2017 9th International Conference on Cyber Conflict
Defending the Core
H. Rõigas, R. Jakschis, L. Lindström, T. Minárik (Eds.)

Mission Assurance: Shifting the Focus of Cyber Defence*

Brad Bigelow
Principal Technical Advisor
SHAPE DCOS CIS and Cyber Defence
Mons, Belgium
brad.bigelow@shape.nato.int

Abstract: With the decision by the North Atlantic Council to recognize cyberspace as an operational domain, the NATO Command Structure is now taking on the task of implementing the doctrine, organization and capabilities to incorporate operations in cyberspace into the overall framework of joint operations. This paper outlines some of the challenges implicit in the Council's decision, which was both long-expected due to growing awareness of cyber security challenges within the Alliance and bold in its willingness to recognize what is still an immature and evolving discipline. It addresses two key challenges facing those involved in implementing cyberspace as a domain: understanding the complex composition of cyberspace and accurately identifying the consequences of the asymmetric nature of cyberspace threats. The paper then addresses two key aspects for cyberspace as a domain: mission assurance and collective defense. In the context of implementing cyberspace as an operational domain in traditional military operations and missions, cyberspace operators need to focus on mission assurance, which recognizes the reality of a contested cyberspace, and not simply on cyber security concerns. Although the military role in collective cyber defense is still a somewhat politically-charged issue, the author argues that the best way to enable effective mission assurance in cyberspace is to recognize the need for a clear role for the NATO Command Structure to act as an enabler for the open exchange of cyber defense information with military, civil and commercial organizations.

Keywords: *cyberspace, cyber defence, mission assurance, NATO*

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

1. INTRODUCTION

The implications of cyberspace as a new domain for national and collective security have increasingly consumed the time and attention of political and military leaders. The rise of the Internet (and now the Internet of Things), of ubiquitous connectivity, of electronic commerce, of networks with scales several orders of magnitude larger than anything seen even a decade ago, have made cyberspace an essential element in all aspects of public life. At the same time, media coverage highlighting the growing frequency, sophistication and impact of cyber attacks has led to a number of policy and organizational decisions. For the North Atlantic Treaty Organisation (NATO), the most recent and significant of these was the decision, taken at the Warsaw Summit in July 2016, to recognize cyberspace as a domain of operations:

> in which NATO must defend itself as effectively as it does in the air, on land, and at sea. This will improve NATO's ability to protect and conduct operations across these domains and maintain our freedom of action and decision, in all circumstances. It will support NATO's broader deterrence and defence: cyber defence will continue to be integrated into operational planning and Alliance operations and missions, and we will work together to contribute to their success (NATO 2016).

Since 2002, cyber defense topics have been included in the deliberations of the North Atlantic Council and Defense Ministers. Attacks on public and private networks in Estonia in 2007 spurred NATO to issue its first policy on cyber defense in 2008. This was updated in 2011 and again in the enhanced policy issued at the Wales Summit in 2014. At the Warsaw Summit in July 2016, Allies pledged to be capable of defending themselves in cyberspace as in the air, on land and at sea. The decision to recognize cyberspace as an operational domain represents, therefore, just a further step in the evolution of NATO's understanding of the importance of cyberspace as an aspect of collective defense.

It was a bold decision, in that it was a strong commitment to incorporate into the Alliance's framework for military operations a domain that is relatively immature in terms of doctrine and capabilities, hampered with vaguely defined terms and concepts, and widely misunderstood. This paper outlines key challenges to implementing the Council's decision to recognize cyberspace as an operational domain, including the lack of common understanding of cyberspace itself and of the nature of the threats in cyberspace. It then outlines the two most important facets of NATO military efforts in cyberspace: mission assurance at the operational and tactical levels, and collective defense at the strategic level. Finally, it argues that the two are inextricably linked and must be approached in an integrated manner to ensure that the Alliance keeps pace with its cyber threats.

2. UNDERSTANDING CYBERSPACE

Of all the challenges, first and foremost is the lack of understanding of what is meant by cyberspace and what constitutes "cyberspace" as an operational domain. The Warsaw Summit

declaration itself did not include a definition of the term, nor has it been included in the official NATO Glossary of Terms and Definitions (AAP-6). NATO is not alone in struggling with this. General Michael Hayden (2011, p. 3), who was at the center of the initial development of US cyberspace operational capabilities as Director of the National Security Agency and Director of Central Intelligence, commented: "Rarely has something been so important and so talked about with less clarity and less apparent understanding". Daniel Kuehl (2009, p. 3) listed thirteen different definitions of the term, and Peter W. Singer and Allan Friedman (2014, p. 13) were able to identify twelve different definitions that had been used within the US Department of Defense. For NATO's purposes, however, a good working definition can be established by appropriating a term already used in basic Alliance operational doctrine: "information environment". Allied Joint Publication 3, Allied Doctrine for the Conduct of Operations, defines the information environment as: "[t]he entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information" (NATO 2011, pp. 4-5).

This definition overcomes the limitations of equating cyberspace with the "global grid" of the Internet and public telecommunications networks. While the Internet is certainly the largest "land mass" of cyberspace, there are many other cyberspaces – closed or largely isolated networks – of which national security, intelligence, law enforcement and classified military networks are the most obvious examples. Deployed military operations rely heavily on operational and tactical communications and networks over radio and satellite links and often secured through a variety of encryption systems. Despite the increasing use of Internet Protocol-based systems and the gradual phasing out of analogue and older digital systems among military forces, the types of attacks and sources of threats seen in the global grid are not necessarily – and certainly not automatically – directly or immediately applicable in the context of all military instantiations of cyberspace.

Neither is cyberspace purely a virtual environment. It has what have been referred to as "littorals" – points at which it overlaps with other environments, much as land and sea converge in the littorals in which amphibious operations take place. These include:

> physical infrastructure, cabling and electrical power; the electromagnetic spectrum that data traverses; electro-mechanical processes under computer control; and the senses and cognition of computer users (Withers 2015, p. 133).

These cyberspace littorals play a significant role in considering the military aspects of cyberspace – again, particularly in the context of deployed operations, where radio and satellite communications provide the primary transmission systems. The new functions of cyberspace operations in a deployed context must be coordinated or integrated with the existing functions of spectrum management, electronic warfare and what some forces call "electromagnetic operations".

A key concern in implementing cyberspace as an operational domain, therefore, is to establish an accurate understanding of the actual "territory" that comprises the cyberspace upon which

a military operation depends. In NATO operations, the area in which a designated Joint Force Commander plans and executes a specific mission at the operational level is referred to as the Joint Operations Area (JOA). The boundaries within which a JOA is defined are contingency or mission-specific, and intended to focus and enhance military activities within that area (NATO 2011, pp. 1-23).

For cyberspace operations to be integrated as part of a NATO operation, therefore, it would be necessary to identify the cyberspace JOA – the specific elements of what one might call the total geography of cyberspace relevant to the operation. This would certainly include the communications and information systems used to carry out the command and control of operational forces. In addition, it would include all supporting systems, including intelligence, logistics, medical, civil-military cooperation, information and psychological operations, and force protection, as well as all long-haul reach-back communications and any systems and networks in the static infrastructure at home that support the deployed operation. It might include commercial systems, given that military forces increasingly augment limited military satellite communications with commercial satellite services. And it would almost certainly include the Internet and any interfaces to it, since the Internet has become the primary medium through which news reports, morale and welfare communications, social media discussions, strategic communications, information exchanges with non-governmental organizations and supporting financial, procurement and transportation arrangements will be conveyed.

A good illustration of the complexity and geographically dispersed nature of cyberspace is offered by the example of one capability likely to be employed in future NATO operations: the NATO Alliance Ground Surveillance (AGS) system. For this one system alone, a complex set of communications and information system assets, including deployed ground stations, military and satellite communications, air-ground tactical data links, air command and control systems, a Main Operating Base in Europe, and dissemination links to national and multi-national intelligence analysis centers, is required to provide just part of the overall intelligence, surveillance and reconnaissance (ISR) support to the military operation. And some elements, such as the Main Operating Base, are one-deep resources that cannot be dedicated to a single operation and must always be viewed as strategic assets.

When one then considers the number of similarly complex and distributed systems supporting the NATO and national forces involved in a military operation of even moderate scale, it should become clear that it is difficult to draw clear boundaries that distinguish the area within which a NATO operational commander would have authority to take military decisions from that which is subject to civil or political authorities. As Scott Applegate (2012, p. 192) summed it up: “One difficulty in defining borders in cyberspace is that the physical geography of cyberspace does not even remotely match the logical geography”. Indeed, one can argue that, given the heavy use of reach-back capabilities and Alliance and national strategic assets, it would be difficult to define a cyberspace JOA that is purely mission-specific and does not overlap substantially with the strategic Area of Responsibility (AOR) for which the Supreme Allied Commander Europe (SACEUR) is assigned sole responsibility (NATO 2011, pp. 1-23). Because of this, the principles of levels of command and delegation of authority that can be applied within the

physical boundaries of a JOA for the air, land and maritime domains, where clear boundaries can be established, may be difficult to implement within a cyberspace JOA. And this is not the only unique aspect of cyberspace as an operational domain.

3. UNDERSTANDING THE NATURE OF CYBERSPACE THREATS

A second challenge in implementing cyberspace as a domain of military operations is the nature of cyberspace threats – in particular, the asymmetries in the relationships between attackers and defenders. As illustrated in the description of a cyberspace JOA above, military operations conducted by NATO and its member nations are hugely dependent upon a complex set of supporting military, governmental and commercial networks and systems. No NATO operational commander can automatically assume that the parties responsible for these networks and systems will allow their use by military cyberspace forces to launch attacks or take other measures that might put them at risk. Attribution can be extremely difficult, or simply impossible. Even with certain attribution, the organizations attacked will often lack the legal authority or appropriate tools to strike back directly or in kind.

But there are other aspects of the asymmetric nature of cyberspace threats that represent complex challenges when considering the use of military forces and capabilities in defense of cyberspace. Cyber attacks are not always immediate in effect, let alone easily attributable. Analogies between cyber and air defense fail: cyber defenders will not be watching incoming attackers on a "cyber radar" and launching cyber weapons in response. Instead, cyberspace defenders are more likely to be sifting through log files and employing sophisticated analytical tools, searching not only to pick up the trail of the attacker but even just to detect what the actual impact of the attack might have been.

Although the trend has been improving in recent years, the fact remains that there is often a significant delay between the initiation of an attack and its detection. According to one recent report, the median number of days between a cyber attack and its discovery was 146, which is well beyond the timescale traditionally associated with tactical operations in other domains (FireEye/Mandiant Consulting 2016, p. 4). As Dr Jan Kallberg (2016, p. 103) wrote recently: "In reality […] cyber-attacks would be over before any leadership understood the strategic landscape". In addition, cyber attackers may not consider themselves obliged to comply with the rule of law, to limit themselves to launching attacks after a formal declaration of war or to confine their attacks to clearly designated military targets. Indeed, they may be able to achieve a desired effect simply by asserting that successful attacks have taken place, or by manipulating perceptions via social media, as has been seen in support of Russian incursions into Ukraine (NATO Strategic Communications Centre of Excellence 2016, pp. 11-12).

If the tactics of cyber attackers may take months to detect, may have effects that are difficult to assess, are problematic to attribute to specific sources or involve exploitation of systems clearly outside military or governmental control, fall outside periods of formally-declared operations,

and involve manipulation of social media, then the resources available to an operational commander in theatre are simply inadequate to develop effective responses or mitigations. As with the difficulty of establishing boundaries in cyberspace for NATO operations, these aspects of potential cyber threats suggest that the traditional distinctions between tactical, operational and strategic levels of command that apply in other domains may not be appropriate for cyberspace as a domain. Unlike the kind of threats a NATO operational commander may face in the air, land or maritime domains, in cyberspace there is a good chance that adversaries will undertake attacks against which there are no mature and well-understood responses. Unlike most responses in the other domains, cyberspace responses lack measures of effectiveness that have been established and proven through extensive use in exercises, if not actual operations, and that would allow them to be apportioned within clear rules of engagement at the tactical or operational level. This approach applies as well when considering how to achieve effective mission assurance in cyberspace.

4. UNDERSTANDING MISSION ASSURANCE IN CYBERSPACE

A primary argument made by NATO military authorities in advocating for the recognition of cyberspace as an operational domain was that it would improve mission assurance for NATO's joint military forces in accomplishing their core tasks. As with "cyberspace", NATO has not yet agreed a formal definition of "mission assurance". In its *Mission Assurance Strategy*, the US Department of Defense has defined the term as:

> [a] process to protect or ensure the continued function and resilience of capabilities and assets – including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains – critical to the performance of DoD Mission-Essential Functions (US Department of Defense 2012, p. 1).

What is particularly interesting about this definition is that it positions mission assurance as a supporting consideration to that of actually performing mission-essential functions. This understanding is crucial to ensuring the proper focus of cyberspace as a domain of military operations. According to Colonel William Bryant of the US Air Force (2016, p. 6): "Mission assurance in and through cyberspace is not fundamentally an IT problem, but a mission problem that requires a mission focus and approaches that go beyond what we have come to think of as traditional cybersecurity".

Mission assurance, in Michael Jay Lanham's (2015, p. 24) words, requires acceptance that "bad things will happen to an organization, despite the various avoidance, mitigation, retention and transfer measures in place". Mission assurance in cyberspace focuses on assuring that an organization's mission capability can be maintained not only by preventing degradations but by minimizing effects and orchestrating rapid responses when they do occur (Pritchett 2012, p. iv). Unlike cyber security, which strives to protect all information systems and assets, mission assurance seeks to ensure that the mission can be carried out even if some systems have failed.

One paper concluded that: “mission-critical assets do not have to be perfectly secure; they just have to be secure enough to reliably accomplish their mission” (Peake, Underbrink & Potter 2012, p. 30). A military operation with a strong level of cyber mission assurance is one capable of continuing its mission-essential functions even in the presence of cyber attacks, not one that simply aims to prevent these attacks. As Internet security expert Dan Geer (1998) once phrased it: “The ability to avoid loss never makes up for the ability to absorb loss”.

What cyberspace operators need to focus on, instead of protection and prevention measures, are effects. These should include both the negative effects that disruptions, compromises, outages, exploitations or other degradations in the cyberspace supporting the operation might have, and the positive effects that defensive or mitigation measures might have to ensure effective command and control. And, where appropriate, authorized and made available by contributing nations, the enabling effects that offensive cyberspace capabilities might contribute. However, given the scale and complexity of the cyberspace elements supporting a typical NATO operation, cyberspace operators need to consider the full scope of the communications and information systems involved, not just those deployed in theatre, and all possible threats against them including self-inflicted disruptions. At least until tools, techniques and tactics mature, this may be a task best approached at the strategic level.

Of course, the best time to do this analysis is before the operation begins, through exercises, simulations and training. This is why in recent years the US has made a priority of the exercise of its capabilities to operate effectively in “denied, manipulated, and/or contested cyberspace” (Chairman Joint Chiefs of Staff 2014, p. 3). This is also why it is important to separate cyberspace operations from traditional network operations. A good network operator will always strive to provide the most secure and reliable service possible and will be disinclined to arbitrarily cause outages or disruptions. But a responsible cyberspace operator should always want to test the operational force’s ability to deal with the unexpected when there is still time to learn where the key constraints in the supporting cyberspace are and mitigate the impacts of their disruption or loss. Placing the responsibility for cyberspace operations outside the network operations function improves the ability of cyberspace operators to focus on mission assurance. Without explicit planning and exercising for cyberspace incidents – whether hostile or self-inflicted – the effectiveness of detection and response measures, particularly those that involve multiple organizations or force elements, is significantly undermined (Lanham 2015, p. 50).

NATO has already begun to put a greater emphasis on integrating cyber defense into its military exercise and training program, but as it now implements cyberspace as an operational domain, that emphasis will need to shift from focusing on information assurance to focusing on mission assurance. Exercises should incorporate more scenarios aimed at testing the ability of coalition forces to operate effectively under constrained cyberspace conditions and in the presence of a variety of cyber attacks, including attacks that target strategic elements of Alliance cyberspace, supporting critical infrastructures and even social media. NATO cyberspace doctrine development should also explore techniques and tactics to enable forces to recover more quickly in the event of attacks or other disruptions.

And in implementing cyberspace as a domain, NATO should recognize that, unlike other domains, cyberspace enjoys the blessing (as well as the curse) of being an environment in which attacks and responses to their effects are part and parcel of everyday business for the NATO Command Structure and other elements of the NATO enterprise, for national military and government organizations and for commercial and non-governmental organizations. Every nation in the Alliance has some equivalent to the NATO Computer Incident Response Centre (NCIRC), dealing with cyber incidents on a daily basis. Every one of these incidents is an opportunity to get smarter about the techniques and capabilities of cyber attackers, to better understand how to eliminate or compensate for the vulnerabilities exploited, to improve response mechanisms, and to make the affected organization better able to cope with future attacks. As a recent survey of the arrangements for management of major cyber incidents in a number of European and Asian countries found, expecting "issues of command and responsibility to be resolved during the evolution of the crisis […] will likely have a negative impact on the effectiveness of the response" (Boeke, Heinl & Veenendaal 2015, p. 73). Given the lack of clear boundaries in cyberspace and the high probability that cyber attacks may occur outside the context of approved NATO operations, mission assurance in the cyberspace domain is not just something to worry about when drawing up an operational plan, it is a continuous concern for every organization operating in cyberspace. That is why mission assurance in cyberspace cannot be divorced from the issue of collective defense in cyberspace.

5. THE MILITARY ROLE IN COLLECTIVE DEFENSE OF CYBERSPACE

In recognizing cyberspace as an operational domain, the North Atlantic Council inevitably opens a dialogue over the appropriate role for NATO military commands and forces in the collective defense of cyberspace. This is still a highly-charged issue for some. They recognize that the portion of cyberspace supporting military operations represents only a fraction of the total cyberspace geography upon which their government, commercial organizations and private citizens depend. Some share Martin Libicki's (2012, p. 321) view that "cyberspace is not a warfighting domain".

In committing to the Cyber Pledge at the Warsaw Summit, the Council agreed to enhance the cyber defenses of national infrastructures and networks and recognized the indivisibility of Allied security and collective defense (NATO, Cyber Defense Pledge 2016). Although the Council recognized that "[o]ur interconnectedness means that we are only as strong as our weakest link", it also qualified that co-operative efforts such as "multinational projects, education, training, and exercises and information exchange" were only "in support of national cyber defense efforts". However, the Council did not make a direct connection between the operational domain of cyberspace and any standing role it might play in collective defense outside the context of military operations.

Indeed, perhaps the primary obstacle to acknowledging a role for the NATO Command Structure in the collective defense of cyberspace is the tendency to view this role in terms of analogies

with collective defense functions in other domains. NATO maintains, for example, under its Air Component Command, a peacetime collective defense Air Policing mission that safeguard the integrity of the Alliance members' national airspace. NATO's Maritime Command has a standing task to maintain maritime situational awareness across national and international waters. When it comes to the defense of cyberspace, however, some nations are reluctant to entertain the possibility of the military, let alone an international organization such as NATO, controlling a cyber defense force with access to national networks or even with access to information about national cyberspace vulnerabilities. According to Cavelty (2012, p. 151): "Protecting them [critical information infrastructures] as a military mandate is an impossibility and considering cyberspace as an occupation zone is an illusion".

Yet even without such a commitment, the NATO Command Structure plays a significant role in the defense of what are known as the NATO enterprise networks. Allied Command Operations (ACO) funds over 80% of the annual operating costs of these networks and 100% of the cost of operating the NCIRC and other cyber defense capabilities such as the Malware Information Sharing Platform (MISP). In addition, ACO maintains a full-time strategic cyber defense situational awareness capability under a multi-disciplinary team known as Task Force Cyber, part of SACEUR's standing task to provide the Council with military advice on indications and warnings of threats to collective security. Allied Command Transformation (ACT) supports joint cyberspace doctrine development and sponsors Cyber Coalition and other events intended to improve cyber incident response capabilities. And as a high-visibility organization operating on an international scale, NATO represents an attractive target for cyber-attackers interested in making headlines.

There is a natural role, therefore, for the NATO Command Structure to support collective cyber defense through information-sharing and situational awareness. This is not the cyberspace equivalent of air policing. This is not a matter of any NATO organization gaining access to national systems or networks or commanding the application of defensive measures within those networks. Protection of national networks is and remains strictly a matter of national responsibility. Establishing a clear role for the NATO Command Structure in collective cyber defense is a matter of recognizing that the complex and distributed nature of cyberspace – which cuts across all levels of systems and command, from tactical to strategic – and the unique characteristics of cyber threats – which tend to involve timescales, employ techniques, and include targets that go well beyond the domain of traditional military operations – requires an operational approach involving continuous collaboration, rather than simply a capacity to gear up a cyberspace mission assurance capability in the event of a crisis.

Every day, some part of the Alliance experiences attacks or disruptions that provide live scenarios far better than could be constructed in any exercise or simulation. Without a clear task to participate in, which will foster the kind of information-sharing that can both improve collective defense and better prepare the command to address mission assurance in cyberspace, the NATO Command Structure can only maintain a limited cyberspace situational awareness function, organize a small number of exercises each year, and develop its cyberspace operational doctrine in relative isolation.

Sensitivities over the role of an international military organization in cyber defense, however, have left the responsibilities for these functions vaguely and inconsistently defined. The Charter of the NATO Communications and Information Organisation (NCIO) assigns the responsibility for protection of NATO's communications and information infrastructures to the NATO Communications and Information Agency (NCIA) (NATO 2012, pp. 1-12). Although the expectation that cyberspace will be addressed in the context of NATO operations is clear from the decision to recognize it as a domain, the NATO Command Structure has not been assigned specific tasks or authorities to establish formal cyber defense information-sharing mechanisms with equivalent elements in the NATO Force Structure.

The value of information-sharing, under SACEUR's leadership, to improve the state of collective cyber defense cannot be overestimated. A recent study by the RAND Corporation found that "[i]nformation exchange is an indispensable element in the improvement of cybersecurity" (Meulen 2015, p. viii). The NATO Command Structure already plays key roles in maintaining effective information exchange with Alliance national military forces regarding capabilities, readiness, certification, doctrine, training and a wide array of other common interests in the other operational domains. With the recognition of cyberspace as an operational domain, it only makes sense to add cyber defense to this list. NATO and national military cyber defense organizations should maintain a strong partnership, not just on cyber incidents and malware, but also on advancing doctrine, techniques, tactics and procedures and improving collective situational awareness capabilities.

Collective defense can only be improved by encouraging collective cyber defense throughout the Alliance through a healthy, open and lively exchange of information between military cyber defense organizations and, of course, with their civil and commercial counterparts. This should not be considered just a "nice to have", but an essential element of the collective cyber defense strategy. One can hardly imagine how Alliance leaders expect collective cyber defense to be improved by remaining mute on the question of the military's role. As Thomas Rid (2012, p. 29) stated: "The world's most sophisticated cyber forces have an interest in openness if they want to retain their edge, especially on the defensive. […] Only openness and oversight can expose and reduce weaknesses in organization, priorities, technology, and vision".

6. CONCLUSION

Recognition of cyberspace as an operational domain certainly presents considerable challenges for NATO. The Alliance must achieve a more accurate understanding of the scale and complexity of cyberspace, particularly as it applies to the support of NATO operations, and its inherent reliance on strategic information assets and even critical infrastructures. It must acknowledge the nature of cyber threats, which often involve timescales, targets or effects that can only be addressed effectively at the strategic level. In their assessment of the implications of recognizing cyberspace as an operational domain, NATO military authorities identified improving mission assurance for joint operations as a key benefit, and this perspective will help to shift the focus of cyberspace operators from information assurance and cyber security. But the best way to

improve NATO mission assurance in cyberspace is to recognize the opportunities presented by the cyber incidents dealt with on a daily basis by cyber incident response centers and the networked organizations they support. And this means to recognize the legitimate role for the NATO Command Structure to act as an enabler for collective defense in cyberspace through partnership and information-sharing.

REFERENCES

Applegate, S. D. (2012). The Principle of Maneuver in Cyber Operations. *2012 4th International Conference on Cyber Conflict* (pp. 183-195). Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.

Boeke, S., Heinl, C. H. & Veenendaal, M. (2015). Civil-Military Relations and International Military Cooperation in Cyber Security: Common Challenges & State Practices Across Asia and Europe. *7th International Conference on Cyber Conflict* (pp. 69-80). Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.

Bryant, W. D. (2016, Winter). Mission Assurance through Integrated Cyber Defense. *Air & Space Power Journal*, 5-17.

Cavelty, M. D. (2012). The Militarisation of Cyberspace: Why Less May Be Better. *2012 4th International Conference on Cyber Conflict* (pp. 141-153). Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.

Chairman Joint Chiefs of Staff. (2014). CJCS Notice 3500.01, 2015-2018 *Chairmans Joint Training Guidance*. Retrieved from US Department of Defense, Chairman Joint Chiefs of Staff: www.dtic.mil/cjcs_directives/cdata/unlimit/n350001.pdf.

FireEye/Mandiant Consulting. (2016). *M-Trends 2016*. Retrieved from FireEye Corporation: https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016-NEW.pdf.

Geer, D. (1998). Risk Management is Where the Money Is. *Risks-Forum Digest*, 20(6). Retrieved from http://cseweb.ucsd.edu/~goguen/courses/275f00/geer.html.

Hayden, M. V. (2011, Spring). The Future of Things Cyber. *Strategic Studies Quarterly*, 5(1), 3-7.

Kallberg, J. (2016). Strategic Cyberwar Theory–A Foundation for Designing Decisive Strategic Cyber Operations. *The Cyber Defense Review*, 1(1), 113-125.

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In F. D. Kramer, S. Starr, & L. K. Wentz, *Cyberpower and National Security*. Washington, DC: National Defense University Press.

Lanham, M. J. (2015). *Rapid Mission Assurance Assessment via Sociotechnical Modeling and Simulation* (Published Dissertation). Pittsburgh, PA: Institute of Software Research, Carnegie Mellon University.

Libicki, M. C. (2012). Cyberspace Is Not a Warfighting Domain. *I/S: A Journal of Law and Policy for the Information Society*, 8(2), 321-336.

Meulen, N. v. (2015, October 14). *Investing in Cybersecurity*. Retrieved from Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC): https://english.wodc.nl/onderzoeksdatabase/2551-investeren-in-cyber-security.aspx.

NATO. (2011). Allied Joint Publication 3. *Allied Joint Doctrine for the Conduct of Operations*.

NATO. (2012). *C-M (2012)0049, Charter of the NATO Communications and Information Organisation*. Retrieved from NATO Communications and Information Agency.

NATO. (2016, July 9). *Cyber Defence Pledge*. Retrieved from NATO: http://www.nato.int/cps/en/natohq/official_texts_133177.htm.

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

NATO Strategic Communications Centre of Excellence. (2016). *Social Media as a Tool of Hybrid Warfare*. Riga, Latvia: NATO Strategic Communications Centre of Excellence.

Peake, C., Underbrink, A. & Potter, A. (September-October 2012). Cyber Mission Resilience: Mission Assurance in the Cyber Ecosystem. CrossTalk, pp. 29-33.

Pritchett, M. D. (2012). *Cyber Mission Assurance: A Guide to Reducing the Uncertainties of Operating in a Contested Cyber Environment*. Retrieved from Air Force Institute of Technology: http://www.dtic.mil/dtic/tr/fulltext/u2/a563712.pdf.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), 5-32.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York City, NY: Oxford University Press.

US Department of Defense. (2012). *Mission Assurance Strategy*. Washington, DC.: Deputy Secretary of Defense.

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