyberspace, then they will not include actions taken external to these networks.

This confusion mirrors discussions of the concept of "active defense," which is the term most often used outside the U.S. military for DCO-RA. Scott Berinato has written, "As active defense tactics gain popularity, the term's definition and tenets have become a muddy mess. Most notably, active defense has been conflated with 'hacking back'—attacking your attackers" (Berinato, 2018). Others state that active defense measures fall into two categories: "those that have effects on systems or networks inside the organizational span of control of the defender and those that have effects on systems or networks outside that span of control"—leaving it unclear whether "outside that span of control" includes systems owned by unwilling system owners (Kehler, Lin & Sulmeyer, 2017). Former U.S. Air Force cyberspace operator Robert M. Lee, on the other hand, defines active defense as "the process of security personnel taking an active and involved role in identifying and countering threats to the system," and attributes association of the term with "hacking back" to "poor translations of active defense theory in military strategies into the field of cyber security" (Lee, 2015).

Elsewhere in *JP 3-12*, however, one can see that DCO-RA and OCO tasks are, in fact, carried out by different forces from DCO-IDM and DODIN Ops tasks. (For the sake of this discussion, DODIN Ops will hereafter be referred to as Defense network ops). DCO-IDM tasks are performed by Cyber Protection Forces, teams "organized, trained, and equipped to defend assigned cyberspace in coordination with and in support of segment owners, cybersecurity service providers (CSSPs), and users." DCO-RA and OCO tasks, on the other hand, are carried out by National Mission Teams or, when supporting a Joint Force commander, Combat Mission Teams (Joint Chiefs of Staff, 2018). These teams, in other words, exist to operate in external networks and without the permission of the owner of the affected system.

Military cyberspace forces intending to apply force or the threat of force against adversary systems must work very closely, if not side-by-side, with the elements authorized to collect intelligence and conduct reconnaissance and surveillance of these adversaries. This intelligence is essential to support the development and testing of cyberspace weapons, techniques, and tactics, to support targeting and intelligence gain/loss assessment, and, in most cases, to gain access to the systems they intend to affect. According to Sergei Boeke and Dennis Broeders: "Cyber operations are tailor-made combinations of intelligence, intrusion, and attack, and it is seldom clear where one phase ends and another begins" (Boeke & Broeders, 2018). These forces must not only develop in-depth understanding of the technical details of targeting systems but some understanding of how the adversary uses these systems in day-to-day business or operations. This typically also requires these forces to be capable of conducting covert operations and their personnel to hold special security clearances.

Contrast these constraints with the forces and personnel engaged in Defense network ops or DCO, which do not involve the use or threat of force. Here, there is far less of a dependence upon intelligence (and essentially none when it comes to knowledge of intelligence means and sources). U.S. Cyber Command, for example, distinguishes between securing systems, which it considers “threat agnostic,” protecting systems, which is “threat specific but passive,” and defending systems, “a threat and capability-focused activity designed to counter adversary strategy and capability” (U.S. Cyber Command, 2018). Likewise, while attribution of cyber-attacks is of critical importance in guiding decisions to apply offensive cyberspace capabilities in a pre-emptive or reactive manner, attribution is far less important in the majority of decisions involved in DODIN Ops or DCO tasks.

To accurately identify the appropriate roles for the military in cyberspace operations other than war, therefore, perhaps the most important distinction to be made is between military cyberspace operations that involve the use or threat of force in cyberspace and those that do not, particularly in the context of operations below the level of conventional conflicts. This can be demonstrated by contrasting the characteristics and considerations of these two different efforts.

4. MILITARY CYBERSPACE OPERATIONS INVOLVING THE USE OR THREAT OF FORCE BELOW THE LEVEL OF CONFLICT

In recent testimony before the U.S. Senate Armed Services Committee, Michael Sulmeyer proposed “two necessary conditions of posture” for U.S. military cyber mission forces to be better prepared to defend the U.S. against foreign attempts to interfere with elections. First, “Our cyber mission forces should be constantly conducting reconnaissance missions abroad to discover election-related threats to the United States and provide indicators and warnings to our forces and decision-makers.” Second, “Our cyber mission forces must be sufficiently ready to strike against targets abroad identified by reconnaissance as threats to our election” (Sulmeyer, 2018).

Although Sulmeyer’s proposal was in the specific context of reactions to Russian meddling in U.S. elections in 2016, at a more general level these two conditions apply to any application of military OCO capabilities: first, they are highly dependent upon sustained reconnaissance of potential adversaries and their systems; and second, they need to be maintained at a high level of readiness because there may be little or no warning before they need to be engaged. If a nation intends to use offensive cyberspace capabilities to precede or pre-empt kinetic operations, then operational preparation of the cyber battlefield must become “as routine as reconnaissance or surveillance of potential adversary activity” (Kehler, Lin & Sulmeyer, 2017). What does “operational preparation of the cyber battlefield" involve? Robert Chesney spells it out clearly in his analysis of the *2018 DOD Cyber Strategy*: "Intrusions into the systems of potential adversaries in order to secure access of a kind that can be exploited for disruptive or destructive effect if and when the need later arises" (Chesney, 2018).

One can also argue that military OCO requires the same framework of command and control, rules of engagement, weapons release control, and damage assessment processes whether employed below the level of conflict or not. When *JP 3-12* states that "Clearly established command relationships are crucial for ensuring timely and effective employment of forces" in cyberspace operations, it does not stipulate at what level of conflict these forces are engaged (Joint Chiefs of Staff, 2018). If, as James Lewis has written, "The implicit threshold governing cyberattack is the line between force and coercion", then this line must apply to both those authorizing the attack and those affected by it (Lewis, 2018) This is why, as C. Robert Kehler and colleagues have written, standing rules of engagement for military cyberspace operations need to be in place to inhibit the unintended escalation of conflict (Kehler, Lin & Sulmeyer, 2017).

Recognizing the unique role of the military in conducting OCO—whether below the level of conflict or not—would also improve the ability of a nation to plan and organize how it deals with deterrence in cyberspace. Alex Wilner has written that the U.S. continues to struggle to understand which government agency or department is expected to engage in cyber deterrence: "To date, the division of labor remains uncertain" (Wilner, 2017). Of course, while some argue that a ready military OCO capability is essential to ensuring deterrence in cyberspace, others have suggested that deterrence in cyberspace is an impossible goal. But one good reason to clearly establish the unique military role of such a capability is to counter attempts to create OCO capabilities in the private sector. As Peter Singer testified before the U.S. House of Representatives in 2017, allowing companies to engage in OCO "is a very bad idea. It's is a bad idea for the same reason that vigilantism in general is a bad idea." Singer pointed out that such activities could raise significant risks at the international level because other nations could mistake private attempts to attack their systems for state-sponsored actions (US House of Representatives, 2017).

Establishing a military capability to conduct OCO below the level of conflict may be one key to realizing the unique benefits of cyberspace as an operational domain. Gregory Rattray and Jason Healey have argued that: "It may be that the future of cyber conflict is not equivalent to larger, theatre-level warfare but only to select covert attacks which could range across a wide set of goals and targets." In part, this argument draws upon the substantial base of experience showing that offensive operations between nations using conventional forces are relatively rare and usually condemned by other states (Rattray & Healey, 2010). But conventional offensive operations are also quite visible, are easy to attribute, and raise higher risks of escalation, which is why they have traditionally been seen as "a last resort and a temporary state" (Maurer, 2012).

OCO below the level of conflict, on the other hand, demonstrates the potential for states to exploit "grey zones"—areas where "international law principles and rules that are poorly demarcated or are subject to competing interpretations" (Schmitt, 2017). The willingness to operate in this "grey zone" is clearly demonstrated in the *2018 DOD Cyber Strategy*, which states that in the U.S. "the Department seeks to pre-empt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident regardless of whether that incident would impact DoD's warfighting readiness or capability." In the United Kingdom, Defence Minister Sir Michael Fallon called for "new doctrine to clarify our response within NATO to anonymous cyber activity which often takes place now in that grey zone below the previously understood threshold of war" (Fallon, 2017). A similar appetite is demonstrated in the Netherlands' *Defence Cyber Strategy 2018*, which states an intent to focus Defence support for civil authorities "on the vital infrastructure through closer collaboration with the responsible security partners" such as the National Cyber Security Centre (NCSC) (Netherlands Ministry of Defence, 2018). And in Germany, Defense Minister Ursula von der Leyen has stated that the Bundeswehr's cybersecurity forces are permitted to "offensively defend" their networks if attacked (Somaskanda, 2018).

NATO heads of state and governments have also recognized the value in leaving some amount of "greyness" in the "grey zone," as Jonatan Vseviov, the permanent secretary of the Estonian Ministry of Defence, explained in an interview: "there is a good level of what I would call 'constructive ambiguity' built into the wording of the Washington Treaty and also Article 5…. We don't want to give anybody a list of attacks that would trigger Article 5 because that would obviously mean that we automatically also create a list of potential attacks that would not trigger Article 5" (Mehta, 2018). The willingness of nations to consider use of OCO capabilities below the level of conflict is also a recognition that, as Michele Flournoy and Michael Sulmeyer have written, "for all the increasingly vehement warnings about a cyber Pearl Harbor, states have shown little appetite for using cyberattacks for large-scale destruction. The immediate threat is more corrosive than explosive" (Flournoy & Sulmeyer, 2018). All of which suggests that OCO can fulfil the vision proposed by Bernard Brodie at the dawn of the nuclear age: "Thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them" (Brodie, 1946).

From a doctrinal standpoint, however, the importance of recognizing OCO as a type of military operation that can be carried out not only in "war"—large-scale armed conflicts—but below the level of crisis, in the context of *jus ad bellum*, is that such capabilities cannot be employed in any context unless they are ready at the time of need. For conventional forces to be ready to act on short notice, they have to exist. They have to be equipped, armed, trained, sustained, able to move, informed about their potential adversaries, positioned to able to engage within their required readiness timelines—even though they may never need to move past that point of readiness and actually engage in battle. The same is true for cyberspace forces.

5. MILITARY CYBERSPACE OPERATIONS NOT INVOLVING THE USE OR THREAT OF FORCE

Readiness is just as critical for Defense network ops and DCO, if far less controversial. Today's militaries depend upon myriad networks, information systems, and communications transmission systems operating at different levels of classification and involving a wide variety of static, deployable, strategic, operational, tactical, and commercial systems and services. They also depend to a greater or lesser extent on the "littorals" of cyberspaces—the places where cyberspaces meet other environments, including physical infrastructure such as fences, buildings, gates, and transportation networks, the radio frequency spectrum, and critical infrastructures such as electrical power and water supplies (Withers, 2015). Many of these systems must be in constant operation to support standing tasks as well as to meet their readiness requirements, and consequently, must be protected against threats to their availability, confidentiality, and integrity.

This level of readiness raises the possibility that some of these capabilities can be employed below the level of conflict in support of some of the types of non-combat operations identified in *JP 3-07*, such as providing support to civil authorities and humanitarian assistance. In the case of a natural disaster, combat deployable communications and information systems could be used to restore or augment critical civil communications capabilities while the damaged infrastructure is being repaired. The U.S. Defense Information Systems Agency, for example, put its Transnational Information Sharing Cooperation network, which was still in preparation, into live operation in January 2010 to support U.S. Southern Command efforts to coordinate relief operations following a devastating earthquake in Haiti (Chossudovsky, 2010).

Effectively employing these capabilities in support of civil authorities, however, remains a relatively immature aspect of military cyberspace operations. For one thing, when the support takes place within the nation's borders, there can be complex legal and regulatory constraints, which stem in part from the aim of maintaining civil control over military affairs. This is illustrated by the use of the terms "secure" and "defend" in distinguishing whether the DOD or the Department of Homeland Security (DHS) is the lead agency. *JP-3-28, Defense Support of Civil Authorities*, states that the DOD "is the lead agency for homeland defense," while *JP 3-12, Cyberspace Operations*, states that the DHS is the lead agency for homeland security, including the responsibility to "safeguard and secure cyberspace" (Joint Chiefs of Staff, 2013), (Joint Chiefs of Staff, 2018).

In addition, while there is general agreement that the military should play some role in responding to cyber incidents with national-level impacts, the precise nature of this role, what responsibilities and authorities are required to perform it, and how it relates to the roles performed by civil authorities are still unclear. In some nations, even the statutory foundation for such cooperation is lacking. Piret Pernik found that Finnish Defence Forces had not been assigned any responsibility to support civil authorities in the event of a "cyber emergency" (Pernik, 2018). A 2013 assessment by the U.K. House of Commons suggested that the role was similar to that associated with other military capabilities such as medical and logistical resources: in the event of a large-scale cyberattack, the military could be drawn upon to provide "additional staff, planning resources or technical expertise" (House of Commons Defence Committee, 2012). *JP 3-12* notes that the military may be called upon to perform DCO in support of civil authorities, but a 2016 study by the U.S. Government Accountability Office (GAO) found that the DOD's basic doctrine publication on defense support of civil authorities (DSCA), *JP 3-28*, "does not provide specific details on how DOD will provide cyber support to civil authorities" (U.S. Government Accountability Office, 2016). A subsequent GAO report published in 2017 found that the DOD had not yet developed a plan for "collective training activities that are integrated with exercises conducted with other agencies and state and local governments" (U.S. Government Accountability Office, 2017).

Nations attempting to develop the military role in the defense of non-military domestic networks are running into "grey zone" challenges of their own. Although protection of critical infrastructures against cyber-attacks has been a topic at the national policy level since President Clinton established the President's Commission on Critical Infrastructure Protection in 1996, views on the appropriate role for the military to play remain divided. Some argue that any such involvement would represent a militarization of cyberspace as a whole. Others suggest the role is limited to that of offering OCO as a response option. Alex Wilner, for example, has written "It is not clear, however, if Cyber Command has a role to play in protecting both military and civilian cyber infrastructure. It may chiefly respond to attacks on the former, despite the fact that civilian cyber infrastructure appears far more vulnerable than military infrastructure to cyber-attack" (Wilner, 2017).

There is some merit to this argument. The development of military cyberspace capabilities has, from the very beginning, suffered from the inappropriate use of analogies from conventional domains. The military can, for example, protect a power plant from ground and air attack by positioning land and ground-based air defense troops around it. In neither case is the military defense taking an active role in the operation of the infrastructures they are supporting. A military cyber defense unit positioned to protect the networks and information systems of the power plant, on the other hand, would be challenged *not* to interfere with the plant's operation. "The private sector knows its own systems better," Peter Singer has argued, "so it is going to be the one best equipped to defend itself, set aside all of the other kind of appropriate questions." Singer put the situation in well-recognized military terms: "I think the private sector should be the supported command, not the supporting command" (U.S. House of Representatives, 2017).

A number of nations are now building new mechanisms to enable the military to play an effective supporting role in the defense of critical national infrastructures against cyberattack. Estonia has established a volunteer Cyber Defence Unit of the Estonian Defence League (CDU), which can be deployed to assist civilian authorities with cyber security challenges in both crises and routine operations. Monica Ruiz proposes a similar approach for the U.S.: "state-level volunteer units … [for] the protection of critical U.S. infrastructure." These units would focus on "[i]mproving general readiness through trainings, exercises, and strengthening cooperation and synergy between public and private sectors through information sharing" and on providing support—particularly technical and analytical—in the event of major cyber incidents (Ruiz, 2018). Germany has launched a program of regular information exchange and job visits of members of its new Bundeswehr cyber service and Deutsche Telekom employees (Knirsch, 2018). Nina Kollars has suggested the need for the military to reach beyond established civil and commercial cyber defense organizations and establish better links with the "white hat" or ethical hacker community: "the work of the white hat defender community is largely unrecognized in the discourse surrounding national security and cyber strategy" (Kollars, 2018).

It is not surprising that nations are struggling with the military role in critical infrastructure defense. This is still very much work in progress. In the *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, the U.S. Senate approved establishment of a "Cyberspace Solarium Commission" charged to "develop a consensus on a strategic approach to protecting the crucial advantages of the United States in cyberspace against the attempts of adversaries to erode such advantages." One particular task of the commission was to weigh "the options for defending the United States, to consider possible structures and authorities that need to be established, revised, or augmented within the Federal Government" (U.S. Senate, 2018). Michele

Flournoy and Michael Sulmeyer have already proposed a possible structure: “a new cyberdefense agency whose purpose would be not to share information or build criminal cases but to help agencies, companies, and communities prevent attacks” (Flournoy & Sulmeyer, 2018). The discussions demonstrate Jan Kallberg and Thomas S. Cook’s argument that “cyber as an area of conflict will require unorthodox approaches, innovation, and an ability to look beyond how we are used to organize defenses” (Kallberg & Cook, 2017).

6. CONCLUSION

Joint Publication 3-07, Joint Doctrine for Military Operations Other Than War was, in its time, an attempt to define the military’s role in a variety of unconventional situations. It was useful in moving the military mindset—in the U.S., at least—away from the view that fighting wars on a large scale was not only the military’s ultimate purpose but also its only proper role. The development of military cyberspace capabilities, however, has progressively revealed the need to move beyond thinking of military roles in the simplistic terms of “war” and “other than war” and to focus instead on the appropriate role for the military’s defensive and offensive cyberspace capabilities across a variety of situations, ranging from supporting civil authorities in disaster relief to responding to threats against critical infrastructure or the security of elections.

On the one hand, while the appropriate scenarios for nations to employ offensive cyberspace capabilities continue to be debated, the development of these capabilities cannot be deferred until there is an immediate need. Instead, like any conventional military capability, they need to be organized, equipped, trained, and sustained at a high level of readiness—and supported as necessary through intelligence preparation of potential cyberspace battlefields. On the other hand, it will be difficult to organize, train, and equip military cyber defenders to lead or support the defense of civil and commercial networks and information systems until the nation can decide on the appropriate structures by which to bring together military, intelligence, diplomatic, law enforcement, governmental, and commercial resources. In the meantime, however, *JP 3-07* still offers some value in reminding us that the primary role for the military in peacetime is to help “keep the day-to-day tensions between nations below the threshold of armed conflict or war” (Joint Chiefs of Staff, 1995).

REFERENCES

Anderson, S. J. (2016). *Airpower Lessons for an Air Force Cyber-Power Targeting Theory (Drew Paper No. 23)*. Maxwell Air Force Base, AL: Air University Press.

Berinato, S. (2018, May 21). *Active Defense and 'Hacking Back': A Primer.* Retrieved from *Harvard Business Review*: https://hbr.org/2018/05/active-defense-and-hacking-back-a-primer

Bigelow, B. (2002). Forces, Targets, and Effects: Militarising Information Warfare. *Journal of Information Warfare*, 2(1), 15-22.

Boeke, S., & Broeders, D. (2018). The Demilitarisation of Cyber Conflict. *Survival: Global Politics and Strategy*, 60(6), 73-90.

Brodie, B. (1946). "The Development of Nuclear Strategy". In B. Brodie, *The Absolute Weapon* (p. 76). New York: Harcourt Brace.

Chesney, R. (2018, September 25). *The 2018 DOD Cyber Strategy: Understanding 'Defense Forward' in Light of the NDAA and PPD-20 Changes*. Retrieved from Lawfare Blog: https://www.lawfareblog.com/2018-dod-cyber-strategy-understanding-defense-forward-light-ndaa-and-ppd-20-changes

Chossudovsky, M. (2010, January 21). *A Haiti Disaster Relief Scenario Tested by US Military One Day Before the Earthquake*. Retrieved from Global Research: https://www.globalresearch.ca/a-haiti-disaster-relief-scenario-was-envisaged-by-the-us-military-one-day-before-the-earthquake/17122

Dunn Cavelty, M. (2012). The Militarisation of Cyberspace: Why Less May Be Better. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.), *2012 4th International Conference on Cyber Conflict* (pp. 141-153). Tallinn: NATO C.

Fallon, M. (2017, June 27). *Defence Secretary's speech at Cyber 2017 Chatham House Conference*. Retrieved from Gov.uk: https://www.gov.uk/government/speeches/defence-secretarys-speech-at-cyber-2017-chatham-house-conference

Fischerkeller, M. (2017). Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies. *Survival: Global Politics and Strategy*, 59(1), 103-134.

Flournoy, M., & Sulmeyer, M. (2018, September/October 2018). Battlefield Internet: A Plan for Securing Cyberspace. *Foreign Affairs*, *97*(5), pp. 40-46.

House of Commons Defence Committee. (2012). *Defence and Cyber-Security: Sixth Report of Session 2012-13, Volume I*. London: The Stationery Office Limited.

Joint Chiefs of Staff. (1995). *Joint Publication 3-07, Joint Doctrine for Military Operations Other Than War*. U.S. Department of Defense.

Joint Chiefs of Staff. (2013). *Joint Publication 3-28, Defense Support of Civil Authorities*. U.S. Department of Defense.

Joint Chiefs of Staff. (2018). *Joint Publication 3-12, Cyberspace Operations*. U.S. Department of Defense.

Joint Chiefs of Staff. (2018). *Joint Publication 3-27, Homeland Defense*. U.S. Department of Defense.

Kallberg, J., & Cook, T. S. (2017). The Unfitness of Traditional Military Thinking in Cyber. *IEEE Access, 5*, 8126-8130.

Kehler, C. R., Lin, H., & Sulmeyer, M. (2017). Rules of Engagement for Cyberspace Operations: a View from the USA. *Journal of Cyber Security, 3*(1), 69-80.

Knirsch, R. (2018, September 25). *Deutsche Telekom and Bundeswehr (German Armed Forces) cooperate in cyber defense*. Retrieved from Deutsche Telekom: https://www.telekom.com/en/media/media-information/archive/dt-and-bundeswehr-cooperate-in-cyber-defense-542510

Kollars, N. (2018, September 6). *Beyond the Cyber Leviathan: White Hats and U.S. Cyber Defense*. Retrieved from War on the Rocks: https://warontherocks.com/2018/09/beyond-the-cyber-leviathan-white-hats-and-u-s-cyber-defense/

Lee, R. M. (2015, February 25). *The active cyber defense cycle*. Retrieved from Control Engineering: https://www.controleng.com/articles/the-active-cyber-defense-cycle-a-strategy-to-ensure-oil-and-gas-infrastructure-cyber-security/

Lewis, J. A. (2018). *Rethinking Cybersecurity*. Center for Strategic and International Studies.

Maurer, T. (2012, December 5). *Is it Legal for the Military to Patrol American Networks?* Retrieved from Foreign Policy: https://foreignpolicy.com/2012/12/05/is-it-legal-for-the-military-to-patrol-american-networks/

Mehta, A. (2018, June 26). *'We need to be impatient': Estonia's No. 2 defense official dives into NATO priorities*. Retrieved from Defense News: https://www.defensenews.com/smr/nato-priorities/2018/06/26/we-need-to-be-impatient-estonias-no-2-defense-official-dives-into-nato-priorities/

National Cyber Security Centrum. (2018, August 7). *Cyber Security Assessment Netherlands 2018*. Retrieved from National Cyber Security Centrum: https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2018.html

NATO. (2016, July 9). *Warsaw Summit Communiqué*. Retrieved from NATO HQ: http://www.nato.int/cps/en/natohq/official_texts_133169.htm

Netherlands Ministry of Defence. (2018). *Defence Cyber Strategy 2018: Investing in cyber striking power for the Netherlands*. The Hague: Ministry of Defence.

Pernik, P. (2018, December 1). *Preparing for Cyber Conflict*. Retrieved from International Centre for Defence and Security: https://icds.ee/preparing-for-cyber-conflict-case-studies-of-cyber-command/

Pomerleau, M. (2017, October 19). *DoD says it shouldn't protect homeland from cyberthreats; McCain disagrees*. Retrieved from The Fifth Domain: https://www.fifthdomain.com/congress/capitol-hill/2017/10/19/dod-says-it-shouldnt-protect-homeland-from-cyberthreats-mccain-disagrees/

Rattray, G., & Healey, J. (2010). Categorizing and Understanding Offensive Cyber Capabilities and Their Use. *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (pp. 77-98). Washington, DC: The National Academy Press.

Ruiz, M. M. (2018, January 9). *Is Estonia's Approach to Cyber Defense Feasible in the United States?* Retrieved from War on the Rocks: https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/

Schmitt, M. N. (2017, August 8). *Grey Zones in the International Law of Cyberspace (2017 James Crawford Lecture on International Law)*. Retrieved from University of Adelaide: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjJsdjZornYAhUKbFAKHV7yD8QQFggpMAA&url=https%3A%2F%2Fore.exeter.ac.uk%2Frepository%2Fbitstream%2Fhandle%2F10871%2F27563%2FGrey%2520Zones%2520YJIL%2520-%2520Clean%2520

Somaskanda, S. (2018, June 4). *Cyberattacks Are 'Ticking Time Bombs' for Germany*. Retrieved from The Atlantic: https://www.theatlantic.com/international/archive/2018/06/germany-cyberattacks/561914/

Sulmeyer, M. (2018, February 13). *Department of Defense's Role in Protecting Democratic Elections: Testimony of Michael Sulmeyer before the Senate Armed Services Committee, Subcommittee on Cybersecurity*. Retrieved from U.S. Senate: https://s3.amazonaws.com/files.cnas.org/documents/SASC-Testimony-Feb-8.pdf

Sulmeyer, M. (2018, March 22). *How the U.S. Can Play Cyber-Offense*. Retrieved from Foreign Affairs: https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense

U.S. Cyber Command. (2018, July 11). *2018 Cyberspace Strategy Symposium Proceedings*. Retrieved from U.S. Cyber Command: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Cyberspace%20Strategy%20Symposium%20Proceedings%202018.pdf

U.S. Department of Defense. (2018, September 18). *Summary of the 2018 Department of Defense Cyber Strategy*. Retrieved from U.S. Department of Defense: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

U.S. Government Accountability Office. (2016). *GAO-16-332: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities During Cyber Incidents*. Washington, DC: U. S. Government Accountability Office.

U.S. Government Accountability Office. (2017, November 30). *GAO-18-47: DOD Needs to Address Cyber Incident Training Requirements*. Retrieved from U.S. Government Accountability Office: https://www.gao.gov/products/GAO-18-47

U.S. Senate. (2018, 1 August). H.R.5515 - *John S. McCain National Defense Authorization Act for Fiscal Year 2019*. Retrieved from U.S. Congress: https://www.congress.gov/bill/115th-congress/house-bill/5515/text

U.S. House of Representatives. (2017). *H.A.S.C. No. 115-8, Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities*. Committee on Armed Services. Washington: U.S. Government Publishing Office.

Wallace, I. (2013, October 3). *Cyber security: Why military forces should take a back seat*. Retrieved from Lowy Institute: https://www.lowyinstitute.org/the-interpreter/cyber-security-why-military-forces-should-take-back-seat

Wilner, A. (2017). Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation. *Comparative Strategy, 36*(4), 309-318.

Withers, P. (2015, Spring). What is the Utility of the Fifth Domain? *Air Power Review*, 18(1), 126-150.