2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

Beyond Domains, Beyond Commons: Context and Theory of Conflict in Cyberspace

Jeffrey L. Caton
Science and Technology Division,
Center for Strategic Leadership
U.S. Army War College
Carlisle Barracks, Pennsylvania, U.S.A
jeffrey.caton@us.army.mil

Abstract: This paper examines implications of the collective cognitive blind spot of national security leaders with regard to conflict and warfare in and through cyberspace. It argues that the view of cyberspace as a contested domain within a global commons is not sufficient to address the full range of conflict therein. It posits that deliberate examination of the ontology and evolution of cyberspace is essential to properly inform the management of resources, forces, and risk. It discusses analytical frameworks to explore the fundamental structures of cyberspace and endeavors to provide the theoretical underpinning necessary to inform the broader dialogue addressing concepts such as complexity and emergence, self-organization and self-governance, human-machine integration, influences of ethics and philosophy, and the blurring of distinction between the cognitive, content, and connectivity dimensions. It strongly encourages leaders in cyberspace security planning to adopt a bifurcated approach that not only addresses the immediate challenges in cyberspace, but also includes a parallel and distinct effort to examine and characterize future manifestations of cyberspace.

Keywords: *cyberspace, theory, ontology, evolution, conflict, commons*

1. INTRODUCTION

Often, cyberspace security resembles the analogy of the blind men and the elephant—that is, the scope of activity reflects only the part of cyberspace encountered. Working together, the blind men can divine the whole of the elephant from their perceived parts. Unlike the constant form of the elephant, cyberspace is changing rapidly; this creates an expanding chasm between the perceived and the actual cyberspace environment. This situation may degrade a nation's ability to conduct critical analysis regarding future investments in cyberspace infrastructure,

The views expressed are those of the author and do not necessarily reflect official policy or position of the United States Army War College, the Department of the Army, the Department of Defense, or any other Department or Agency within the U.S. Government. All information and sources for this paper were drawn from unclassified material.

personnel, and education. This paper argues that the current demands of international security entail consideration of contexts beyond the limited view of cyberspace as a contested domain. Further, understanding the future strategic security environment requires the examination of cyberspace ontology, a study of its evolution, and the development of theory regarding activities in cyberspace. To investigate this assertion, we first examine the model of cyberspace as a contested domain and then broaden to view cyberspace as a commons encompassing all elements of national power. Next, we explore the complex structure and dynamic nature of the commons and the related international security implications. Finally, we reach beyond the commons view to address the ontology and future of cyberspace itself. The goal is to broaden the reader's perspective regarding the context and theory of cyberspace in the current global security environment as well as to encourage understanding of the fundamental nature of cyberspace and its complex and dynamic evolution beyond the complacency of technical stovepipes.

2. CYBERSPACE AS A CONTESTED DOMAIN

What are the current perceptions of the roles of cyberspace in the international security environment? The U.S. government defines cyberspace as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers" and it "also refers to the virtual environment of information and interactions between people" [1]. Considering the well-documented historic cases of Titan Rain (2004) [2], Estonia (2007) [3], Georgia (2008) [3], and Operation Buckshot Yankee (2008) [4] as well as recent mysteries such as the Conficker and Stuxnet worms, cyberspace can be portrayed as a contested domain. Consistent with this view, U.S. Cyber Command achieved Full Operational Capability in October 2010, with its mission to direct operations and defense of Department of Defense (DoD) networks, conduct full-spectrum military cyberspace operations, and ensure U.S. and Allied freedom of action in cyberspace and deny the same to adversaries [5]. Complementary to this mission, the *DoD Strategy for Operating in Cyberspace* was released in July 2011 as the first DoD unified strategy for cyberspace [6]. These DoD initiatives mesh well with the tenets of the June 2010 North Atlantic Treaty Organization (NATO) Policy on Cyber Defence which emphasizes prevention, resilience, and non-duplication. This policy strives to "integrate cyber defence considerations into NATO structures and planning processes in order to perform NATO's core tasks of collective defence and crisis management" [7]. The collective approach of these 28 nations is to treat cyberspace as another domain—like land, sea, air, or space—used to control and exploit with the intent of exerting influence on the other domains. The immediate focus is on defense; although clearly a perfect defense is not possible even within the limits of a military domain. It becomes even more challenging when government protection systems, such as the EINSTEIN 3 intrusion-detection system, are considered to protect private critical infrastructure networks [8]. The strategies address recent historical events—distributed denial of service, botnets, patriotic hackers—that reflect the brute-force approach to cyberspace aggression.

Consistent with current U.S. joint force doctrine, cyberspace operations encompass the three dimensions of the information environment—cognition, content, and connectivity. At present, the content and connectivity portions are emphasized since they involve the software and hardware portions of cyberspace. However, many existing plans focus on threats and activities that are actually historical in terms of the relative rate of cyberspace growth and change. Without a more progressive context, near-term activities in cyberspace may be misguided, and long-term planning for investment and force structure there may be obsolete before they are enacted.

3. BEYOND DOMAINS TO THE COMMONS

To gain a broader outlook of cyberspace, let us consider the commons paradigm and then examine theoretical models and the related complex and dynamic nature. Commons are areas not controlled or owned by any single entity, and states and non-state actors use them to conduct commerce and communication [9]. In such a commons, a nation could exercise cyberpower as its "ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power" [10]. The cyberspace commons has unique features that facilitate use to entities smaller than nation-states. There are many low-cost options available that provide users with reliable access. Users' persona in cyberspace need not match their true appearance and it is possible to have multiple representations simultaneously; this degree of anonymity may challenge efforts to attribute activities in cyberspace. Cyberspace can enable one to initiate a variety of physical effects across vast distances at almost instantaneous speeds [11]. Thus, determining if cyberspace should be treated as a domain or a commons depends on the level of application. Developing force structures and unit competencies may be served best by the domain view; examining the extent and priority of cooperative engagement amongst countries may be served best by the commons view.

A. Theoretical Models

What are some methodologies that provide a context beyond the domain concept for evaluating activity in cyberspace? Consider two examples of theoretical frameworks to guide strategy development and implementation.

1. Ecosystem Model

In March 2011, a Department of Homeland Security paper proposed a "healthy cyber ecosystem" as a model for enabling security in cyberspace. Based in part on the human immune system, the concept envisions future cyber devices with "innate capabilities that enable them to work together to anticipate and prevent cyber attacks, limit the spread of attacks across participating devices, minimize the consequences of attacks, and recover to a trusted state" [12]. The model uses mutually supporting healthy cyberspace devices working together proactively and dynamically to assess the severity of any "infection" and respond when an appropriate "alert threshold" is exceeded. But anomalous and negative activities in cyberspace are not always attacks; they may be manifestations of complex interactions and emergence of unanticipated behavior. Thus, automated active defense systems must ensure that attacks are clearly distinguished from mere alerts [12]. Such measures may create an information environment that is largely self-regulating with respect to mundane threats. However, just as strengthening human immune systems may have the counterproductive effect of producing more virulent strains of germs, one may ponder what new threats could emerge in a healthy cyberspace environment.

2.Naval Theory Analogy

Traditional (i.e., Mahanian) naval theory offers value for modeling military activities as domain operations within a global commons. When one connects major ports in the littoral area ("brown water") to other ports in the world, "sea lines of communication" emerge in the broad ocean ("blue water") that have strategic importance based on factors such as geography and traffic volume [13]. Similarly, one can map cyberspace to show "cyber lines of communication" and nodes with tactical, operational, and strategic implications, perhaps even choke points—the "blue water cyberspace" equivalent of the Strait of Hormuz.

Barney [14] uses the 1982 United Nations Convention on the Law of the Sea framework to examine issues related to routing information through cyberspace. He proposed *national cyberspace* as "the region of Cyberspace in which individual States require substantial sovereign rights to preserve the political and economic security." He divided this region into *internal cyberspace*, "where a State may exercise complete sovereignty," and *territorial cyberspace* "through which, and to which, governments, commercial enterprises, or private organization allow generally unrestricted access." *International cyberspace* is a region with no physical analogy to international waters; it "is not a physical place; it is a *characteristic* of Cyberspace by which a data packet is not physically present anywhere but is merely in transit" [14].

Like ship traffic crossing oceans, consider information traffic as packages of data moving across electromagnetic waves in cyberspace. The right of innocent passage provides "the right to traverse the territorial sea in a continuous and expeditious manner, so long as the passage is not prejudicial to the peace, good order, or security of the coastal State." The right of transit passage provides "freedom of navigation and overflight solely for the purpose of continuous and expeditious transit of the international strait between one part of the high seas or an exclusive economic zone and another part." Transit passage provides the advantages that "forces may transit in their normal mode of operation (i.e., warfighting) and bordering States may not suspend the right of transit passage through international straits." Applying these principles to cyberspace, Barney concludes that computer network attack (CNA) "may be lawfully transmitted through the international telecommunications infrastructure, including Internet routers physically located in neutral States." He notes in his scenario that such passage does not violate territorial sovereignty, nor comprise an act of force in the intermediate territory, nor violate the status of neutral States [14]. Perhaps this framework could allow data packets to be "nationally flagged" akin to ships—thus having data itself represent sovereignty and facilitate development of diplomatic measures that allow (or deny) packet transit. In turn, this could help the international community respond to unauthorized rerouting of packets via router disruption, such as China is accused of doing in 2010 [15].

This model may also facilitate development of theory related to virtual environments—that is, the immersion of the cognitive mind in non-physical landscapes defined by code often distributed among many machines. Perhaps the concept of naval subsurface activity can model virtual activity. Arguably, it is more difficult to "track" individuals, groups, and activities when they go below the "normal surface" of cyberspace (whatever that truly is) into the multi-dimensional subsurface virtual environment. Conversely, when they "re-surface," their presence may be more readily acknowledged and attributed. The concept of riverine operations—those that focus on a nation's inland waters—may offer models for devolved operations in cyberspace "backwaters."

This would focus on activities that use older technology, such as telephone modems and DOS-based bulletin boards, instead of modern Internet connections [16]. Regardless of how packets travel, their movement through cyberspace may meet resistance in the same way ships navigate through waves and currents. Thus, ensuring freedom of navigation in cyberspace must necessarily include not only adversarial efforts to deny or disrupt, but also entropic effects and physical environment impacts (e.g., power outages, solar storms).

B. Key Characteristics of its Complex Structure

The limits of cyberspace are uncharted with rapidly expanding boundaries and increasingly complicated internal configurations. With land, sea, air, or space, technology dictates the ability to access and maneuver within the commons, but the physical structure remains relatively constant. For cyberspace, technology not only dictates how we access the common, but it also empowers the manifestation of the common. Cyberspace may be unique in that access and creation are almost synonymous—that is, the technology used to access cyberspace (e.g., computers, mobile devices) becomes an inherent part of the domain. When entering cyberspace, one must consider the *reciprocity of connectivity* associated with the access. If a user connects a device to the cyberspace commons, then the whole of the commons can connect to that device—this axiom helps define the realm of the possible. Thus, it is impossible to open a perfect one-way portal into cyberspace; any data sent or accessed over cyberspace can be viewed by anyone in cyberspace. Some applications of this process go unnoticed by even experienced users, such as the demonstrated vulnerability of modern automobile electronic control units to access and command by wireless systems [17]. Granted, such access may require illegal or unethical activity, but this does not make the action impossible.

Similar to other mediums, the active cyberspace environment has discernable structure that supports the disorderly movement of its contents. Classic thermodynamic modeling characterizes such random motion and disorder as "entropy." The transmission of data over the Internet may result in its division into many subpackets sent over different paths through an unknown number and type of processors and switches. Cyberspace is inherently complex and disorderly; the degree of which only increases as cyberspace expands with additional devices and infrastructure. It is not logical to expect order to arise spontaneously out of such a cacophony. This means that deliberate energy is required to accomplish specific tasks, and designers of content and connectivity may attempt to decrease the entropy involved with their specific function. Conversely, one could consider the overlay of security measures as purposely adding entropy to a system to thwart unauthorized use (e.g., using encryption to leverage the disorder for security's advantage). To overcome such entropy, an adversary must expend effort.

Operations in cyberspace are more difficult to accurately characterize in the realm of human cognition than traditional kinetic domain operations. Thus, promises that cyberspace offers the ultimate form of achieving precision effects may be hollow. Achieving well-characterized and bounded effects in cyberspace is more difficult than doing so in physical space, and the potential for unanticipated consequences is more likely. Further, the means and methods used to achieve precision have limited utility since their design is based on a configuration of cyberspace that is destined to change (by design or coincidence). For example, the unpredictable interaction of well-designed trading algorithms led to the "flash crash" disorder in the U.S. stock market on May 6, 2010 [18].

C. Challenges of its Dynamic Nature

Internet-enabled communications have progressed to where most users consider them direct and instantaneous. This illusion reflects the shortcoming of human perception—electrons traveling at the speed of light can circle Earth in about 130 milliseconds, one-third the time of a human eye blink. In the physical world, if one fires a weapon at a 10-meter target, the bullet follows a largely predictable path based on the gross properties of the air (e.g., temperature, wind). Interactions at the molecular level are negligible compared to the bullet's momentum, thus it follows a direct path and achieves kinetic effects at the point of impact. In cyberspace, the transmission of a data packet is assumed to follow a direct path in a stable environment. In reality, one could argue that the configuration of cyberspace at the micro level may change significantly in the milliseconds it takes to press the "Enter" key. Although the effects and path appear to be direct from a human perspective, in the relative framework of cyberspace operations, they are indirect, inefficient, and slow to manifest. Thus, projecting a guaranteed path in cyberspace is nearly impossible, just as it is impossible to align the molecules of air to accommodate a passing bullet. Consider that the May 6, 2010 stock market "flash crash" was preceded by over 10,000 ultrafast-duration crashes and spikes (less than 950 ms each) over 5 years, and that these ultrafast events continue to occur [19]. Then, the goal of the cyberspace operator is to determine not only the gross properties affecting cyberspace operations (if indeed they exist) but also the potential anomalies that may arise spontaneously as well as how to operate in them.

How should nations balance the command and control of cyberspaces forces at the battlespace level with those at the strategic level? Tyugu [20] argues that application of artificial intelligence methods (e.g., neural nets, expert systems, intelligent agents) is unavoidable for such large-scale cyber defences. Leaders must consider the scope of operational effects within the commons to coordinate them with other commanders and allies as well as affected public and industry. For example, it may be prudent to receive "cyberspace over flight permission" for offensive actions that may transit the territorial cyberspace of other nations.

4. CURRENT INTERNATIONAL SECURITY IMPLICATIONS

For alliances such as NATO, what implications arise from adopting an analysis framework for international security of a contested cyberspace domain within the larger commons? Let us examine three topics—the development of cyberspace policy and strategy; operational planning considerations to address immediate issues; and future planning. These topics mirror the NATO overarching cyber defence principles of prevention, resilience, and non-duplication.

In an ideal world, a policy that maintains the cyberspace commons as a sanctuary free of conflict is laudable. However, previous and ongoing aggression in cyberspace mandates that portions of cyberspace be militarized. The November 2010 Lisbon Summit's new NATO Strategic Concept calls for a "full range of capabilities necessary to deter and defend against any threat" among which is the requirement to "develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities" [21].

Developing cyberspace deterrence is a challenging task still in its infancy. Traditional Cold War deterrence experience may have limited application in cyberspace, given the capabilities of nonstate actors as well as the possibility of cyberattacks originating from co-opted servers in neutral countries[4]. The May 2011 U.S. *International Strategy for Cyberspace* [22] includes a deterrence policy with application to all national interests (including NATO obligations). Based on the principle that "consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace," the strategy states that "when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country." Further, the U.S. will "reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests." These words send a serious message to potential adversaries without limiting the type of U.S. response.

But if deterrence fails, what analysis can support assessment of cyber incidents to determine if they require a NATO response? There is no internationally accepted definition of when hostile actions in cyberspace are recognized as attacks, let alone acts of war. An analytical framework developed by Schmitt [23] attempts to determine if a cyber attack equates to the use of force per terms of the U.N. charter. His analysis considers the intensity of damage in seven areas (severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility) to provide a composite assessment of the effects of the cyber attack. Further, it addresses implications of applying Article 51 of the United Nations (U.N.) Charter for attacks prior to acknowledged armed conflict, and the law of armed conflict (LOAC) criteria for acknowledged conflict.

When it is clear that aggressive actions in cyberspace require a response, alliance actions need appropriate planning and execution. Analyzing courses of actions should include thorough evaluation of nth-order effects, not only for desired military outcomes but also for related diplomatic and economic consequences [24]. While some measures of automated defense may be necessary to protect critical functions, perhaps like neural reflexes to protect one's hand from a hot stove, the indiscriminate application may create more problems than it solves. Determining the appropriate collective response is a balancing act that may require the rapid synthesis of multiple distributed systems as well as a clear representation of any automated response, perhaps aided by graphical means, to assess the impact of the countermeasures on network resources [25].

Credible responses also depend on having properly equipped and trained personnel. Can our current understanding of cyberspace properly inform resource and force management decisions? Despite some technical promises, it is risky to consider the current application of cyberspace operations as guaranteed successes. Developing theoretical principles for cyberspace may help to explore the opportunities as well as shortcomings that affect such operations. In a technical sense, planners and decision makers need to recognize that applications may be neither precise nor free from disorder. Thus, they should conduct critical, perhaps even skeptical, reviews of promised capabilities—especially when making resourcing decisions. Investments in technology to enhance effective command and control of alliance forces must consider the implications of operating at ever-faster network speed, such as the risks associated with selecting between proactive and reactive actions to address simultaneous system challenges [26]. Changes in the cyberspace domain and commons may be significant in the time between decision for action and its execution. Also, responsible offensive actions should incorporate "cyberspace battle damage assessment" to help ensure the necessity, distinction, and proportionality of the effects meet acceptable norms. The access to nearly limitless data may be used wisely for evaluation, but biases in data mining methodologies may reinforce and propagate cognitive blind spots. The best way to avoid such pitfalls is to examine objectively and holistically the fundamental nature of cyberspace and to envision its evolution and future embodiment.

5. BEYOND THE COMMONS – ONTOLOGY AND FUTURE

Are we developing methods to achieve situational awareness at all levels of cyberspace? This section discusses the ontology of cyberspace and recommends action in four areas to facilitate international security efforts: develop cyberspace theory; assess cyberpower of global actors; anticipate radical change; and bifurcate future-focused efforts from current operational activities.

Military activities in other domains (land, sea, air) often strive to gain local and temporal control of such domains. In contrast, cyberspace can be considered an artificial domain created for the purpose of exercising control or governing activities. It requires energy to exist (e.g., use of the electromagnetic spectrum) and its control can be first-order—conscious and deliberate—or various levels of nth-orders that may be unconscious, accidental, or emergent. It exists as part of a larger commons, both physical and virtual. To prepare for conflict beyond our current technological manifestation of cyberspace, even the commons model is insufficient. For a truly holistic view, one must examine the ontology of cyberspace (i.e., its fundamental essence) and determine how its current form fits into its overarching evolutionary path. Cyberspace ontology must address fundamental issues, such as the balance of dynamic stability for activity in cyberspace; the self-organization and self-regulation of its functions; the modeling of entropy to include concepts of convergence, divergence, and emergence; and the changes in the cognitive dimension caused by more sophisticated human-machine interfaces (e.g., neuralprosthetics [27]). Proper cyberspace theory can provide the foundation necessary to explore these ontological themes.

Starr [28] advocates that proper cyberspace theory address five areas: definition of terms; categorization and structure of theory elements; explanation of elements by analysis and example; connection of elements for comprehensive examination; and anticipation of future activities. As cyberspace theory is refined, it should be used to assess the relative strength of global actors possible through cyberpower. Future embodiments of cyberspace will likely follow the model of human conflict described by the Clausewitzian trinity of emotion, reason, and chance. As witnessed in the so-called "Arab Spring" events, social media via cyberspace can provide a conduit for human expression to force change on the world stage [29]. Pursuing holistic situational awareness can help decision makers distinguish aggression in cyberspace from coincidental events with negative repercussions. This may be crucial during times of increased global tension. It is unlikely that cyberspace will lift the fog of war or make the application of force less subject to chance; entropy and emergence simply cannot be quantified in all circumstances. Cyberspace strategies that anticipate flaws and failures, and emphasize resilience by design, may provide enduring principles for the future.

With its increasingly complex and dynamic nature, future embodiments of cyberspace may exhibit radical change. If its structure progresses toward self-organization and self-regulation, cyberspace may surpass fully human design and control. Important research is addressing some specific aspects of change, such as the behavior and long-term strategic evolution of botnet armies [30]. Sornette [31] examined how the strengths of heterogeneity and coupling interactions among systems may shift their overall behavior from synchronization to self-organization. Of note is that extreme-risk events may occur more often than predicted for systems with low heterogeneity and high coupling—basically the situation one might find in centralized network controls with standardized desktops.

We must refine theoretical models to reflect how the balance shifts among the cognitive, content, and connectivity dimensions in the information environment. This may ameliorate the current overemphasis on information technology, as its influence may diminish. Leaders should anticipate significant blurring of the cognitive and connectivity dimensions as human-machine interfaces become more engrained and pervasive. Temmingh and Geers [32] have examined some the present challenges of distinguishing real individuals from potentially multiple cyber persona. For the future, leaders should consider the possibilities presented by blurring of the cognitive and content dimensions as information is consolidated in cloud-type applications and the collective computational and memory capacities of machines exceed that of humankind. Koch and Hepp [33] explore the possible roles of quantum mechanics in creating higher brain functions (e.g., perception, consciousness, free will). Eventually, the examination of cognition will expand to the broader human condition to include concepts of morality and ethics, and perhaps theology. This presents an essential question: is cyberspace merely a manifestation of technology, or possibly a fundamental step in human evolution?

Consider two concepts regarding the potential role of cyberspace in human evolution. First is the concept of “the singularity” explored by futurist Ray Kurzweil [34] as a “future period during which the pace of technological change will be so rapid, its impacts so deep, that human life will be irreversibly transformed.” Kurzweil posits three overlapping revolutions surrounding this event—genetics, as an intersection of information and biology; nanotechnology, as an intersection of information and the physical world; and robotics, as a growth of artificial intelligence. The second concept is “the noosphere” explored by Pierre Teilhard de Chardin [35] as an extension of the biosphere to the realm of human thought. In *The Phenomenon of Man*, he describes it as “much more coherent and just as extensive as any preceding layer, it is really a new layer, the ‘thinking layer,’…outside and above the biosphere there is the noosphere.” Teilhard de Chardin posited some implications for humanity like those of Kurzweil, albeit through an approach of philosophy vice technology. Whether such predictions come to fruition is not the point; their ideas influence the views of human behavior that in turn influence activities of creation and utilization in cyberspace. Since it is doubtful that legal and governance regimes will keep pace with a dynamic cyberspace environment, the establishment of a cooperative set of cyberspace ethics and value may facilitate stability and organization.

The urgent needs of international security leave few resources available for the study of cyberspace ontology and future. Relegating such activity to a mere afterthought of domain operations promises its failure, or at best, an empty victory. Thus, a bifurcated approach to policy, strategy, planning, and military preparation can best serve international cyberspace security. The first part—addressing immediate challenges in cyberspace—is in place, albeit with limitations. Actions are often reactive and ad hoc, with a decision-making context that may lag technology and not consider synergistic implications. The second part—examining future manifestations of cyberspace—can provide the cognitive foundation that informs the development of strategy, doctrine, force structure, and prioritization of resources; these in turn can help achieve unity of effort amongst all instruments of national power. This must be a separately resourced effort focused on development of theory as well as the study of ontology and evolution. This may require bold leadership and perhaps the courage to risk considering concepts that may appear foolish at times.

6. SUMMARY

While we can evaluate certain aspects of international competition and conflict in cyberspace using a domain model, the proper examination requires a holistic approach that includes concepts of the commons as well as a conscious future-directed model that recognizes the continuing evolution of cyberspace. Cyberspace theory should embrace the potential for radical emergent behavior that may shift the balance of influence among the cognition, content, and connectivity dimensions. This requires the deliberate and thoughtful pursuit of cyberspace theory as a continuing dialogue that may include multiple frameworks for analysis. This may not occur without a formal bifurcated approach to international efforts—one that is integrated to address both the pragmatic and urgent present challenges as well as a separately resourced effort dedicated to examining the changing nature of cyberspace itself. NATO has the nascent elements of such a bifurcated approach in place with its Allied Command Operations for the immediate issues and Allied Command Transformation for the future issues related to conflict in cyberspace. Without such a comprehensive view, planners and decision makers add risk in their activities by not characterizing the full spectrum of the interactions and effects of creation and operation in cyberspace.

REFERENCES

[1] "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure." Washington, DC: The White House, May 2009.

[2] T. L. Thomas. "Google Confronts China's 'Three Warfares'." *Parameters*, vol. 40, no. 2, pp. 101-113, Summer 2010.

[3] S. W. Korns and J. E. Kastenberg. "Georgia's Cyber Left Hook." *Parameters*, vol. 38, no. 4, pp. 60-76, Winter 2008-2009.

[4] W. F. Lynn III. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs*, vol. 89, no.5, pp. 97-108, Sep./Oct. 2010.

[5] "U.S. Cyber Command Fact Sheet." Fort Meade, MD: U.S. Cyber Command Public Affairs, Oct., 2011.

[6] "Department of Defense Strategy for Operating in Cyberspace." Washington, DC: Dept. of Defense, Jul. 14, 2011.

[7] "Defending the Networks: The NATO Policy on Cyber Defence." Brussels, Belgium: NATO Public Diplomacy Division, Jun. 2011.

[8] S.M. Bellovin et al. "Can It Really Work ? Problems with Extending EINSTEIN 3 to Critical Infrastructure." *Harvard National Security Journal*, vol. 3, pp.1-38, 2011.

[9] A. M. Denmark and J. Mulvenon. "Contested Commons: The Future of American Power in a Multipolar World." Washington, DC: Center for a New American Security, Jan. 2010.

[10] D. T. Kuehl. "From Cyberspace to Cyberpower: Defining the Problem." in *Cyberpower and National Security*, Washington, DC: National Defense University Press and Potomac Books, 2009, pp. 24-42.

[11] J. L. Caton. "Cyberspace and Cyberspace Operations." in *Information Operations Primer*, AY12 ed., Carlisle, PA: U.S. Army War College, Nov. 2011, pp. 19-32.

[12] "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action." Washington, DC: Depart. of Homeland Security, Mar. 23, 2011.

[13] A.T. Mahan. *The Influence of Sea Power Upon History 1660-1783*. Mineola, NY: Dover, 1987 reprint, pp. 30, 31-32.

[14] S. M. Barney. "Innocent Packets? Applying Navigational Regimes from the Law of the Sea Convention by Analogy to the Realm of Cyberspace." *Naval Law Review*, vol. 48, pp. 58-87, 2001.

[15] "2010 Report to Congress of the U.S.-China Economic and Security Review Commission." Washington, DC: U.S. Government Printing Office, Nov. 2010, pp. 243-244.

[16] "The 'Wild and Woolly' World of Bulletin Boards." *All Things Considered*, National Public Radio, Nov. 21, 2009.

[17] K. Koscher *et al*. "Experimental Security Analysis of a Modern Automobile." presented at the 2010 IEEE Symp. On Security and Privacy, Oakland, CA, May 2011.

[18] "Finding Regarding the Market Events of May 6, 2010: Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues." Washington, DC: U.S. Commodity Futures Trading Commission and U.S. Securities and Exchange Commission, Sep. 30, 2010.

[19] Johnson et al. "Financial black swans driven by ultrafast machine ecology." technical working paper, Cornell University Library, Ithaca, NY, Feb. 2012.

[20] E. Tyugu. "Artificial Intelligence in Cyber Defense." *Proc. 2011 3rd Conf. on Cyber Conflict*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2009.

[21] "Active Engagement, Modern Defence: Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation." adopted by Heads of State and Government in Lisbon, Portugal: NATO, Nov. 19, 2010.

[22] B. Obama. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." Washington, DC: The White House, May 2011.

[23] J. B. Michel et al. "Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System," *Proc. of Twenty-seventh Annu. Int. Software and Applications Conf.*, Dallas, TX: IEEE, Nov., 2003.

[24] D. Bilar. "On nth Order Attacks." *Proc. 2009 Conf. on Cyber Warfare*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2009.

[25] G. Klein *et al*. "Enhancing Graph-based Automated DoS Attack Response." *Proc. 2009 Conf. on Cyber Warfare*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2009.

[26] L. Beaudoin, N. Japkowicz, and S. Matwin. "Autonomic Computer Network Defence Using Risk State and Reinforcement Learning." *Proc. 2009 Conf. on Cyber Warfare*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2009.

[27] E. Skoudis. "Information Technology and the Biotech Revolution." in *Cyberpower and National Security*, Washington, DC: National Defense University Press and Potomac Books, 2009, pp. 241-250.

[28] S. H. Starr. "Toward a Preliminary Theory of Cyberpower." in *Cyberpower and National Security*, Washington, DC: National Defense University Press and Potomac Books, 2009, pp. 43-88.

[29] N. J. DeLong-Bas. "The New Social Media and the Arab Spring." *Oxford Islamic Studies Online*, Jun. 2011.

[30] O. Thonnard, W. Mees, and M. Dacier. "Behavioral Analysis of Zombie Armies." *Proc. 2009 Conf. on Cyber Warfare*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2009.

[31] D. Sornetter. "Dragon-Kings, Black Swans and the Prediction of Crises." *Int. J. of Terraspace Sci. and Eng.*, pp. 1-18, 2009.

[32] R. Temmingh and K. Geers. "Virtual Plots, Real Revolution." *Proc. 2009 Conf. on Cyber Warfare*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2009.

[33] C. Koch and K. Hepp. "The relation between quantum mechanics and higher brain functions: Lessons from quantum computation and neurobiology." California Institute of Technology, Pasadena, CA, Apr. 2007.

[34] R. Kurzweil. *The Singularity is Near: When Humans Transcend Biology*. New York, NY: Viking, 2005.

[35] P. Teilhard de Chardin. *The Phenomenon of Man*. English translation by Bernard Wall, New York, NY: Harper Brothers Publishers, 1959, pp. 18, 182.