The US Army War College Quarterly: Parameters

Volume 43
Number 3 *Parameters Autumn 2013*

Article 11

Fall 9-1-2013

Cyberwar to Wikiwar: Battles for Cyberspace

Paul Rexton Kan

Cyberwar to Wikiwar: Battles for Cyberspace

Paul Rexton Kan

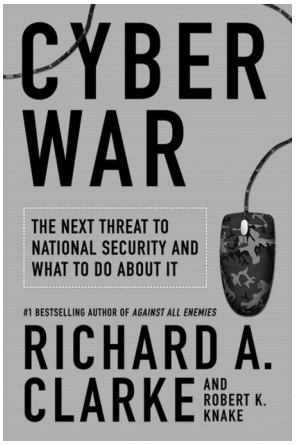
Abstract: National leaders warn of a cyberwar and cyberterrorism that may lead to a potential "cyber Pearl Harbor." To prevent such an occurrence requires cyber defense or even some sort of cyber deterrence. Some policymakers even want cyber arms control. However, these concepts are a retrofitting of those used in the physical domain to describe violent acts and responses to them. Do these concepts help policymakers, national security professionals, and scholars understand aggressive acts perpetrated in cyberspace?

A few days after the bombings at the Boston Marathon in April 2013, the Associated Press (AP) reported via Twitter, "Breaking: Two Explosions in the White House and Barack Obama is injured." The Dow Jones Industrial lost nearly 150 points; $136 billion of equity was suddenly gone. The AP's Twitter account, whose feed had been integrated into the reporting algorithms of the New York Stock Exchange a few days prior, was hacked by a group calling itself the Syrian Electronic Army, allowing it to tweet the fake message. Fortunately, the loss in national wealth was short-lived as stocks recovered their value within three minutes.

How do we place a context around what happened within those three minutes? Was this a salvo in a cyberwar initiated by the Syrian regime or a prank by an unaffiliated group for "lulz" (a corruption of "lol," "laugh out loud")? There was no permanent loss of capital and aside from the perpetrators, few would have actually laughed out loud. But there is still a sense of seriousness about this episode that reveals the genuine limits of our understanding of the cyber domain in the national security arena. Given the newness of the digital domain, its man-made origins, and its constantly changing nature due to manipulation by human beings, it should not be surprising that national security professionals reach for comfortable and familiar approaches. "Cyberattacks" are a daily, or more accurately a nanosecond-after-nanosecond, occurrence that requires "cyber security." National leaders warn of a "cyberwar" and "cyberterrorism" that may lead to a potential "cyber Pearl Harbor." To prevent such an occurrence requires "cyberdefense" or even some sort of "cyberdeterrence." Some policymakers want "cyber arms control" to limit what types of cyberattacks can be perpetrated against another country. These concepts are a retrofitting of those used in the physical domain to describe violent acts and responses to them. Do these concepts help policymakers, national security professionals, and scholars understand aggressive acts committed in cyberspace?

Richard Clarke in his book, *Cyber War: The Next Threat to National Security and What to Do About It*, believes these concepts are not only relevant, but also consistently overlooked by policymakers. For Clarke, a cyberwar refers "to actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption" (6). In his first chapter, he details "trial runs" which are incidents

Paul Rexton Kan is Professor of National Security Studies and the Henry L. Stimson Chair of Military Studies at the US Army War College. He is the author of the books *Drugs and Contemporary Warfare* and *Cartels at War: Understanding Mexico's Drug-Fueled Violence and the Threat to US National Security*. His recent article, "Cyberwar in the Underworld" appeared in the *Yale Journal of International Affairs*.



New York: HarperCollins, 2010. 320 pages. $17.58.

of cyberwar perpetrated most notably by the Russians, North Koreans, and Israelis. These episodes are now well-known—the Israeli "owning" of Syria's air defense system in 2007; the suspected Russian distributed denial of service (DDOS) attacks against Estonia in 2007 and the more sophisticated cyberattacks against Georgia in 2008; and the North Korean botnet attack against US websites in 2009. From these episodes, he derives four maxims: cyberwar is real; cyberwar happens at the speed of light; cyberwar is global; and cyberwar has begun. These maxims form the core of his book as he presents more accounts of the "cyberwarriors" in the "battlespace" and how the United States should prepare, defend, and retaliate.

Clarke spends the majority of his time reemphasizing these maxims throughout the book with brief examples. Clarke appears to be most worried about China, which he argues is "systematically doing all the things a nation would do if it contemplated having an offensive cyber war capability and also thought that it might itself be targeted by cyber war" (54). Clarke's chief concern is that the United States is lagging far behind countries like China. "Indeed, because of its greater dependence on cyber-controlled systems and its inability thus far to create national cyber defenses, the United States is currently far more vulnerable to cyber war than Russia or China. The US is more at risk from cyber war than are minor states like North Korea" (155).

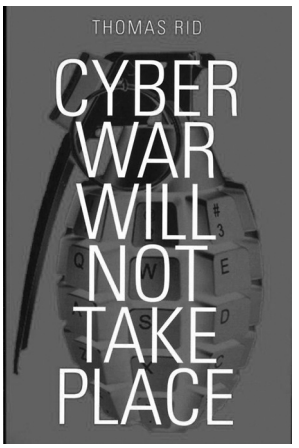
Given the seriousness of Clarke's assessment and the examples of grave consequences of previous cyberattacks, his book deserves particular scrutiny. The narrowness of Clarke's definition of what constitutes a cyberwar is problematic. Do the myriad events he details really constitute "war"? Causing damage or disruption is a rather large range of consequences—from defacing a website to crippling a power grid. In the physical world, one act could be interpreted as vandalism and the other may be viewed as malicious destruction of property. Without a coercive intent to achieve a political goal, would the range of attacks—cyber or otherwise—be considered an act of war?

This is where Thomas Rid's, *Cyber War Will Not Take Place*, is especially useful in clearing up much conceptual fuzziness surrounding cyberwar. In contrast to Clarke's book, Rid's is a more scholarly work. Rid, a reader at King's College in London, makes the argument that all the disruptive acts perpetrated via cyberspace do not constitute war or warfare, nor are they even particularly violent. "No cyber offense has ever caused the loss of human life. No cyber offense has ever injured a person. No cyber offense has ever seriously damaged a building" (166). Taking Clausewitz's theory of war, Rid argues "if the use of force in war is violent, instrumental and political, then there is no cyber offense that meets all three criteria. But more than that, there are very few cyber attacks in history that meet only *one* of these criteria" (4, emphasis in the original). For Rid, the events via cyberspace recounted by numerous

national security professionals such as Clarke fall into one or more categories of espionage, sabotage, or subversion. "Despite the trends the 'war' in 'cyber war' ultimately has more in common with the war on obesity than the Second World War—it has more metaphorical than descriptive value" (9).

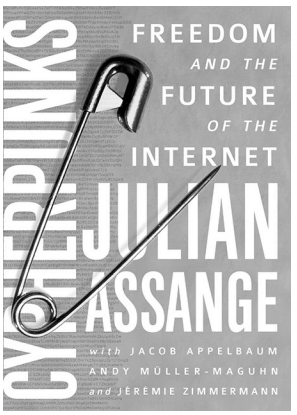
Rid's point about being careful with metaphors and concepts in a new domain is well taken. The goal of his book is "to attempt to help consolidate the discussion, attenuate some of the hype and adequately confront some of the most urgent security challenges" (ix). Much thought has been brought to bear on the mechanics of nefarious acts in cyberspace, but comparatively little time has been spent on putting the acts into context. Understanding the motivations of groups and individuals who act in cyberspace is essential. Rid's main argument and his subsequent chapters on "Violence," "Sabotage," "Espionage," and "Subversion" are powerful tonics to some of the more alarmist literature on cyberwar. His conclusion is as interesting as it is provocative—cyberattacks are an attack on violence itself. Because activities like sabotage, espionage, and subversion can now be accomplished in cyberspace, fewer personnel are needed to conduct such activities in the physical world. Where at one time special forces would have been sent to destroy a facility, spies would have been dispatched to steal secrets and mobs organized to protest government policies, cyberattacks can now accomplish these goals simply and clandestinely. This conclusion, however, needs to be treated with great caution. It is vaguely reminiscent of early airpower theorists who predicted that the airplane would make wars less violent by shortening their duration. Secondly, while cyberattacks may only indirectly create destruction or disruption in a targeted nation, there may be direct costs to pay in the physical world. Digital acts may be met with kinetic reprisals. Sabotage, espionage, and subversion may not fit into the definition of war, but they have served as *casus belli* for the outbreak of wars in the past.

Where Rid is helpful in clearing up the parameters of the discussion over cyberwar by focusing on stricter definitions, clearer concepts, and more apt metaphors, he does not delve deeply enough into cyberattacks perpetrated by nonstate groups. Rid's chapter on "Subversion" only lightly touches on the topic of nonstate groups who use the digital domain to change the behavior of states. These groups should not be overlooked because another question surrounding the fake AP tweet that sent the stock market plunging is who exactly is the Syrian Electronic Army? Is it a group of a state-sponsored "patriotic hackers," an unaffiliated association, a loose assemblage of individuals sympathetic to the regime of Bashar Assad, or some combination of each? With the anonymity that cyberspace affords, both Clarke and Rid agree that the problem of attribution is difficult. If the Syrian Electronic Army is an unaffiliated collective of some kind, the cyberwar



London: C. Hurst & Company Publishers, 2013. 256 pages. $27.95.

debate fails to capture the significance of its activities. Cyberwar between countries does not occupy all the space in the debate, much like interstate war does not cover all aspects of war. Dispersed groups of hacktivists engage in many of the same damaging cyber activities as nation-states. This demonstrates a uniqueness of the cyber domain. Due to the ease of entry into cyberspace, hacktivists have committed the same online acts like defacing websites, stealing proprietary information, DDOS attacks, and launching botnets that are in the repertoire of cyberattacks conducted by countries. As a result, hacktivists have much the same power in cyberspace as the infamous Chinese hackers of the People's Liberation Army. But unlike countries that launch cyberattacks for political reasons linked to foreign policy, hacktivists use the Internet to advance political and social goals that center around the Internet itself.



New York: OR Books, 2012. 186 pages. $9.99.

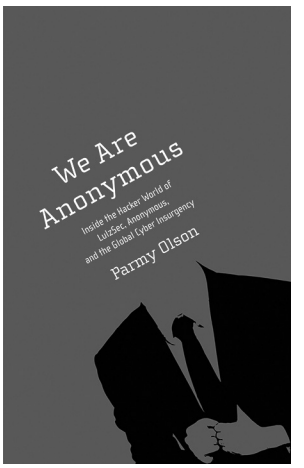
Groups like Anonymous and WikiLeaks see themselves as combatants in a war to achieve the goal of Internet freedom. For them, human liberation begins with the liberation of information. In Julian Assange's book, *Cypherpunks: Freedom and the Future of Internet*, this belief comes into sharp focus. The book takes its name from the cypherpunks movement that emerged in the late 1980s; it believed in the widespread use and availability of cryptography to protect and foster human liberty against intrusive state surveillance. The book is a compilation of discussions of fellow believers in the cypherpunks' slogan of "privacy for the weak, transparency for the powerful." The discussions occurred with Assange, the founder of WikiLeaks, while he was under house arrest in the United Kingdom awaiting extradition to Sweden, but before he sought asylum at the Ecuadorean Embassy in London where he continues to reside. The conversations reveal how the group sees itself as engaged in a violent struggle against what it views as the "coming surveillance dystopia" organized by countries and powerful corporations. They argue they and their fellow believers have "had conflicts with nearly every powerful state. . . . We know it from a combatant's perspective, because we have had to protect our people, our finances and our sources from [them]."

But it is not only countries that are the subject of the discussions. Google is the subject of the chapter, "Private Sector Spying." There is a typical but thought-provoking exchange between two group members:

> Jeremie: State-sponsored surveillance is indeed a major issue which challenges the very structure of all democracies and the way they function, but there is also private surveillance and potentially private mass collection of data. Just look at Google. If you're a standard Google user Google knows who you're communicating with, who you know, what you're researching, potentially your sexual orientation, and your religious and philosophical beliefs.
>
> Andy: It knows more about you than you know yourself.

> Jeremie: More than your mother and maybe more than yourself. Google knows when you're online and when you're not.
>
> Andy: Do you know what you looked for two years, three days and four hours ago? You don't know; Google knows.

The rhetoric of the conversations can be overly dramatic; labels like "Nazi youth camp" and "Stasi acts" are bandied about without care. The chapter on "The Militarization of Cyberspace" begins with Assange arguing that all communications linked to the Internet are monitored by military intelligence organizations. "It's like having a tank in your bedroom. It's a soldier between you and your wife as you're [texting]. We are all living under martial law as far as our communications are concerned; we just can't see the tanks" (33). For many, the group's constant use of metaphors, analogies, and rhetoric of war will be off-putting. However, it is important to wade through and come to grips with the implications of their arguments rather than get bogged down in their use (or abuse) of language. Most problematic is its ideology of Internet freedom. An ideology centered around the free use of technology becomes ironic, especially in the case of the Syrian Electronic Army. It is unclear whether the group of cypherpunks would approve of another hacktivist group's online activities done in the name of a tyrannical regime in Damascus, a regime that has used an Internet "kill switch" to stop Internet traffic out of it borders. Yet, if the Internet were entirely "liberated," the activities of the Syrian Electronic Army would be permitted if perpetrated against a surveillance state like the United States. In short, not all hacktivism serves human liberation; it can cut both ways. To paraphrase one technology observer, Farhad Manjoo, the Internet is just a series of tubes without ideology.



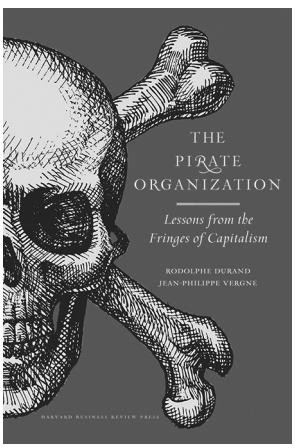
New York: Back Bay Books, 2012. 528 pages. $16.00.

While *Cypherpunks* lays out the ideology as espoused by a core group of hacktivists, Parmy Olson's book, *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous and the Global Cyber Insurgency,* is a richly detailed, journalistic account of the history and acts of a cyber group that pushes this ideology forward with its cyberattacks. Unlike the inner circle of WikiLeaks, Olson's book chronicles the rise of a hacktivist collective that is now more like a social cyber movement. One of the most important observations by Olson is the misconception that Anonymous is a "small clique of super hackers." In fact, only a few in the collective were hackers and the rest were "simply young internet users who felt like doing something other than wasting time [in anonymous chat forums]" (81). The rallying cry for Anonymous mirrored that of the cypherpunks, "information wants to be free."

If Russian attacks against Estonia and Georgia are the *sine qua non* of cyber war in the interstate realm, the attacks by Anonymous against the Church of Scientology, PayPal, and Sony are the *sine qua non* of hacktivism in the hacking world. Olson details how Anonymous gained

notoriety for its 2008 operations against the Church of Scientology. In that year, the church pressured YouTube to remove a leaked video of church member and actor Tom Cruise. Such pressure exerted by the Church of Scientology ran counter to the Anonymous ethos of transparency. In response, Anonymous launched an operation to bring down the church's website that combined DDOS attacks with pranks such as phone calls with repetitive music, constant faxing of black paper to drain printer cartridges, and ordering unwanted pizza deliveries and taxi service. The group has found common cause not only with WikiLeaks founder Julian Assange, but the Occupy movements, and accused leaker Bradley Manning. Olson also covers the numerous Anonymous' operations aimed at agencies and institutions such as PayPal, Mastercard, and Visa, which refused to process payments for websites that were raising funds for the legal defense of Assange, Manning, and those associated with Occupy movements.

Particularly revealing in Olson's book is the notion that the ethos of the group is also how the group is structured. Information on the Internet is dispersed and decentralized, as is Anonymous. Marshall McLuhan proclaimed the "medium is the message"; for hacktivists the medium is the ethos. The structure of the collective is also a reflection of its ethos. As a loosely affiliated group of online social activists, Anonymous takes pride in being unstructured without a hierarchy or central authority. This nebulous structure has strategic advantages, but operationally, as Olson covers in her chapter "Civil War," these characteristics have proven troublesome. Due to Anonymous's loose structure, any operation can move forward or be cancelled in a capricious manner. Furthermore, as a collective, members can do more than just dissent against a planned operation and opt out; they can actively work against the operation by launching counterattacks against factions with whom they disagree. They can also prevent members from accessing online fora, where many members find each other. Internal schisms have occurred among Anonymous members who wanted to undertake operations in accordance with the hacker ethos, others who wanted to take on morals-motivated attacks against organizations that suppress human freedom in the physical world, and yet others who were purely interested in hacking for "spite and fun."



Boston: Harvard Business School Publishing Corporation, 2013. 208 pages. $22.00..

Finally, unlike a book written for a popular audience, an academic work, a collection of discussions and a journalistic investigation, *The Pirate Organization: Lessons from the Fringes of Capitalism* is an essay written by Rodolphe Durand and Jean-Philippe Verne. Although the authors do not focus exclusively on the cyber domain, they do discuss the historical struggle between sovereign actors and those who seek and exploit ungoverned areas. For them, a pirate organization,

> regardless of time, share the following features: they enter into a conflictive 'relationship' with the state, especially when the state claims to be the sole source or sovereignty; they operate in an organized manner, from a set of support bases located outside this territory, over which

> the state typically claims sovereign control; they develop, as alternative communities, a series of discordant norms that, according to them, should be used to regulate uncharted territory; and ultimately, they represent a threat to the state because they upset the very ideas of sovereignty and territory by contesting the state's control and the activities of the legal entities that operated under its jurisdiction, such as for-profit corporations and monopolies. (15)

Given this definition, WikiLeaks and Anonymous fit easily inside the parameters of a pirate organization. In fact, the authors make it clear that concentrating solely on contemporary maritime piracy is misplaced. "Blackbeard, for example, has far more in common with a cyberpirate than with a Somalian peasant who uses a Kalashnikov to attack a fishing boat from a makeshift craft" (15). The authors insightfully and succinctly go through the history of pirate organizations—the 17th and 18th century buccaneers, radio DJs at sea, cyberpirates on the Web, and biopirates in the lab . According to the authors, pirate organizations emerge because a new, ungoverned territory is ripe for exploitation. As seen in the four previously reviewed books, cyberspace is the ultimate ungoverned territory. Hacktivists, as understood through the definition of a pirate organization, are in some ways more central players in the cyber domain than nation-states.

Groups like Anonymous and WikiLeaks clearly represent one side of the tension between sovereignty and stateless actors. Also, the way the authors set up the tension between such an organization and the state is a useful tonic for those like Clarke who see hacktivism as a "fairly mild form of online protest" (55). Those who set their sights on a cyberwar occurring between nation-states would do well to read this book to gain a broader perspective on what they are missing from the larger discussion of cyberwar.

There is plenty to quibble about when it comes to their definition of pirate organizations, and their glib dismissal of maritime piracy off the Horn of Africa is a pity; a deeper understanding would show that it is a more complex activity, which in fact supports their thesis. Contemporary maritime piracy takes advantage of regional and global networks of finance, insurance, and shipping that occur far from the acts of high seas hijacking. The network is dispersed, somewhat durable, and resilient to detection and elimination.

The five books portray the growing complexity of conceptualizing malicious online actions. Policymakers, national security professionals, and scholars often dismiss hacktivists or cyber pirates as collections of socially awkward malcontents who find a sense of belonging by creating mischief online. Instead, they focus on cyberwar conducted or supported by nation-states. Placing complicated changes in the security environment back into the nation-state box is easy, but to do so would be short-sighted. We have done this before not so long ago and to disastrous effect. Between the fall of the Berlin Wall and the fall of the World Trade Center, nonstate actors were ignored in favor of state-based challenges. Even today, after more than a decade of the War on Terror and wars in Iraq and Afghanistan, our grasp on topics like terrorism, insurgency, and asymmetric war is not completely firm.

Moreover, given the newness of the cyber domain and its rapidly changing nature, it would be a mistake to disregard any groups who

have as an ethos the desire to define cyberspace through online acts that challenge the fundamental elements of national security. This is especially so if some of those groups feel they are besieged by governments and routinely use the rhetoric of war—"this seemingly platonic realm of ideas and information flow, could there be a notion of coercive force? A force that could modify historical records, tap phones, separate people, transform complexity into rubble and erect walls, like an occupying army?" (3) Policymakers, national security professionals, and scholars have previously dismissed groups who believe they are acting in self-defense and who then strike out unexpectedly and in unanticipated ways only to our surprise and detriment.

What is present in varying degrees throughout the literature about cyberspace and cyberwar are the five distinct ongoing debates about this new domain and how to act within it. The debates include who sets the boundaries of cyberspace; how should online information be controlled; to whom should information be available; can hierarchies and networks of people coexist in cyberspace; and what is the difference between "war" and "crime" in cyberspace.[1] In the reviewed books, it is evident that each cyber attack or cyber assault not only adds to these debates but helps the cyber domain gain more definition. Paradoxically, the debates to define cyberspace are occurring via cyberspace.

The paradox will likely become ever more acute with the advancement of cyber technology and the increasingly intertwined nature of the internet with our daily lives. With the advent of the "wearable web" like Google Glass, the Apple Iwatch, and even the potential for spray-on wi-fi, this intertwined nature will become incarnate. We won't be in cyberspace; we will be cyberspace. Being prepared for this future makes these five books essential reading.

1 For a very solid exploration of the debate over what is "war," "crime," and "violence" in the cyber domain, please see the series of articles by John Stone, Gary McGraw, Dale Peterson, Timothy Junio, Adam Liff, and Thomas Rid in the "Cyber War Roundtable" of the *Journal of Strategic Studies 36, no. 1* (February 2013).