2018 10th International Conference on Cyber Conflict
CyCon X: Maximising Effects
T. Minárik, R. Jakschis, L. Lindström (Eds.)
2018 © NATO CCD COE Publications, Tallinn

The Topography of Cyberspace and Its Consequences for Operations*

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

Abstract: For all the focus on cyberspace as a source of security threats and a domain of military operations, there has been little progress on establishing a consistent approach to describing what constitutes cyberspace. Dozens of definitions of the term "cyberspace" have been developed, but consensus on its essential attributes has yet to be achieved. Similarly, a number of different models have been offered to describe cyberspace in terms of layers, such as the physical, logical and cyber persona layers used in US Joint Publication 3-12, *Cyberspace Operations*. This paper argues that cyberspace as a label for a domain should not be confused with the individual networks – some interconnected ("open") and some relatively isolated ("closed") – involved in military operations. As illustrated by the STEADFAST COBALT exercise, military operations often involve a complex set of networks. The paper then uses the example of the Internet to illustrate the need to take a topographical approach – one that identifies the features of the objects or entities and their structural relationships – to enable effective military operations. This more detailed topographical view of the Internet is used to illustrate how cyberspace considerations relate to existing operational doctrine such as concepts from the operational environment (Joint Operational Area and Area of Interest). Some considerations fit well within this framework. Others require some adaptation, such as shifting some responsibilities to a centralized and persistent function such as the Cyberspace Operations Centre (CyOC) being established by NATO. Others fall outside military control and are better addressed through civil-military cooperation. This example also illustrates how precision in describing the

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

composition of cyberspace is essential if military operations in and through cyberspace are to develop into a mature discipline with a solid base of concepts, terminology, techniques, tactics and procedures.

Keywords: *cyberspace, cyberspace operations, cyberspace topography*

1. INTRODUCTION

For all the words that have been written about cyberspace, the lack of a consistent definition and approach to describing it remains one of the biggest obstacles to achieving an effective foundation upon which to advance the state of theory and practice. When the NATO heads of state and government recognized cyberspace as a domain of military operations at the Warsaw Summit in 2016, they managed to do so without actually defining what cyberspace constitutes. While constructive ambiguity might be a useful tool in political negotiations, it becomes an impediment when trying to develop techniques, tactics and procedures for military operations.

The lack of precision in defining what cyberspace comprises undermines the development of effective military responses to its threats and risks because it leads to generalizations that are inaccurate at best and misleading at worst. In a 2015 paper titled "On Cyberwarfare", for example, Fred Schreier postulates five characteristics that make cyberspace unique, including that "the cost of entry into cyberspace is relatively cheap." Because of this, he argues: "The resources and expertise required to enter, exist in, and exploit cyberspace are modest compared to those required for exploiting the land, sea, air, and space domains" (Scheier, 2015). This point about the low cost of entry is often repeated in discussions of cyberspace and its security. For example, the US Army's most recent edition of one of its most basic doctrine publications, Field Manual 3-1, *Operations*, states that:

> Cyberspace is highly vulnerable for several reasons, including ease of access, network and software complexity, lack of security considerations in network design and software development, and inappropriate user activity (US Army, 2017).

The official *NATO Glossary of Terms and Definitions* (AAP-6) does not yet offer a definition of the term "cyberspace". The US Department of Defense issued at least twelve different definitions over the years before issuing its joint doctrine on cyberspace operations in 2013 (Singer, 2014). In its list of cyber definitions, the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) has collected

29 examples for "cyberspace"– some identical, some similar, some very different (CCD COE, 2017). It is not surprising, then, that as significant a figure as General Michael Hayden, who as Director of the National Security Agency and Director of Central Intelligence was at the center of the initial development of US cyberspace operational capabilities, has written that: "Rarely has something been so important and so talked about with less clarity and less apparent understanding…." (Hayden, 2011).

2. CYBERSPACE, NETWORKS AND CYBERSPACE LITTORALS

One of the basic misunderstandings of cyberspace is the assumption that it is synonymous with the "global grid" of the Internet and public telecommunications networks. By at least three orders of magnitude, the Internet is certainly the largest instance of cyberspace. The Internet Protocol version 6 address space has the capacity to encompass 2^{128} addresses, or something on the order of ten million trillion times the total number of grains of sand on all the beaches in the world. It has also reached many more users than any other network ever developed. It is estimated that, as of mid-2017, over 50% of the world's population are able to access the Internet (World Internet Users and 2017 Population Stats, 2017).

While the Internet is certainly the largest network in cyberspace, it is not the only one. There are still many networks that do not interconnect with the Internet. Closed networks such as classified intelligence, law enforcement and military networks are perhaps the most obvious examples. Others include such closed networks as that operated by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) to provide secure messaging to support international financial transactions. In discussions of the application of international law to military operations in cyberspace, such as the *Tallinn Manual 2.0*, "public, internationally and openly accessible" networks, such as the Internet, are explicitly distinguished from "closed military" networks, in part because this distinction can be important, for example, in determining the appropriate rules of engagement (Schmitt, 2016). Further, as Dror Kenett and his colleagues have written, "In most real-world systems an individual network is one component within a much larger complex multi-level network"– a network within a network of networks (Kenett, et al., 2014).

Each of these networks of networks is an instance of cyberspace. Within a single network there is, at least in principle, the possibility of end-to-end connections: the ability to transfer data, enable transactions, disseminate information, or, from the standpoint of cyberspace operations, create effects. The sum of all the networks that

exist equates to what is referred to as cyberspace in conceptual discussions, but it quickly becomes problematic to make assertions that there are characteristics – such as ease of access – that apply universally across all known networks. Ease of access may be a characteristic of the Internet, but it is certainly not a characteristic of a highly secure network and largely isolated network such as SWIFT.

This distinction between cyberspace as a label for a domain of military operations and individual networks as particular instances of cyberspace is no different from how the term domain has been applied in the context of air, land and maritime operations. While the Earth is wrapped in an atmospheric blanket we refer to as air or aerospace, much of it is divided into airspaces (plural) that are under some level of control – usually national – for such purposes as air safety and national security. Armies concern themselves with land operations, but these must always be tailored to the conditions of a particular location (desert, mountain or jungle). And even the simple distinction between surface and subsurface has profound implications for maritime operations. Indeed, the term "waterspace management" is specifically used for the coordination between submarine and anti-submarine operations.

The need to recognize that cyberspace is more than just the Internet is of critical importance when it comes to planning, organizing and carrying out military operations. In a complex, communications-intensive coalition operation such as that simulated in STEADFAST COBALT – NATO's annual command and control (C2) interoperability exercise – myriad networks, information systems and communications transmission systems are employed. These networks include NATO's unclassified Intranet and its classified network as well as the national equivalents for most of the coalition. The classified networks are then federated through a mission network as a primary interoperability and C2 environment. In addition, the operation will often employ other classified networks handling intelligence or other sensitive data.

The information systems for these operations range from what are termed "core services" – electronic mail, websites, collaboration and office automation – to functional services such as Common Operational Picture and Order of Battle managers. Numerous support applications, such as logistics, movement and spectrum management and external communications tools, such as public affairs, strategic communications and social media, will also be involved. These information systems, along with voice and video traffic, are connected through transmission systems that include both wired and wireless media. Wireless communications span radio frequency bands reaching from VLF (Very Low Frequency) through HF (High Frequency) and VHF (Very High Frequency) to UHF (Ultra High Frequency) and SHF (Super High Frequency). And no military operation today can be carried out without heavy reliance on Positioning, Navigation and Timing (PNT) services such as the Global

Positioning System (GPS), almost entirely carried over portions of a very crowded radio spectrum.

If one looks at the networks at static military facilities, this complexity only increases. The number of networks and information systems in static facilities, as well as the variety of classifications and handling controls of the information they support, typically exceeds that in deployed operations, if only because of the much wider range of functions supported. Some of these are directly connected to the Internet and some are "air-gapped" – isolated from the Internet and other networks through a combination of physical separation, personnel clearances, classification, handling restrictions and encryption. Fewer and fewer military organizations, however, are finding it possible to operate effectively with completely isolated networks, and the pressure to share information is driving them to close the "air gaps" by means of security mechanisms such as guards, gateways, diodes, or encryption, thereby introducing potential vulnerabilities.

Many of the networks, information systems and transmission systems used in deployed operations are anchored through reachback links to these static facilities, which are themselves linked through numerous wide area networks, operating at different levels of classification. Here again, some of these wide area networks are connected to the Internet, directly or indirectly, and some operate over dedicated transmission systems. Because dedicated radio and cable transmission systems tend to play a much smaller role in the interconnection of static facilities than they do in deployed operations, most wide area network connections between static facilities are reliant on commercial leased circuits or tunneled IP services.

Every network also connects to what Paul Withers has termed "cyberspace littorals" – the places where individual instances of cyberspace meet other domains (Withers, 2015). These cyberspace littorals include: the physical infrastructure, including fences, buildings, gates and transportation networks, within which any equipment providing the cyberspace resides; the radio frequency spectrum through which the cyberspace transmissions are carried; the critical infrastructures such as electrical power and water that support the equipment and its supporting personnel; the cyber-physical systems used to control critical infrastructures, force protection systems, industrial systems and even cars and trucks; and finally, the cognitive dimension of decision-making, doctrine, perceptions and even the attitudes shaped through mass and social media.

The term "littoral" should be familiar to military personnel from its use in describing the zone in which the responsibilities of land and maritime forces converge in such operations as amphibious assaults. Applying this term to cyberspace helps to identify those areas in which the responsibilities of cyberspace operators converge with

those of existing military disciplines such as physical security, force protection, area defense, electronic warfare and psychological operations (PSYOPS). It can be useful in better understanding the roles a particular network plays in a military operation and in determining how it can be defended. Indeed, protection of the electromagnetic littoral through spectrum management and electronic countermeasures, for example, can be more critical to the success of a deployed operation that is heavily dependent on radio and satellite communications than any combination of cyber security measures. In the same way, understanding an adversary's cyberspace littorals can help identify effective ways to exploit or disrupt an adversary's use of cyberspace (although this paper does not address offensive considerations).

3. THE TOPOGRAPHY OF ONE INSTANCE OF CYBERSPACE: THE INTERNET

Accurately identifying and understanding the characteristics of any particular network as an instance of cyberspace requires a closer look at its topography – the features of its objects or entities and their structural relationships (Merriam-Webster, 2018). What networks connect to it? Where and how do they connect? How big is it? What types of communications and transactions does it support? And what are the specific features of its littorals? Although the Internet is just one of the networks involved in a military operation, an overview of its topography provides useful insights into how it can be approached in the context of a military operation. It also reveals aspects that military operations are ill-prepared – and arguably ill-suited – to address.

Let us consider, then, the Internet as it might be employed in support of an operation in which a NATO command element and a coalition of forces from NATO and partner nations deploy to an operational theater under the mandate of an operational plan approved by the North Atlantic Council. As with the STEADFAST COBALT exercise, classified networks are still the primary networks employed to support NATO operations. Indeed, for these operations, the reliance on classified networks remains perhaps the single most effective protection against not only conventional military threats, but also threats from the Internet. As standard practice, however, the NATO Unclassified network, which is connected to the Internet through managed gateways hosted in static NATO command structure facilities, is extended to support the NATO command element and eligible parts of national forces. Many nations do much the same, deploying equipment forward to enable access to one or more national networks that are also connected to the Internet.

So, the Internet, the direct and indirect dependencies of his mission on it, and the resulting risks are all considerations for the operational commander. From a

topographical standpoint, every device that can connect to the Internet – directly or indirectly – shares access to a common space defined by an Internet Protocol address (whether version 4 or version 6) and the core Internet link, internet, transport and application protocols (IETF, 1989; IETF, 1989). This is the common plane or elevation (to use a topographical term) on which all Internet-connected devices converge. This is the part of the Internet for which ease of access is indeed its most salient characteristic, and it is understandably the space in which vulnerabilities and attacks that exploit them are most frequently experienced.

As has often been noted, these protocols were designed primarily for fault tolerance and not for trustworthiness or the presence of malicious actors. Consequently, it is also the space where most cyber security efforts are focused. With the growing sophistication of the threats (as one recent Cisco (2016) report puts it: "the time of amateur hackers is long over, and hacking is now an organized crime or state-sponsored event"), however, some in the field of cyber security are arguing that their goal must shift from intrusion prevention to intrusion tolerance – to what has been called the "assume breach" paradigm (Cisco, 2016; Pompon, 2016). While this approach may be new to the Internet, military personnel will recognize it as an example of operating in a contested environment.

Every point of interconnection between information systems supporting military operations and the Internet is a point of exposure to such attacks. Even if such interconnections are minimized or eliminated, these measures do not address the extent to which the Internet has become embedded into most individuals and organizations in the developed world – any of which can, directly or indirectly, represent a dependency for the operation. As Dan Geer has put it, "If […] you are dependent on those who are dependent on the Internet, then so are you" (Geer, 2013).

The risks arising from the use of the Internet in industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems to manage critical national infrastructure such as electrical power generation and distribution is of growing concern for military operations. Combat and direct support units typically bring their own critical infrastructure in the form of power generation, water treatment, field medical units and other support functions when they deploy. However, this level of autonomy is rare at the reachback command and support facilities to which they are connected, and even the autonomy of deployed units is constrained if this reachback support is disrupted for more than a short time.

If one digs into the Internet below the link layer and looks at the next layers down – what in the Open Systems Interconnection (OSI) model are referred to as the data link layer and the physical layer – ease of access can no longer be taken for granted. Access

to traffic at these layers requires access to the physical transport medium, meaning the radio frequency signal or telecommunication cable carrying the data. It requires the attacker to be within the range of the WiFi access points or to have physical access to the actual cable plant of a local area network or to the cabling carrying traffic across the wide area network through the services of telecommunications providers. The first two – access to WiFi networks and local cable plants – are well within the control of most military commanders. While WiFi vulnerabilities are well known and frequently exploited, so are relatively cheap and effective methods to defend against common threats. However, WiFi availability remains problematic, as WiFi jammers can be easily purchased or manufactured, unless the commander can assure the physical security of all space within jamming range.

Most of the physical transport media carrying Internet wide area traffic, on the other hand, lies outside a commander's control. For short-term deployed operations this is not an issue, because any extension of Internet access to the theater is likely carried over military radio or satellite communications links rather than leased lines. These links are typically protected against a wide range of threats through the use of encryption and anti-jamming mechanisms.

For static facilities, however, the risks arising from dependence on external telecommunications infrastructure are a fact of life, frequently demonstrated through the phenomenon known as "backhoe fade" – damage to underground telecommunications cabling caused by construction equipment. In its *2016 Damage Incident Reporting Tool (DIRT) Analysis and Recommendations Report*, for example, the Common Ground Alliance (2017) reported that nearly 130,000 events (breaks or damage to telecommunications cabling) occurred in the United States and Canada. The potential to exploit or disrupt submarine telecommunications cables is one that has long been known to, and used by, nation states with sufficient technical and operational means (Khazan, 2013).

The Internet also depends on the whole infrastructure of intermediaries involved in any end-to-end communication: foremost, the applications, equipment, facilities and personnel of the Internet Service Providers (ISPs) and Tier 1 (settlement-free interconnection) network providers. The days of the "ISP in the garage" are long past and the vast majority of Internet traffic is carried by a small number of Tier 1 providers. According to the Center for Applied Internet Data Analysis, the top 10 Tier 1 providers support interconnections for over 4.8 billion IPv4 addresses (CAIDA, 2016). In addition, commercial data centers, including those supporting cloud services, have already overtaken the size and capacity of private enterprise on-premise server rooms and data centers, and an increasing number of public and military organizations are shifting applications and services to external data centers and cloud providers.

Finally, this infrastructure also provides much of the intermediary transport media for long-distance telecommunications, which have largely been migrated from circuit-switched to IP transport services.

These providers operate the core physical infrastructure of the Internet that a Belfer Center report recently described as "too connected to fail" – in other words, whose failures could have widespread and potentially global impacts (Snyder, 2017), although these providers have also recognized that high availability and effective physical and personnel security are integral to a viable business model in a highly competitive market. Top-end hyperscale data centers feature security and resiliency measures that equal or exceed those of the most secure military command posts (Branscombe, 2016). These data centers illustrate one of the paradoxes of security on the Internet: while they are protected by many layers of physical security and maintain low profiles to avoid drawing attention to themselves – that is, they fit the profile of a "closed" network facility – many of the services they host are available to anyone with an email address, a valid credit card and access to a device running the essential IP protocol stack – in other words, they host "open" services.

Moving up from the core IP protocol layers of the Internet, one encounters the diverse set of software applications – core and functional services – that play a role in a military operation. Here again, ease of access varies widely and should not be taken as a "one size fits all" measure. For those applications that are available as open source or commercial off-the-shelf, the attack surface and the potential threats tend to be closely related: the more people using an application, the better the chance that attacks have been developed to exploit their vulnerabilities. For the many custom-developed applications employed in military operations, on the other hand, access to source or executable code, development and test documentation, and especially operationally relevant data, is much more limited. However, the simple cost of developing custom military software applications tends to prevent rigorous vulnerability testing.

Finally, moving up from the applications layer in the Internet, one leaves the man-made technical environment and enters what Withers calls the cognitive dimension: decision-making, doctrine, norms, perceptions and attitudes. This is easily the most complex dimension, but it is also not a new consideration for military operations. What is new is the role the Internet plays in enabling access to the cognitive dimension, both through new applications such as social media and streaming video and through new outlets for old applications such as electronic mail, chat, news reporting and psychological operations.

Even in the complex cognitive dimension, however, ease of access is neither universal nor something that can safely be taken for granted. At the simplest level, language is

still an effective barrier to entry. English might be the predominant language on the Internet, but it still ranks behind Mandarin and Spanish in number of native speakers. Context is another: although spearphishing still succeeds in fooling some users to click on links in untrustworthy emails, it would be much more difficult to convince a military operator to trust an email pretending to be a fragmentary order (FRAGO), if only because such communications are usually confined to military message handling systems. Finally, just because there is content on the Internet, it does not mean that anyone is looking at it. With over 1.3 billion websites alone, let alone social media services aimed at mobile users, there are a lot of opportunities to miss the audience.

Revelations about Russian manipulation of social media and its role in the 2016 US presidential election have certainly demonstrated how effective social media can be in advancing state aims. A recent report from Freedom House stated that: "Online manipulation and disinformation tactics played an important role in elections in at least 18 countries over the past year" (Freedom House, 2017). Skillfully positioned and executed, social media can be highly effective. Just six Facebook pages intended by Russian operators to sway US voter perceptions stimulated over 18 million interactions with other Facebook users before being shut down (McCarthy, 2017). As Michael Schmitt, editor of the *Tallinn Manual* and *Tallinn Manual 2.0*, has written, the Russian example illustrates the potential for states to exploit "grey zones" – areas where "international law principles and rules… are poorly demarcated or are subject to competing interpretations" (Schmitt, 2017).

4. THE INTERNET AND THE OPERATIONAL ENVIRONMENT

Part of the task of integrating cyberspace as a domain of military operations is that of fitting into an existing framework of operational doctrine. One aspect of this doctrine is that of the operational environment. NATO's basic doctrine for military operations, AJP-3(B), *Allied Joint Doctrine for the Conduct of Operations*, sets out the operational environment in terms of areas and boundaries. In particular, the Joint Operational Area (JOA) is defined as the "temporary area defined by the Supreme Allied Commander, Europe (SACEUR), in which a designated joint force commander plans and executes a specific mission at the operational level" (NATO, 2011 p. 1-23). While AJP-3(B) recognizes that "the operational environment is expanding, becoming more dispersed and non-linear", the intent of the definition of the JOA remains to ensure that all elements of a joint force "have a common understanding of its principal boundaries" (NATO, 2011 p. 1-22).

AJP-3(B) also establishes the concept of an Area of Interest (AOI), which it defines as "the area of concern to a commander relative to the objectives of current or planned operations, including his areas of influence, operations and/or responsibility, and areas adjacent thereto" (NATO, 2011 p. 1-23). These operational environment constructs have traditionally been defined in geographic terms and are intended to help the commander and operational planners to bound the area within which forces are employed and effects achieved. The operational environment also helps delineate the boundaries of command and control authorities and the rules of engagement.

Taking the topographical overview of the Internet as it relates to a NATO operation as above, there are aspects that fit well within the existing concept of the operational environment. The actual equipment used to access these Internet-connected networks and the troops supporting it in the operational theater – the cyber boots on the ground – clearly fall within the JOA. The equipment is an asset that must be protected as any other physical asset belonging to the forces in theater, and the troops are under the joint force commander's force protection responsibilities. In the same manner, the joint force commander would be expected to exercise operational control to ensure the availability, confidentiality and integrity of the information processed by these assets, whether against kinetic weapons, electronic warfare capabilities or cyber effects. This responsibility also extends to the data link and physical layers described above, so cabling and WiFi signals must be protected as well.

Interconnection to the Internet, however, is a primary reason for deploying this equipment to the theatre, and the gateways in the reachback facilities that provide those interconnections likely fall outside the geographical boundaries of the JOA. These anchor points and gateways may also fall outside the joint force commander's direct operational control. NATO is not alone in assigning the responsibility to run the information systems and networks supporting static military facilities to a civilian organization outside a direct military chain of command. For these reasons, the command and control (C2) arrangements between the joint force commander and the organization(s) providing his reachback support can be complicated and problematic. The commercial service providers responsible for the interconnections between these gateways are certainly both outside the JOA and outside the commander's operational control, as are the vast number of Internet users, devices, applications, data and services and the physical infrastructure supporting them that lie on the other side of the NATO and national static gateways. This also applies to most, if not all, of the Internet-connected critical infrastructures that might be supporting the operation of the static command and support facilities.

Given the prevalence of threats against the Internet and the networks that interconnect with it, it should also be clear that all of these aspects fall within what NATO doctrine

would consider the joint force commander's AOI. Each presents a greater or lesser risk to the success of the operation. Understanding and managing such risks, however, presents a significant challenge for a deployed commander. The already difficult task of situational awareness in cyberspace is further complicated by limitations on bandwidth to the theater and on the tools and expertise of the analysts in theater.

This is one reason why NATO, following the example of numerous nations, is centralizing its support for cyberspace situational awareness and operational planning support in the Cyberspace Operations Center (CyOC). It is far more effective to concentrate the technical, intelligence and operational expertise required for a credible cyberspace situational awareness capability than to attempt to replicate them in one or more operational theaters. However it is organized, this capability – even given the limitations of existing tools, models and data sources – is essential for effective military operations. Another reason is that Internet threats and their risks to operations often arise outside the JOA, not just in terms of geographical boundaries but also in terms of timeframe. Indeed, some of the most significant risks arising from the Internet are those we refer to as advanced persistent threats. Establishing a centralized and persistent situational awareness, planning and coordination capability is perhaps the single most important way in which existing NATO operational doctrine is being adapted to accommodate the unique aspects of cyberspace as a domain.

The delineation of the operational environment geometry also needs to extend to the littorals of the Internet-connected networks supporting an operation. Protection against physical and electronic threats has already been mentioned and is generally within the scope of established capabilities. Likewise, long-standing military practices developed well before the rise of the Internet, such as the use of radio silence, minimize, visual signaling and operational security (OPSEC), can still be of use to mitigate or avoid risks presented by Internet-based threats.

The cognitive dimension, however, still presents challenges. Clearly within the JOA and the commander's operational control are the troops in theater: their decisions, perceptions and actions, and how they communicate them, including over the Internet, are his responsibility. In the same way, he is responsible for how the joint force influences the perceptions of the adversary and affected populations, which is why psychological operations, information operations and strategic communications are integral to military operations. The Internet represents both a medium for conveying his messages and for assessing perceptions among targeted audiences.

As the examples of state-sponsored manipulation of social media demonstrate, however, Internet-based threats are emerging that are difficult to fit into the traditional concept of the operational environment geometry. Indeed, it could be

argued that military operations are not the appropriate mechanisms to target what are purely civilian objects (Harrison-Dinniss, 2015); but the key problem in applying the operational environment geometry is that these threats currently fall into what Schmitt calls the "grey zone," where boundaries of operational control are informed and guided by international law. As Schmitt has put it: "The brighter the redlines of international law as applied to cyber activities, the less opportunity states will have to exploit grey zones in ways that create instability." (Schmitt, 2017) And the easier it will be to delineate how to draw the lines of military responsibility and interest.

The closed networks required to support an operation tend to have far fewer cyber defence considerations for a commander than the Internet. The example of the Internet's topography is offered, however, to illustrate that it is certainly possible to sort these considerations into three rough categories: those within the JOA and under operational control; those within the AOI and within some level of control, if indirect; and those that fall well outside both military authority and the means of any commander to control. By sorting the cyberspace considerations for an operation into these three categories, commanders can begin to identify where effective military response options exist and where they do not.

Those considerations that are within the JOA and within the commander's operational control are those for which existing doctrine is most suitable. Considerations in this category must clearly take first priority for operational planning and situational awareness. This is the area where planners need most to be informed by intelligence about the physical, electronic and cyber threats to be expected in theater. This is also where the commander needs to assess the value of such tried and true practices as the use of radio silence, alternate communications and minimize to mitigate or avoid the risks these threats might present. Finally, this is where the protection – or vulnerability – of cyberspace littorals can have the greatest direct impact on the operation.

The next category covers those considerations that are within the commander's AOI and within some type of C2 arrangement, however problematic. From a planning standpoint, considerations in this category are better addressed by a central and strategically-placed function such as the CyOC for the reasons noted above: theater-based limitations (bandwidth, tools and personnel) and the fact that many of these considerations derive from conditions that are persistent and not tightly coupled to the specifics of the operation, and which likely span multiple operations.

The third category covers those that are within the AOI but outside operational control, even via C2 arrangements. Most of these considerations, such as the protection of critical infrastructures, the security of Tier 1 Internet providers and hyperscale data centers, and state manipulation of social media and other examples of what Schmitt

terms the "grey zone" are wholly outside the military span of control. These challenges can only be addressed through political, diplomatic, legal or regulatory channels. Such liaison falls well outside the current scope of Civil-Military Co-operation (CIMIC), which is typically focused on liaison between the joint force commander and civilian authorities in theater. Another important adaptation of existing doctrine to accommodate cyberspace may be in developing persistent versions of CIMIC between centralized military capabilities like the CyOC and their civil counterparts.

5. CONCLUSIONS

There has been no shortage of sweeping generalizations in much that has been written on cyberspace operations and cyber security. As NATO and national militaries work to establish cyberspace as an operational domain, precision is essential to developing a mature discipline with a solid base of concepts, terminology, techniques, tactics and procedures. One such precision is to recognize that operations in the domain of cyberspace always involve specific networks of networks, of which the Internet is only one. Another is to recognize that the characteristics, threats and risks associated with any particular network vary depending on which aspect of its topography is considered. The ease of access that exists on one plane or elevation, such as the common core set of Internet Protocols, might not characterize another, such as that of submarine telecommunications cables.

This precision is also important to integrating cyberspace into existing doctrine. Cyberspace considerations that fit well within existing constructs such as the JOA and operational control can, for the most part, be addressed by the operational commander in theater. Others are better addressed by a central cyberspace operational planning and situational awareness function such as the CyOC being established in NATO. Finally, there are considerations that either fall clearly outside the scope of military control, or for which such demarcation is still difficult. For these, effective mechanisms for civil-military co-operation need to be established. Such a framework can channel efforts in a practical way and help speed the process not only of implementing cyberspace as an operational domain but of better defending the Alliance against the threats arising from the Internet and the other networks it depends upon.

REFERENCES

Branscombe, M. (2016, November 2). *Inside a hyperscale data center (how different is it?)*. Retrieved from CIO.com: https://www.cio.com/article/3137719/data-center/inside-a-hyperscale-data-center-how-different-is-it.html.

CAIDA. (2016, September 1). *AS Ranking*. Retrieved from Center for Applied Internet Data Analysis (CAIDA): http://as-rank.caida.org/.

CCDCOE. (2017, December 16). *Cyber Definitions*. Retrieved from NATO Cooperative Cyber Defence Centre of Excellence: https://ccdcoe.org/cyber-definitions.html.

Cisco. (2016). *Cisco Global Cloud Index: Forecast and Methodology, 2015–2020*. Retrieved from Cisco.com: https://www.cisco.com/c/en/us/solutions/service-provider/global-cloud-index-gci/white-paper-listing.html.

Common Ground Alliance. (2017, August 11). *2016 Damage Incident Reporting Tool (DIRT) Analysis and Recommendations Report*. Retrieved from Common Ground Alliance: http://commongroundalliance.com/media-reports/dirt-report-2016.

Freedom House. (2017, November). *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy*. Retrieved from Freedom House: https://freedomhouse.org/report/freedom-net/freedom-net-2017.

Geer, D. (2013, April 26). Resolved: the Internet Is No Place for Critical Infrastructure. *ACMQueue, 11*(4). Retrieved January 1, 2018, from http://queue.acm.org/detail.cfm?id=2479677.

Harrison-Dinniss, H. (2015, March). The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives. *Israel Law Review, 48*(1), 39-54.

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

IETF. (1989, October). *RFC (Request for Comments) 1122: Requirements for Internet Hosts - Communication Layers*. Retrieved from Internet Engineering Task Force (IETF): https://tools.ietf.org/html/rfc1122.

IETF. (1989, October). *RFC (Request for Comments) 1123: Requirements for Internet Hosts - Application and Support*. Retrieved from Internet Engineering Task Force (IETF): https://tools.ietf.org/html/rfc1123.

Kenett, D. Y., et al. (2014). Network of Interdependent Networks: Overview of Theory and Applications. In G. D'Agostino, et al. (*SCALA, Network of Networks: The Last Frontier of Complexity* (pp. 3-13)). Cham: Springer International Publishing.

Khazan, O. (2013, July 16). The Creepy, Long-Standing Practice of Undersea Cable Tapping. *The Atlantic*. Retrieved January 1, 2018, from https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/.

McCarthy, T. (2017, October 14). *How Russia used social media to divide Americans*. Retrieved from The Guardian: https://www.theguardian.com/us-news/2017/oct/14/russia-us-politics-social-media-facebook.

Merriam-Webster. (2018, January 1). *Topography - definition of topography*. Retrieved from Merriam-Webster: https://www.merriam-webster.com/dictionary/topography.

NATO. (2011, March 16). *Allied Joint Publication (AJP) 3(B), Allied Joint Doctrine for the Conduct of Operations*. Retrieved from NATO Standardization Office: http://nso.nato.int/nso/zPublic/ap/ajp-3(b).pdf.

Pompon, R. (2016). *IT Security Risk Control Management: An Audit Preparation Plan*. New York City, NY, USA: Apress.

Scheier, F. (2015). *On Cyberwarfare (DCAF Horizon 2015 Working Paper No. 7)*. Retrieved from Geneva Centre for the Democratic Control of Armed Forces (DCAF): https://www.dcaf.ch/cyberwarfare.

Schmitt, M. N. (Ed.). (2016). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. New York City, NY, USA: Cambridge University Press.

Schmitt, M. N. (2017, August 8). *Grey Zones in the International Law of Cyberspace (2017 James Crawford Lecture on International Law)*. Retrieved from https://ore.exeter.ac.uk/repository/handle/10871/27563.

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

Snyder, C. (2017). *Too Connected to Fail*. Harvard Kennedy School, Cyber Security Project. Cambridge, MA, USA: Belfer Center. Retrieved January 1, 2018, from https://www.belfercenter.org/publication/too-connected-fail.

US Army. (2017). *Field Manual 3-0, C1: Operations*. Washington, DC, USA.

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

World Internet Users and 2017 Population Stats. (2017, June 30). Retrieved December 2017, from Internet World Stats: http://www.internetworldstats.com/stats.htm.