Journal of International and Global Studies

Volume 6 | Number 2 Article 4

4-1-2015

Keeping Pace with Cyber Power, Defense, and Warfare

Michael Olender
Carleton University, michaelolender@gmail.com

Recommended Citation
Olender, Michael (2015) "Keeping Pace with Cyber Power, Defense, and Warfare," *Journal of International and Global Studies*: Vol. 6: No. 2, Article 4.
DOI: 10.62608/2158-0669.1241
Available at: https://digitalcommons.lindenwood.edu/jigs/vol6/iss2/4

Keeping Pace with Cyber Power, Defense, and Warfare

Review Essay by Michael Olender, Norman Paterson School of International Affairs, Carleton University, Ottawa, Canada, michaelolender@gmail.com

Joseph S. Nye, Jr., *The Future of Power*. New York: PublicAffairs, 2011.

Daniel Ventre (ed.), *Cyber Conflict: Competing National Perspectives*. Hoboken: John Wiley & Sons, 2012.

Paulo Shakarian, Jana Shakarian, and Andrew Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Amsterdam and Boston: Syngress, 2013.

Cyber power continues to take shape in accordance with world events. Three recently published books have taken different approaches to the subject of what may be broadly termed "cyber operations." The context for these operations is strictly the 21st century, and the evolving notion of power involves the diffusion of power among countries and non-state actors. Questions abound about the contours and limitations of cyber power, but what is clear across these books is that the cyber domain is indeed the next power frontier, within which both vulnerabilities and opportunities are created.

Cyber power

In *The Future of Power*, Joseph Nye looks at dimensions of power—itself a contested concept that he says often reflects interests and values—and how power evolves. Nye (2011, pp. 5-7) defines power thusly: "For my interest in actions and policies . . . power is the capacity to do things and in social situations to affect others to get the outcomes we want . . . . A policy-oriented concept of power depends upon a specified context to tell us *who* gets *what*, *how*, *where*, and *when*." First, he outlines types of power, covering the various aspects of power in world politics—such as the three faces of relational power, which are commanding change, controlling agendas, and shaping preferences—then moves on to discuss military power, economic power, and soft power. He then identifies two power shifts occurring in this century, one being power diffusion related to the evolution of cyber power, the other being power transition based on the question of American decline. He concludes the book with a policy-oriented elaboration of "smart power," a mix of hard and soft power strategies. Many of Nye's arguments and evidence hardly need to be repeated, as they are part of a synthesis of decades' worth of scholarship in the field of international relations, but it should be mentioned that he shows a deft hand with his writing on conceptual innovations in power.

Nye's contribution to existing scholarship lies in his analysis of power diffusion with respect to the cyber domain. While power transition from one hegemonic state to another is a process that has been repeated throughout history, power diffusion is more novel, writes Nye. He should be commended for deciphering the cyber domain as a new power frontier with analytical precision and linking it to the phenomenon of power diffusion. The "Information Revolution," with advancements in communication through the Internet and reductions in the costs of computing and communication, is the enabling factor that brings down barriers to entry into world politics. With lower barriers to entry, non-state actors "are empowered to play direct roles

in world politics," with some aspects of the Information Revolution helping small states and non-state actors, while others help large, already powerful states (Nye, 2011, pp. 116-117). Avoiding oversimplification, he provides an overview of new opportunities and diffusion trends in transnational activity involving non-state actors such as multinational corporations and terrorist groups, specifying: "The real issue related to the diffusion of power is not the continued existence of the state, but how it functions" (Nye, 2011, p. 119). Understanding cyber space as a relatively new operational domain premised on interconnected electronic systems and associated infrastructure, Nye (2011, p. 123) writes:

> Cyberpower can be defined in terms of a set of resources that relate to the creation, control, and communication of electronic and computer-based information—infrastructure, networks, software, human skills . . . . Defined behaviorally, cyberpower is the ability to obtain preferred outcomes through the use of the electronically interconnected information resources of the cyberdomain. Cyberpower can be used to produce preferred outcomes *within* cyberspace, or it can use cyberinstruments to produce preferred outcomes in other domains *outside* cyberspace.

Further, noting that small states and non-state actors can play significant roles in world politics at low levels of cost, Nye maintains that large, already powerful states, such as the United States, Russia, Britain, France, and China, do not enjoy dominance in the cyber domain. Rather, their dependence on interconnected electronic systems for military and economic activities creates vulnerabilities that can be exploited. His extensive discussions about information and physical instruments that can act as hard and soft power resources—with hard power including the use of malicious code to steal intellectual property or disrupt electronically controlled industrial systems and soft power including the utilization of software to help human rights activists—along with his discussion of the relational power resources of actors in the cyber domain can be instructive in mapping power relations and vulnerabilities among actors. Regarding major cyber threats to national security, he highlights economic espionage and crime, which currently have the highest costs, and cyber war and cyber terrorism, with states having offensive capabilities that are stronger than defensive capabilities and with terrorist groups ranking near the bottom of the capabilities hierarchy. Normative differences largely preclude reaching multilateral agreements on issues related to the cyber domain, with Nye (2011, p. 150) offering the example: "From the American point of view, Twitter and YouTube are matters of personal freedom; seen from Beijing or Tehran, they are instruments of attack." Hence, self-help is the dominant governance norm, and policies on international deterrence as well as network and infrastructure resilience are the dominant management strategies.

Nye's inquiry into power diffusion and the new implications of cyber power should inspire reflection, especially regarding limitations. Diffusion evidently does not imply the equality of power among traditional and new actors in world politics. His assessment of how technological change is reshaping international relations is thought-provoking, but the chapter is arguably relatively light on evidence. Other shortcomings also slightly weaken Nye's text. Only being able to discuss rather recent events notwithstanding, Nye too often assumes knowledge about cyber issues on the part of his readers. For instance, he makes passing mention to "hacktivism" and provides the example that "Taiwanese and Chinese hackers regularly deface each other's Websites with electronic graffiti" (Nye, 2011, p. 126). Later, on the issue of governments remaining the most powerful actors in world politics, he writes, "Even the small United Arab Emirates was able to force the maker of the BlackBerry to compromise," without

giving details about the compromise between the monarchy and BlackBerry creator Research in Motion, a Canadian company (Nye, 2011, p. 150). He provides only a single case study, one on the interactions between Google, an American company, and the government of China related to alleged efforts by the government to steal the company's source code and enter the email accounts of Chinese activists, to illustrate how companies, governments, and individual hackers use various instruments to generate their preferred outcomes within and outside the cyber domain. Moreover, his American-centric perspective makes the scope of cyber power discernible but its scale difficult to estimate. Nye's final chapter on smart power is largely an articulation of how the United States can manage political decline and boost economic prosperity by being open to alignment with other countries rather than seeking primacy within the international system. Problematically, however, such a strategy may be able to stem power transition but not power diffusion. With the onus of its message on the future, the book's value, then, is its systematic conceptual elaboration of how cyber power is increasingly undergirding international interactions among a vast number of traditional and new actors, with the consequence being the reduction in relative power differentials among these actors.

Cyber defense

Daniel Ventre's edited volume *Cyber Conflict: Competing National Perspectives* goes beyond the American experience to look at the perspectives of Canada, Cuba, France, Greece, Italy, Japan, Singapore, Slovenia, and South Africa on developing cyber strategies and managing cyber operations. It takes a high-level policy view and mainly focuses on cyber security and defense. Twelve authors, including Ventre, offer much insight into national interpretations of the concepts of cyber threats, conflict, attacks, and warfare. National doctrinal frameworks and the connections between the civilian and military dimensions of cyber operations are critical for understanding cyber warfare in particular, since "the reality is that national doctrines of information operations and cyber-warfare are as varied as human fingerprints. Countries . . . carry their particular historical experiences and strategic concerns with them. These are instrumental in shaping national cyber-warfare doctrines with distinct features, reflecting the geopolitical identity of each nation" (Fitsanakis, qtd. in Ventre, 2012, sec. 4). Across the volume's studies, the sometimes surprising degree of countries' shared dependence on the cyber domain and the variety of instruments they use to manage the negative effects of that dependence, such as policies, laws, standards, and the creation of agencies, make for a compelling read.

Studies come to varied conclusions based on policy documents and historical events. In Canada, the development of cyber-security policies has accelerated in this century, with the major concern being the protection of critical infrastructure. In Cuba, the regime in power perceives cyber space to be a threat to its stability, so the flow of information is strictly controlled to stem foreign interference or influence. France structures its defense in relation to economic crises and the new international balance related to the recent revolutions in North Africa. Italy has established agencies and policies to combat cyber crime and protect intellectual property rights, but its cyber-security strategy is at a nascent stage. In Japan, a new strategy has been put forward that includes the use of cyber space in defense policy and military doctrine, a shift for a country with a unique defense arrangement following the Secord World War. Singapore's approach is twofold, with a cyber-security authority collaborating with the private sector to defend the island's highly globalized economy against the high incidence of cyber

attacks on corporations, as well as the military expanding cyber capabilities to enhance conventional capabilities. Given an already high general sense of security, Slovenia sees the costs of investment in cyber security difficult to justify and is thus largely unprepared for cyber attacks. South Africa has the most advanced communication infrastructure in Africa and is in the process of developing cyber-security policies since there is potential for the exploitation of vulnerabilities in a cyber-warfare scenario on the continent.

An outstanding study is Joseph Fitsanakis's chapter on Greece. Despite its relatively small size and weak economy, Greece's geopolitical position at the crux of Europe and the Middle East means that spillover effects from cyber threats or attacks within the country "could massively impact on international shipping patterns, energy transportation networks, global banking, [North Atlantic Treaty Organization] NATO military and communications assets, and regional telecommunications systems" (Fitsanakis, qtd. in Ventre, 2012, sec. 4.1). A major part of the country's doctrinal framework is informed by power politics with Turkey—an age-old ethnic, religious, and geostrategic rival—characterized by internal balancing based on technological superiority. Events such as the 1974 invasion of Cyprus by Turkey and the Ergenekon affair—revealed in 2007, involving Turkish military and intelligence officers devising propaganda to destabilize Greece for the benefit of Turkish national interests—are considered to be formative experiences that catalyzed Greece's drive to maintain defensive technological superiority. Despite the ongoing European sovereign debt crisis that began in 2009, Greece maintains the highest proportional defense spending in NATO, and asymmetrical balancing may be enabling capabilities beyond communication systems: "In the particular context of Greek–Turkish strategic relations, the anticipatory (preventive or pre-emptive) aspects of information operations are in agreement with broader efforts by Greek military planners to steer the country's military thinking toward offense-oriented strategic concepts" (Fitsanakis, qtd. in Ventre, 2012, sec. 4.8). Notably, Greece's Ministry of National Defense announced the formation of a new National Cyberdefense Authority in 2011 to protect the country against cyber attacks following new organizational standards set by NATO, of which both Greece and Turkey are members. The case of Greece is exemplary, as it demonstrates why and how a country can become an innovator in cyber defense given economic problems, regional context, and alliance arrangements.

The edited volume contains exceptional scholarship that underscores the relevance of the cyber domain to all types of countries. Constraining international contexts based on alliances and obligations often affect the development of national cyber strategies, which in turn determine capabilities and power resources. Hence, various contexts, especially military and economic contexts, must be taken into account in estimates of the scale of cyber power. Distinct historical experiences and strategic concerns are paramount in the cyber domain, which is evidently an extension of other domains rather than something completely novel. A fine contribution is Ventre's concretization of a visualization of cyber space, which he defines as a "fifth dimension" of general human activity, consisting of three layers—from bottom to the top, the physical, material, hardware, infrastructure, networks layer, the application layer, and the cognitive layer—and intersecting with the four conventional dimensions, land, sea, air, and space. Ventre (2012, sec. 10.1) outlines the association of each layer with relevant actors, actions, and theoretical considerations, affirming that the definition of cyber space "expresses the transversality of cyberspace with the real dimension" and is useful in reconsidering perceptions of incidents, actions, and stakes as well as representations of threats. His visualization of cyber space as a matrix could have wide analytical applications since it improves upon oversimplified

definitions. The only oversight in this volume is the choice to forgo a discussion on the overall strategic purposes of cyber power in favor of a short, arguably underdeveloped conclusion about cyber operations as an evolution in policy, rather than a revolution, given regional contexts and geopolitical strengths. Technological, tactical, and operational aspects are discussed throughout, but the strategic purposes of cyber power for the ends of policy during both peace and war are assumed to be (perhaps necessarily) context-specific.

Cyber warfare

Introduction to Cyber-Warfare: A Multidisciplinary Approach by Paulo Shakarian, Jana Shakarian, and Andrew Ruef comprises a series of comprehensive case studies that present in detail the scope of cyber warfare, specifically how cyber warfare is used to achieve political objectives, cyber espionage and exploitation, and cyber attacks on various kinds of physical infrastructure. The authors focus on the strategic purposes of cyber power in consideration of the fact that the origins of cyber attacks can be obscured. Notably, they offer middle-range theoretical perspectives—integrating theory with empirical research by identifying an empirical phenomenon that appears to explain correlations, abstracting from it, then verifying it with data, or at least deriving research questions. This approach proves to be quite fruitful for an area of research that changes rapidly.

Political cyber attacks first garnered major international attention in 2007 when Estonia endured distributed denial of service attacks following the movement of a Second World War–era monument to Soviet soldiers, which incited a Russian pro-Kremlin youth group to target the Estonian Parliament's email servers. Cyber attacks then augmented Russia's military campaign against Georgia in 2008 by silencing the media and effectively isolating the country from the international community. The cyber domain was also used to publicize different narratives during the Israel-Hezbollah "July War" of 2006 and has been manipulated to limit the free speech of domestic dissidents in Russia and Iran over time. An extended chapter on cyber attacks by Anonymous and its affiliates adds an additional perspective on the ideologies, capabilities, and (largely benign though symbolic) efforts of non-state hacking groups, which tend to act against abuses of power by governments, corporations, and individuals related to the freedom of information and right to online privacy. Regarding cyber espionage and exploitation, case studies on Chinese cyber espionage against militaries, dissidents, and corporations, malware such as Duqu, Flame, and Gauss, and the hacking of drone feeds by Iraqi insurgents illuminate the computer science aspects of cyber operations that allow political objectives to be achieved. A look at the references for these chapters indicates the types of sources—publications by computer security firms, for example—that need to be surveyed to gain a better understanding of cyber operations. With regard to cyber attacks on infrastructure, which include those on industrial control systems, power grids, and Iran's nuclear facilities, palpable are the advancements in computer science that broaden the potential targets for political attacks. Cyber operations became a widely credible threat in 2010 when the Stuxnet worm was discovered at Iranian nuclear facilities, an event that galvanized international discourse on the subject of cyber power. Stuxnet, which destroyed centrifuges and set back Iran's nuclear program, is considered representative of a "revolution of military affairs" since the software invalidated several security assumptions, such as the presumed benefits of computer systems isolated from the Internet (Shakarian, Shakarian, & Ruef, 2013, p. 233).

Middle-range theorizing throughout the book is innovative since it breaks the confines of international relations theories such as realism and liberalism to tap into the insights of people closest to relevant events, abstract from these insights, then apply them to other events over time. For instance, Shakarian, Shakarian, and Ruef (2013, p. 120), preceding their discussion on China's cyber strategy being an integral component of its international relations, outline the thinking behind Chinese cyber doctrine:

> Another line of thought in Chinese writing to justify their seemingly bold moves in cyber space is that they believe these activities can be done with relative impunity. In a 2009 article in *China Military Science*, Senior Colonel Long Fangcheng and Senior Colonel Li Decai state that cyber operations directed against social, economic, and political targets can be done without fear of such activities leading to large-scale military engagements. As such is the case, they generally regard cyber warfare as an element of soft power—albeit one with great effects. They then proceed to claim that the ultimate effect of this highly effective form of soft power is that the line between peacetime and wartime becomes blurred. This blurring may be a hallmark of cyber operations in general and might lead to the metaphorical endless war in the near future.

By using qualitative methodologies, highlighting contextual factors and caveats, and avoiding causal hypotheses, middle-range theoretical approaches appear to boost explanatory power. The book, however, is missing a comparative investigation of middle-range theoretical perspectives, with most theories applying only to a certain national context and assuming a unified state by not considering intervening variables, such as public opinion and political opposition. Comparative investigation is certainly an avenue for future study in this area of research. A comparison of the cyber doctrine of China to those of the United States and Russia would be fascinating.

Sometimes the authors seem to overestimate what counts as an *effective* attack with their use of language—freely using the word "assault" for distributed denial of service attacks, for example—and, overall, references suggest that many cyber attacks are not garnering the attention of distinguished scholars. Given difficulties with data availability and the rapid pace of developments in the area of research, the authors use open sources, including conference papers and media reports, an approach that may sometimes be necessary and thus should be noted by both scholars and policy-makers going forward. Nonetheless, the book strikes an important balance on the issue of information dissemination, with the capabilities to provide or block information, which have bearing on the world's attention and action, being perhaps the most salient strategic purposes of cyber power. The problem of the attribution of attacks is well covered, with interesting political perspectives on combatants and observers in Israel and Gaza supporting war efforts by uploading digital images to Twitter and YouTube from mobile phones, Russia appearing to be in a constant state of cyber civil war, and Iran's formal Iranian Cyber Army as an offensive asset and its Cyber Police as a defensive one. Overall, the book's scope, which is enabled by a multidisciplinary approach, is its primary value, and its depth and detail make it more than an introductory text.

Cyber surveillance?

The overarching theme across these three vital books is emergence, and each of the three texts' distinct angles either fill each other's gaps or provide correctives. Still, there is a pervasive sense of catching up to speed, with authors (some of whom admit that they are learning as they

go along) highlighting policy-makers' quotes about the need for comprehensive strategies going forward. The multidisciplinary approach employed in these works greatly helps delineate conceptualizations of cyber power and implications for policies on cyber defense and warfare. To further strengthen the relevance of this area of research (and to speak to the larger field of international relations), it would be advisable for scholars to engage in a feedback loop and continuously comment on what cyber power, defense, and warfare are and what they can be. Former National Security Agency contractor Edward Snowden's leaks beginning in June 2013 about American global surveillance programs have provided a glimpse into the ever-broadening scope of cyber power. These leaks necessitate further study that moves beyond cyber attacks, information assurance, and political and legal accountability to contemplate the politics and power implications of cyber surveillance. Is cyber surveillance a strategy to stem power diffusion? How do the realities of cyber surveillance change the way that the state functions? And what does cyber surveillance mean for the cyber power of non-state actors? What seems niche now appears to be impacting the nature of power around the world, and scholarship must keep pace.