Don't Forget the Humans: Toward a 21st Century Offensive Cyber Strategy

Mr. Josh M. Cartin
U.S. Army War College, DDE Class of 2014
U.S. Department of State
4170 AIT Taipei Place
Dulles, VA 20189
+886-933-192-451
josh@desertdragon.com

Abstract

As military competitors and allies alike explore military applications of cyberspace of increasing scope and complexity, a debate rages in national security circles about cyber war: what might it look like, whether one is imminent, and whether such a phenomenon is even possible, have become topics of debate given characteristics that distinguish cyberspace from other warfighting domains. This paper proposes two types of offensive cyber operation, instrumental and strategic, and argues that strategic offensive cyber operations are a form of information warfare that aim primarily to act upon adversary perceptions, which are fundamental to warfare as viewed as a contest of wills. A close examination of recent cyber campaigns attributed to China yields a nuanced understanding of from whence cyber operations derive their strategic potential. Such an understanding will be critical if the United States is to leverage its current technological advantage and imagine offensive cyber operations to maintain the initiative against able adversaries whose own strategic traditions condition them for warfare that transcends the physical into the information domain.

Key Terms: Information Operations, Warfare, China, Technology, Deterrence, Deception

Introduction

Recent public allegations of Chinese government sponsorship of intrusions into U.S.-based government, military, and commercial information systems have prompted a flurry of commentary, diplomatic activity, Congressional hearings, and at least one Presidential Executive Order. (Obama, 2013) Discussion has settled on the realization that hostile actors have the capability and motivation to erode U.S. military and commercial advantages by exploiting American society's ubiquitous reliance on cyberspace. The conclusion is that all segments of society need to work together to reduce the vulnerabilities that make hostile exploitation possible. (Wallace, 2013) With few exceptions, commentary has focused on defense and resilience of information systems, necessary and worthy investments whether the malicious actors are hostile states, criminal networks, "hacktivists," or bored teenagers in a basement. The concept of offensive cyber operations has been absent from most public discussion, with the notable exception of presumed United States involvement in the 2009-10 Stuxnet worm attack on Iran's nuclear program. (Gross, 2011)

That the main perpetrator in recently revealed cyber attacks is China, the only perceptible potential spoiler of U.S. global dominance, has however revived a debate that has been simmering in national security circles for over a decade regarding the concept of "cyber war":

what it might look like, whether the United States is in one, and indeed whether such a phenomenon is theoretically possible. (Rid, 2012) Since then, just as human interaction with and in the cyber domain has spread around the world at an exponential rate, thinkers drawn from the security, legal, and social science fields have dampened early enthusiasm by pointing out inherent difficulties with bending cyberspace to military ends.

Much of this more arcane debate centers on definitions: what constitutes "offense" in military terms, and what kinds of offensive military operations, in legal terms, could be considered acts of war. However well intentioned, such arguments shift focus from the evident truth that militaries and their civilian counterparts are investing more and more in cyber capabilities as part of their offensive toolkits. In the case of the United States, Stuxnet remains the known *ne plus ultra*. More recent cases involving China, as will be seen below, are legion. North Korea, Iran and, more recently, Syria all provide further examples. (Denning, 2007) Given this increasing tempo of offensive cyber activity, there is a clear need to revisit how and why governments mount offensive cyber operations if indeed their strategic value is as limited as some analysts decree.

This work has two primary goals: to hew sharp definitions of offensive cyber operations that render a nuanced understanding of what characteristics might make them of strategic consequence; and then to use this understanding to assess whether or not the United States is or will be engaged in a cyber war with China. The paper is broken into the following sections: a brief review of core security scholarship on cyberspace; a proposed framework that separates offensive cyber operations into two types and three categories; a look at Stuxnet as a case study in cyber offense; and finally a detailed review of possible motivations behind China's offensive cyber campaign. This paper aims to demonstrate that a full and productive exploration of the potential of offensive cyber operations requires a clear understanding of strategic versus instrumental effect; definitions that reinforce rather than sever cyber operations' connection to other non-kinetic military disciplines such as information operations, military information and support operations ("MISO", formerly "psychological operations" in military parlance), and electronic warfare; and a concept of warfare that extends beyond perfunctory interpretations of Clausewitzian references to force and violence. The paper concludes that a return to a more flexible and ambitious vision for cyberspace will help the United States understand and compete against adversaries whose different philosophies of war facilitate pursuit of a broader spectrum of military cyber operations, as well as enable the United States to manipulate a domain in which it still enjoys a technological advantage.

Theories of cyber warfare

Since the advent of the digital age before the turn of the century, security scholars have grappled with how to place cyberspace and its forebears in the context of historical revolutions in military affairs and technologies. As during previous epochal shifts in opinion, scholars have questioned whether the way war is conducted will fundamentally change in the information age. Writing in 1993 for RAND (long before popular access to the Internet, email, and mobile technologies became globally pervasive), security scholars John Arquilla and David Ronfeldt posited that the "information revolution" and adoption of new technologies not only would in time change the way war is conducted but also alter societies' calculations of whether and when to go to war. (Arquilla et al., 1993) Using the terms "Netwar" and "Cyberwar", the authors differentiated between technology-enabled offensive operations at the grand strategic level that

target an adversary's ability to access, communicate, and interpret information, and use of digital technology at the operational and tactical levels to improve or disrupt battlefield information and its enabling systems. In both cases, the authors highlighted a nexus with psychological dimensions of warfare, and by implication, traditional information operations. Reinforcement of the linkage between the digital revolution and information operations is a theme Arquilla returns to in the introductory chapter of a book he co-edited in 2007. (Arquilla et al., 2007)

The current century's first decade saw several attempts by state and nonstate actors to apply concepts Arquilla and Ronfeldt predicted over a decade earlier. Cyber attacks directed at the United States (2003), Estonia (2007), Georgia (2008), and Iran (2009-10), all widely believed to have enjoyed sponsorship by different states, provided "real world" examples from which security scholars could begin to analyze the causes, effects, possibilities, and limitations of operations in the cyberspace domain. (Rid, 2012) In multiple works over the past two decades, Martin Libicki, also from RAND, has come closest to developing a comprehensive theoretical framework for delimiting cyberspace's strategic usefulness without quite foreclosing further exploration into its offensive potential. Chiseling away different aspects of the difficult problem of contrasting digital activity (conducted in bits and packets) with warfare, which historically has been waged in blood and steel, Libicki warns against overexuberance and overinvestment in offensive cyber capabilities that might prove to be interesting but of little strategic value. (Libicki, 2009)

Libicki's works must be considered in any proper analysis of the offensive potential of cyberspace. This paper cannot do justice to the scholar's complex and elegant argumentation, so will simply distill one aspect of the theory into terms relevant to this work's purpose:

(1) Cyber operations are a form of information warfare, in which one side's information is used to attack an adversary's information. "Information" is broadly defined as encompassing data used both to inform human consumers (semantic) and to enable or manage computerized processes through which information is conveyed (physical and syntactic). (Libicki, 2007)

(2) Offensive cyber operations aim to create an information advantage by complicating, obstructing, or derailing processes through which an adversary accesses, communicates, utilizes, or interprets information, or by improving one's own processes for accessing and interpreting adversary information. Target processes are both human (mental/neurological) and non-human (digital/mechanical). (Libicki, 2007)

(3) There are two types of offensive cyber operation. "Operational" cyberwar supports or improves offensive military (or paramilitary) operations in the physical domain. "Strategic" cyberwar aims to affect an adversary's security calculations or behavior, without recourse necessarily to physical violence. (Libicki, 2009)

(4) Inherent qualities of attack in the cyberspace domain inhibit offensive cyber operations' strategic potential, including: non-lethality and limitation of coercive or destructive capability; reliance on adversary vulnerability ("no forced entry") (Libicki, 2009); difficulty of attack attribution and susceptibility to improved countermeasures (counterproductivity) (Libicki, 2012) and conceptual and legal

> problems associated with escalation management and transferring violence in the cyber domain to the physical domain. (Libicki, 2012)

Befitting the author's RAND heritage, Libicki contrasts the potential of cyber operations with that of the traditional "strategic" threats of aerial bombing and nuclear weapons. He concludes that the particularities of the cyberspace domain are such that offensive cyber operations are unlikely to offer the same decisive capacity in a confrontation or strategic competition, and therefore may not merit the same attention or investment as other strategic weaponry. (Libicki, 2012) Libicki's argumentation eschews definitive pronouncements out of respect for the ambiguities inherent in the rapidly evolving technology of human-computer interaction. He allows that cyberspace, in spite of its limited applicability in warfare, will become more, not less, relevant as human reliance upon it becomes more pervasive and habitual. (Libicki, 2007) His more recent work returns to offensive cyber operations' relevance to affecting adversary psychology, which this paper will explore in detail.

Instrumental versus strategic cyber operations

Drawing upon these scholars' work, this paper proposes two types of offensive cyber operation: instrumental and strategic. The defining characteristic of an "instrumental" cyber attack is that it serves as an enabling action in the pursuit of battlefield objectives that may transcend the cyberspace domain. This could include both extraction of adversary intelligence and tactical actions set in the context of a combined arms maneuver during a military or paramilitary conflict. (Miranda, 2011) Instrumental cyber operations use information to attack information, but to achieve an effect not necessarily limited to information. A cyber attack aimed at a military communications system, for example, is instrumental to the tactical objective of disrupting command-and-control. A cyber attack that inserts a virus into a radar control system could be instrumental to disrupting an adversary's air defenses. A cyber attack that causes a country's major media websites to go dark is instrumental to undermining a government's ability to communicate with its constituents in the event of a conflict. Instrumental offensive cyber operations can but do not necessarily overlap with long practiced and better understood military disciplines including electronic warfare, directed energy attacks, and MISO. Whether an instrumental offensive cyber operation's information targets are hardware or human, the action strives to confer a battlefield advantage that inherently is temporary.

A "strategic" offensive cyber operation is harder to define. Here Libicki's comparison of cyber operations to nuclear weapons is instructive. In American military parlance as well as in its bureaucratic organization, "strategic" forces have evolved over time to denote some but not all of the substructures that manage and deploy nuclear weapons, ballistic and anti-ballistic missiles of a certain range, long-range aerial bombers, space assets, and, since the establishment of United States Cyber Command (USCYBEROM) in 2009, cyber operations. (US Strategic Command, 2013) The etymology of this classification scheme is beyond the scope of this paper, but it is interesting to note that the Defense Department's Joint Publication 1-02 contains definitions for fifteen terms related to the word "strategy," while "strategic forces," "strategic attack," and "strategic weapons" are not included. (JCS, 2013) In the absence of doctrinal clarity, one might extrapolate that offensive or defensive military capabilities are deemed "strategic" if their possession confers a layer of invincibility or invulnerability above and beyond the predominant

conventional capabilities of the time. In this vein, strategic weaponry may be closely aligned to the concept of deterrence.

A strategic capability is a characteristic that helps define the strategic paradigm between competing forces at a certain point in time. It follows that a strategic offensive operation, then, aims in some way to affect that paradigm directly, without necessarily being a component of a larger military campaign or maneuver. In a state-to-state relationship, an offensive strategic operation could be said to have the aim of inducing a change in a country's perception of its overall security situation. This definition is means- or medium-neutral; it does not attempt to define how such an attack is carried out, only the intent of the attack. Moreover, because a strategic offensive operation is aimed ultimately at perception, *actual* lethality or destructive power may be no more important than *implied* lethality or destructive power.

Armed with this distinction between an instrumental offensive operation and strategic offensive operation, this paper may now assess properly the strategic potential of warfare in the cyberspace domain. The first step will be to review known types of offensive cyber operation, zeroing in on Stuxnet as a case study with which to examine strategic versus instrumental effect. A closer look at the strategic implications of Stuxnet then broadens the aperture through which China's offensive cyber strategy might be perceived.

Three categories of offensive cyber operation

A cyber *exploitation* seeks to intrude into an adversary's information system to access, exfiltrate, or monitor privileged information. Target information can be substantive, such as designs for classified weapons systems, or procedural, such as passwords or source code. Cyber exploitations may be conducted for military, intelligence, or economic purposes. Most known cyber attacks emanating from China seem to belong to this category. (Thomas, 2010)

Cyber *disruption* aims to complicate the integrity or correct functioning of an adversary information system. Denial of service and distributed denial of service attacks, such as those seen in the April 2007 attacks on Estonian institutions and the August 2008 attacks on Georgian government agencies and websites, disrupt communication between institutions and their dependents, undermining normal flow of commerce and public confidence. (Rid, 2012) When analysts comment on the need for U.S. networks to reduce vulnerabilities and increase resiliency, they primarily are expressing concern about the potential for adversaries to create instability through disruption of critical systems. These include the informational technology infrastructure upon which the U.S. Joint Force increasingly depends, but in the holistic sense also include the systems that underpin America's banking and finance system, energy grid, media, and other critical infrastructure. (Lynn, 2010) This paper defines certain other familiar types of attack – *sabotage, subversion, denial* – as subsidiary categories of disruption. As such, the 2009 Stuxnet attack, as will be seen, was primarily a disruptive offensive cyber operation. (Sheldon, 2011)

While examples of *deception* as a type of offensive cyber operation are less readily accessible, it is easy to understand how a domain defined by information could be subject to attacks using misinformation, disinformation, or overinformation. (Libicki, 2007) An offensive cyber operation that might cause a system to deliver incorrect information, to deliver information incorrectly, or to obscure correct information, would deceive its operators into making misdirected decisions. As Libicki notes, offensive cyber operations can deceive information systems themselves into making incorrect decisions by corrupting the logic through which automated processes are executed. (Libicki, 2009) Deceptive offensive cyber operations have the

potential to undermine the integrity and reliability of information, thereby complicating decision making processes and softening an adversary's confidence in his own systems. (Sheldon, 2011)

There is no law of correspondence between the three types of offensive cyber operation and an operation's instrumental or strategic functions. Exploitation, disruption, and deception each can be instrumental and/or strategic. Moreover, each of the three types can be instrumental to another: an exploitative attack can enable disruption, a disruptive attack can serve to deceive, or a deception could aim to facilitate exploitation. Finally, an offensive cyber operation can aim to achieve instrumental and strategic effects at different levels.

The curious case of Stuxnet

The complex and fascinating 2009-10 Stuxnet operation integrated all three types of attack and pursued both instrumental and strategic objectives. (Gross, 2011) It is widely understood that Stuxnet's objective was to complicate or slow Iran's development of nuclear weapons capability. The ultimate aim was to corrupt the programmable-logic controllers (PLCs) that operated mechanical centrifuges used in uranium enrichment, causing the process to malfunction. (Gross, 2011) Thus the attack falls into the category of disruption.

However, for the cyber weapon's "payload" to reach its target, its operators first had to employ a sophisticated, multipronged, exploitation campaign to discover which systems around the world were using the specific PLCs manufactured by Siemens and then "paint" the right target. (Gross, 2011) The offensive cyber campaign itself would have been designed based on intelligence about the information systems supporting Iran's nuclear program, gathered through either or both human and technical means, including computer network exploitation. Finally, deceptive tactics were used to divert attention from the main attack vector as well as conceal technically the exploitative and disruptive effects of the attack in order to sustain and amplify its devastation. The timing of the attack waves, their discovery or revelation, and public insinuations regarding their attribution may have been coordinated or timed to increase the psychological impact of the deception. (Gross, 2011)

Was Stuxnet at its core intended as an instrumental or strategic offensive cyber operation? If one agrees that the operation's objective was to delay progress in Iran's nuclear weapons program, then under this paper's definition the operation was clearly instrumental. A pause in Iran's nuclear weapons development would not in and of itself irrevocably change the fundamental strategic paradigm between Iran and its adversaries suspected of engineering the attack. Had Stuxnet aimed to destroy outright Iran's incipient nuclear capability, then it could have a plausible claim to strategic rather than tactical intent. But even then the effects would be temporary, because nuclear capability, as an example, is a function of hardware, knowledge, and will, all of which are either retrievable or regenerable. Nor does this theoretical example account for the difficulty of expunging information with finality, given that multiplexing of systems is by now a common best practice in information security and management. (Libicki, 2009)

The disruption or destruction of its nuclear capability via surreptitious, stealthy means such as Stuxnet employed could, however, complicate Iran's calculation of the deterrent value of an active nuclear weapons program. Here the problem of an offensive cyber operation's attribution supports what could be considered a strategic characteristic. Compare Stuxnet to the Israel Defense Forces' Operation *Opera* in 1981, which caused the destruction of Iraq's Osirak nuclear reactor. If Israel's aerial attack retarded Iraq's nuclear weapons program and altered the perceived military balance of force between the two countries for a certain period of time, the

operation's attribution also exacerbated underlying hostility in the Israel-Iraq relationship and caused second-order effects that may have weakened Israel's international standing. (Kirschenbaum, 2010) Stuxnet's stealthy, deceptive, and deniable components, on the other hand, even given strong presumptions about the identity of its perpetrators, complicate Iran's options for both responding to the proximate attack and using the occasion of the attack to strengthen its defensive claims in the context of its overall strategic environment.

Marginal strategic value could be said to derive from these Stuxnet characteristics, which may be common to offensive cyber operations as a category. However this paper argues that, intentional or not, Stuxnet's enduring strategic value rests in undermining Iran's perceptions of the functionality of its nuclear program within its overall security paradigm. Stuxnet achieved this in two related ways, through: 1) demonstrating a previously unproven, potent, and complex adversary offensive capability, and 2) creating doubts about the reliability of the information systems that undergird Iran's nuclear weapons program. These effects in turn raise questions in the minds of both Iranian national security decision makers and the general population about Iran's ability to protect itself and the systems employed to bolster its defenses. Here the consummate offensive cyber operation finally crosses Libicki's strategic threshold through announcing the potential to soften adversary confidence and engender uncertainty, doubt, and fear about his overall security. Returning full circle, these potentialities confer on offensive cyber operations a strategic value similar to that bestowed by nuclear weapons capability. (Libicki, 2011)

The ultimate target of a strategic vice instrumental offensive cyber operation is, after all, more likely to be software than hardware: adversary perceptions and decision making rather than the digital instrumentation that informs it. In other words: the human side of the information equation. This firmly places offensive cyber operations in the same category as "low tech" military disciplines such as information operations, MISO, military deception, denial, and deterrence. (DoD Pub 1-02, 140&190) Moreover, if the real potency of offensive cyber operations is carried in their ability to affect adversary psychology, then cyber weapons are no less valid as instruments of warfare than nuclear warheads, intercontinental ballistic missiles, and anti-satellite kill vehicles, none of which with two notable exceptions over fifty years ago have been employed to any effect *beyond* the psychological domain. One could argue that offensive cyber operations have the potential to be more strategically effective precisely because their non-lethality makes them morally more deployable and therefore more demonstrable.

This same non-lethality is the characteristic that some scholars seize upon in proclaiming that nothing that happens inside the cyber domain can be considered warfare. (Rid, 2012) Another is the close family resemblance between exploitation, which this paper acknowledges is the most commonly seen of the three categories of offensive cyber operation, and espionage. These arguments reflect important ethical and legal considerations that receive substantial treatment by military and legal scholars in other venues. (Goodman, 2010) Suffice it to repeat the oft-heard line of reasoning that espionage is a normal element in state-to-state relations, and because espionage, unless it can be connected directly to devastating effects, does not constitute a *casus belli*, cyber exploitation therefore cannot be considered a form of warfare. (Dinstein, 2002) In a legal or ethical discussion, this logic prompts valid questions. In an examination of national security strategy, it is a red herring. To understand why, it makes sense finally to turn back to the cause of the cyber warfare debate's latest eruption: China.

A theory of China's offensive cyber strategy

A February 2013 *New York Times* article announcing a detailed, 60-page assessment by American cybersecurity firm Mandiant brought to the front page one of the worst kept secrets in national security circles: Chinese government and military involvement with a wide range of offensive cyber operations against U.S. military, government, and commercial networks. (Singer et al., 2013) The report followed close on the heels of revelations by the same newspaper that China-based cyber attacks targeted its own reporters and operations. The public revelations and accompanying outcry marked a milestone after what is assumed to be over a decade of Chinese offensive cyber activity increasing in frequency and sophistication.

Recent cyber attacks widely believed to have enjoyed Chinese government sponsorship include GhostNet (2008-9) (Rid, 2012); theft and corruption of U.S. company Google's source code (2009) (Thomas, 2012); theft of data from U.S. network security company RSA Security (2011); and, using information gleaned from the latter, a subsequent breach of U.S. defense contractor Lockheed Martin's systems (2011). (Sanger, 2013) These cases represent only the most prominent of the known attacks suspected of originating in China; there are assumed to be more. Chinese government spokesmen have denied official involvement, using such words as "irresponsible" and "unprofessional" to describe reports alleging otherwise, and claiming that China, too, is a victim of offensive cyber operations. (Barboza, 2013)

Even without incontrovertible proof, assuming these high-profile attacks enjoyed some active or passive official sponsorship, China's government and military are revealing themselves to be instrumental operational cyber warriors *par excellence*. The serviced objectives are wide ranging: stealing military secrets; stealing trade secrets; harassing government opponents; exfiltrating information about cybersecurity processes to enable further exploitation; launching probes to identify vulnerabilities that could be exploited in armed conflict; and learning from each and all of these operations to improve capability in the offensive cyber discipline. With its military, commercial, and informational applications, China's multi-pronged, instrumental cyber campaign can be said to have the overarching goal of contributing to China's comprehensive national power. (Blumenthal, 2013) The campaign clearly serves a strategic purpose, but do the discrete attacks in and of themselves satisfy the criteria of strategic offensive cyber operations?

Recall that in this paper's definition, a strategic offensive cyber operation uses information to attack information with the intent of inducing a change in an adversary's perception of his own security situation. Accretion to China of robust cyber capabilities made plain by its decade-long offensive campaign clearly has changed global perceptions of China's strength. When the China variable in any of its bilateral and global security equations increases in absolute value, this necessarily alters, to some extent, China's underlying security paradigm. Thus it can be judged that, instrumentality aside, the demonstration effects of many of China's offensive cyber operations carry strategic weight. But intent as well as effect must be considered before ascribing strategic purpose to an offensive operation. The analysis also must account for the other side of the security equation: the degree to which China's offensive cyber operations affect adversaries' perceptions of their own capabilities.

In the mid-1990s, Chinese military scholars, borrowing heavily from their American counterparts, began to intuit cyber operations as a developing component of information warfare (IW). (Mulvenon, 1999) Having been prompted to a great extent by Chinese impressions of information technology support for American military operations in the 1991 Gulf War, these early writings demonstrate an emphasis on instrumentality, particularly IW support for reconnaissance, communications, and attacks on adversary command-and-control. (Mulvenon,

1999) Though Chinese military scholars' early IW imaginings focused squarely on the operational environment, their efforts to develop a theoretical framework also referred specifically to deception, intelligence collection, and psychological warfare as related concepts. (Wang et al., 1995) And in the view of at least one astute observer, China's emerging IW strategy was distinguishable from its American analogue by its recognition of IW's asymmetric capabilities and potential to contribute to victory without recourse to violence beyond the information domain. (Mulvenon, 1999) With such emphases, these writings found a comfortable home for IW in the center of one of Chinese strategic culture's inner sancta, Sun Tzu's concept of "victory without battle." (Sawyer, 1994)

From this matrix, one may extract how China's offensive cyber operations, as an ideal form of IW, convey strategic purpose beyond their multiple instrumentalities. China's national security and military strategies are built upon the three pillars of sovereignty, modernity, and stability. (Finkelstein, 1999) These encompass internal and external elements: "modernity" for example describes China's absolute conditions but also as refracted back through the prism of its competitors' conditions; "stability" refers both to China's relations with its neighbors and internal political cohesion. The United States and the global system it presides over are seen in China as external forces capable of threatening these pillars and constricting or complicating China's fulfillment of its national destiny. (Finkelstein, 1999)

Beyond the realm of state-to-state relations, worldwide adoption of high technology information and communication systems – global "informatization" – is also recognized by Chinese strategists as a transformative force freighted with opportunity and threat. "Informatization" is at once a benchmark of China's absolute and relative modernity, and at the same time a potential threat to China's prevailing concepts of sovereignty and stability. China in effect is forced to adopt a hedging strategy toward informatization itself: welcoming its natural evolution and adoption when it is channeled toward strengthening the People's Republic, while finding ways to diminish its destabilizing qualities. This explains why so much of China's cyber activity is directed at its own citizenry, especially those who would fuse technological know-how and political bravery to access and deploy information that calls into question the Chinese Communist Party's monopoly on power. (Link, 2012)

The threats posed by informatization are considered even more acute when wielded to great effect by China's adversaries. If Chinese strategists are generally sanguine about China's ability to fend off conventional military threats, they fret constantly about China's vulnerability to Western and American "soft power" predations. The Western-led human rights and democracy agendas, for example, are seen as a form of interventionism aimed at subverting China's sovereignty and stability. Cyberspace is a key battleground. In a recent opinion piece, China's newly elevated Deputy Chief of the General Staff for Foreign Relations and Intelligence went so far as to write that "in the information era, seizing and maintaining hegemony in cyberspace is more important than seizing command of the sea and commanding the air were in World War II." (Qi, 2013)

Adversaries' soft interventionism enabled by the transformative power of informatization is the combination threat that cuts to the heart of China's security paradigm, and explains the Chinese military's preoccupation with cyberspace. Their assessment of the enormity of the challenge demands a comprehensive response that transcends mere instrumentality. In offensive cyber operations, the Chinese military and their civilian overseers have hit upon a military strategy that aims all at once to close the gap between U.S. and Chinese technological-military prowess, blunt the tip of the Western spear of soft penetration, and slow the corrosive effects that

pervasive access to cyberspace will have on the Chinese Communist Party's monopoly on information. Not only do China's offensive cyber operations aim to deny the United States actual employment of information in all its forms as a weapon of choice, they aim to call into question the overall proposition of information-as-weapon until such time as China can wield it more skillfully than its adversaries.

This second aspect of China's offensive cyber strategy demands deeper scrutiny than it is currently receiving. It explains why China's target set has been so broad – governments, Tibetan exile groups, military contractors, technology companies, *New York Times* reporters, etc. – and why China will continue to offend even as its reputation suffers the indignity of its unmasking as the world's leading cyber scofflaw. In addition to multiple instrumental uses, a successful attack on Google, a global symbol of U.S. innovation and technological prowess, makes a mockery of the concept of popular information dominance. It puts the United States on notice that any technological edge it believes it enjoys will not be functional in a conflict with China. It also reminds China's restive domestic audience that unfettered technological advancement alone does not bring security.

The People's Republic at its core is a self-perpetuating information operation. Its survival demands a strategy not only to counter adversaries who would use information against it but also to deny information's innate subversive potency. Any cyber attack – on infrastructure, on privileged information, on privacy – that creates perceptions of information insecurity reinforces the validity of China's authoritarian model, which survives on the Party's mediation of fact. Information as harnessed by government is proven as a national strength, while laissez-faire acceptance of the information age becomes a vulnerability.

Here again offensive cyber operations are seen as a form of information warfare fought mostly in the psychological domain, that is, in the mental and emotional processes of information consumers both friendly and adversarial. In China's strategic tradition, constant agitation against the enemy in the psychological domain – through intelligence exploitation, manipulation, enervation, deception, and exacerbation of internal contradictions – is what prepares the battlefield or achieves strategic victory without physical violence. (Lin, 2013) Millennia of experience refining the functions of information in support of these tactics have conditioned China to be an imaginative and agile adversary in the cyber domain. If China is able to close in on the United States' high-technology head-start, over time the Chinese approach to offensive cyber operations, which emphasizes affinities with information warfare rather than differences, could reshape the two countries' underlying security paradigm.

Cyber war takes its place

There should be no residual doubt that offensive cyber operations, when wielded by able adversaries such as China, are deeply strategic. But do they constitute warfare? Much ink has been spent in the intervening decades since Arquilla and Ronfeldt's 1993 clarion call suggesting all the reasons cyber war does not, cannot, and will not come to pass. These same arguments now are bubbling toward the surface of the American popular consciousness.

There are good reasons for scholars to make them. Perfunctory political declarations of "war" as a catchphrase for complex national security and social phenomena – "War on Terror," "War on Drugs" – have led the United States more than once into rocky terrain that has been equally difficult to traverse or withdraw from. There are also clear ramifications for allocation of scarce national security resources, and many scholars justifiably concerned about an outsized

Department of Defense role in U.S. national security rue premature militarization of the cyber domain. (Rid, 2013) Worthy as they are, however, such concerns should be excluded from theoretical discussions of the plausibility of cyberspace as a warfighting domain.

More thoughtful analyses that come to negative conclusions regarding military possibilities for cyberspace approach the question in reverse: by looking at what makes cyber operations different from what humanity has come to know as "war" throughout history. These arguments usually define war as necessarily involving physical force and violence, which cyberspace's digital weaponry do not readily yield. (Rid, 2012) International laws of war in turn rely on this bounded definition. (Dinstein, 2002) Focus on physical violence as an essential characteristic of warfare seems to spring from a misreading or selective reading of Clausewitz, whose theories pervade Western military thinking. (Beyerchen, 1992)

Violence is indeed a word Clausewitz uses often, but to conclude that his definition of violence applies only to the physical world is merely to acknowledge that his writings are a product of his time and place. Concepts of "emotional violence" and "psychological violence," not unfamiliar terms in the post-modern world, simply had not been articulated in 19th century Prussia. A closer reading of Clausewitz's first core description of war – "an act of force to compel our enemy to do our will" – already implies a strong psychological element to war by focusing on will and compulsion, with "force" only the active agent.

By suggesting "force" as a weapon in a contest of wills, Clausewitz's own definition begins to transcend the word's physical and metaphysical heritage and intuit a deeper relationship to cognition. Contrary to conventional wisdom, Clausewitz's theories both accommodate and prefigure the possibility that organized violence with political purpose can transcend the physical domain. Cyberspace operations as information warfare are as at home in Clausewitz as in Sun Tzu.

Conclusion and recommendations

Misreadings and oversimplifications of history have more than once led militaries into dead-ends, and cultural biases and bureaucratic limitations obscure strategic opportunities readily apparent to adversaries. American politicians, commentators, and yes, even military strategists do not get to decide whether or not the country is engaged in a cyber war. (Barnett, 2013) Adversary actions, in this regard, carry greater weight. U.S. strategists are deprived of the luxury of close-mindedness. The new and changing domain of cyberspace demands an inductive vice deductive approach. When it comes to cyber operations, unhealthy attachment to concepts of physical force and lethality as necessary components of offense drastically limit exploration of a terrain entirely composed of information and therefore oriented more toward human cognition and psychology than to biomechanics. Offensive cyber operations do not have to be kinetic to be strategic.

A functional cyber strategy for the 21st century must be about more than reducing system vulnerabilities – monitoring attack vectors, plugging system flaws, reinforcing firewalls – all adaptations of defensive tactics in the physical domain. To embrace fully cyberspace's offensive potential is to recognize the dynamic nature of technology and respect the game-changing possibilities of increasingly frequent and complex human-technology interactions with and in information. Information ultimately is what determines and explains whether, how, and why countries go to war, because information affects the perceptions, calculations, and emotions of peoples, their militaries, and governments. Strategic offensive cyber operations see information

not just as the weapon but as the prize. In that light, here follow five modest recommendations for consideration by USCYBERCOM:

(1) Assign Joint working groups to assess how traditional warfare concepts such as deception, denial, and deterrence may be applied in the cyberspace domain;

(2) Train information warriors as well as computer network operators. Strategic offensive cyber operations require neurologists, psychologists, and mass media specialists as much as programmers, cryptanalysts, and engineers. The most critical software sits inside adversaries' crania, not in their computer circuitry;

(3) Break down agency barriers: an effective cyber strategy requires fusion centers that integrate intelligence, military, and public diplomacy-related disciplines;

(4) Apply the concept of precision targeting to cyber offense. As commercial marketing companies already know, cyberspace is a mass medium that also can be bent into a highly customized information experience;

(5) Believe the hype: human interaction in and with the cyberspace domain will become more encompassing, pervasive, and complex. And as forms of human interaction go, war has endured the tests of time.

Works Cited

Barack Obama, Executive Order – *Improving Critical Infrastructure Cybersecurity* (Washington, DC: The White House, February 12, 2013).

See, for example, Ian Wallace, "Why the U.S. is not in a Cyber War," *The Daily Beast*, March 10, 2013.

Michael Joseph Gross, "A Declaration of Cyber-War," *Vanity Fair* 53, no. 4 (April 2011).

Thomas Rid, "Cyber War Will Not Take Place," *The Journal of Strategic Studies* 35, no. 1, 5-32 (February 2012), 11-15, 17-19.

Dorothy E. Denning, "Assessing the computer network operations threat of foreign countries," in *Information Strategy and Warfare: A Guide to Theory and Practice*, John Arquilla and Douglas A. Borer, eds. (New York: Routledge, 2007); Nick Hopkins and Luke Harding, "Pro-Assad Syrian hackers launching cyber attacks on Western media," *The Guardian*, April 29, 2013, on http://www.guardian.co.uk/world/2013/apr/29/assad-syrian-hackers-cyber-attacks (accessed May 11, 2013).

John Arquilla and David Ronfeldt, "Cyberwar is Coming," *Comparative Strategy* 12, no. 2 (1993), 27-31.

John Arquilla and Douglas A. Borer, eds., *Information Strategy and Warfare: A Guide to Theory and Practice* (New York: Routledge, 2007), 1 and 8.

Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009).

Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, (Cambridge: Cambridge University Press, 2007), 20, 25-26.

Martin C. Libicki, "Cyberspace is not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (Fall 2012), 331.

Ray J. Miranda, "Offensive Cyber Warfare: An effective weapon for the MAGTF commander," *Marine Corps Gazette* (September 2011), 10.

United States Strategic Command, Fact Sheets, Cyber Command, on http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed April 11, 2013).

U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010 as amended through April 15, 2013), 273-275.

See Timothy L. Thomas, "Google Confronts China's 'Three Warfares'," *Parameters* (Summer 2010), 102.

William J. Lynn III, "Defending a New Domain," *Foreign Affairs* 89, no. 5 (2010), 1-3.

John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly* 5, no. 2 (2011), 104.

For a popular narrative of the Stuxnet case, see Gross, "A Declaration of Cyber-War." A technical analysis of the worm is available on Nicholas Falliere, Liam O. Murchu, and Eric Chien, *W32.Stuxnet Dossier*, Version 1.4, Symantec Security Response (February 2011).

Joshua Kirschenbaum, "Operation *Opera*: An Ambiguous Success," *Journal of Strategic Security* 3, no. 4 (Winter 2010), 55-57.

Martin C. Libicki, "Cyberwar as a Confidence Game," *Strategic Studies Quarterly* (Spring 2011), 137-139, 143.

For doctrinal definitions, see Joint Publication 1-02, *DoD Dictionary*, 140 and 190.

Libicki, *Cyberdeterrence and Cyberwar*, 27-35; Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly* (Fall 2010), 109 and 123.

Yoram Dinstein, "Computer Network Attacks and Self Defense," *Computer Network Attack and International Law* 99, Michael N. Schmitt & Brian T. O'Donnell eds. (2002), (Vol. 76, U.S. Naval War College International Law Studies), 105.

David E. Sanger, David Barboza and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against the U.S.," *The New York Times*, February 18, 2013, on http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all&_r=0 (accessed April 20, 2013)

Ibid; David Barboza, "China Says Army is Not Behind Attacks in Report," *The New York Times*, February 21, 2013, on http://www.nytimes.com/2013/02/21/business/global/china-says-army-not-behind-attacks-in-report.html (accessed April 20, 2013).

Dan Blumenthal, "How to Win a Cyberwar with China," *Foreign Policy*, February 28, 2013, on http://www.foreignpolicy.com/articles/2013/02/28/how_to_win_a_cyberwar_with_china, (accessed April 20, 2013); Thomas P. M. Barnett, "Putting China's 'Hacking Army' into Perspective," *Time*, February 22, 2013, on http://nation.time.com/2013/02/22/putting-chinas-hacking-army-into-perspective/ (accessed April 20, 2013).

James C. Mulvenon, "Chapter Nine: The PLA and Information Warfare," *The Peoples Liberation Army in the Information Age*, James C. Mulvenon and Richard Yang, eds., (Santa Monica, CA: RAND, 1999), 181-182.

Baocun Wang and Fei Li, "An Informal Discussion on Information Warfare," *Jiefangjun Bao*, June 13, 1995, translated and found on Federation of American Scientists website, http://www.fas.org/irp/world/china/docs/iw_wang.htm (accessed April 21, 2013).

Ralph D. Sawyer, ed., *Sun Tzu: Art of War* (Boulder, CO: Westview Press, 1994), 128-129, 177.

David M. Finkelstein, "Chapter Seven: China's Military Strategy," *The Peoples Liberation Army in the Information Age*, James C. Mulvenon and Richard Yang, eds. (Santa Monica, CA: RAND, 1999), 103-4.

Perry Link, "America's outdated view of China," *The Washington Post*, May 11, 2012.

Jianguo Qi, "Unprecedented Great Changing Situation: Understanding and Thoughts on the Global Strategic Situations and Our Country's National Security Environment," *Study Times* (*Xuexi Shibao*), January 21, 2013, trans. by James A. Bellaqua and Daniel M. Hartnett, *CNA China Studies*, 1, 8-9.

Sawyer, *Sun Tzu*, 134-136; Jenny Lin, "Navigating U.S.-China Relations: Complicated by China's 'Unrelenting Strategy,'" *PacNet*, No. 15, Pacific Forum CSIS, Honolulu, HI, March 5, 2013.

Thomas Rid, "The Great Cyberscare," *Foreign Policy*, March 13, 2013, on http://www.foreignpolicy.com/articles/2013/03/13/the_great_cyberscare (accessed March 15, 2013); Wallace, "Why the U.S. is not in a Cyber War."

This passage draws on analysis of Clausewitz's *On War* found in Alan Beyerchen, "Clausewitz, Nonlinearity, and the Unpredictability of War," *International Security* 17, no.3 (Winter 1992), 66-69; and in John Stone, "Cyber War Will Take Place!" *Journal of Strategic Studies* 36, no. 1 (2013).