Beyond the Rift in Cyber Strategy

A middle ground for the US military posture in cyberspace

Jean-Loup Samaan

Introduction

Over the last five years, interest in cyber-defense has grown in earnest, particularly after the cyberattacks against the Estonian government in spring of 2007, the discovery of the GhostNet network targeting the Dali Lama's diplomatic offices in 2009, and the Stuxnet worm's disruption of the Iranian nuclear program in 2010. As a result, the US government has made substantial moves in the last two years towards the institutionalization of cyber-defense:

- The appointment of Howard Schmidt as Cybersecurity Coordinator for the Obama Administration in December 2009;

- The implementation of a formal partnership in October 2010 between the Department of Homeland Security and the Department of Defense, which specifies the responsibilities of each organization;

- Finally, the creation of the US Cyber Command in May 2010, a joint organization including components from all military services (the Army Forces Cyber Command, the U.S. Navy Fleet Cyber Command, the 24th Air Force, the Marine Corps Forces Cyberspace Command).

Despite these bureaucratic efforts in the White House and in the interagency process, this article argues that there remains a lack of consensus in Washington, particularly within the Department of Defense, on threat assessment in cyberspace and its military implications. A stark intellectual rift between "alarmists" and "skeptics" still prevails. As a result, this elementary battle has led to dysfunction in the institutional response to cyber-threats and jeopardizes the implementation of an effective military posture in cyberspace. Consequently, we need to reassess the relevance of cyberspace as a distinct military domain.

To that end, this article aims for a middle ground between these opposing views, supporting the idea that cyberattacks are more than just a technical nuisance, but less than an existential threat to US national security. As of today, they remain a valuable, but not decisive, tool of military action. At the operational level, it means that cyberspace is not an independent domain. In other words, while warfare in the air is different from warfare on the sea, it is possible to have one without the other. But warfare in cyberspace must be accompanied by warfare in one of these other domains to lead to physical effects. As a result, this paper recommends a comprehensive integration of cyberattacks (which are precisely *not* autonomous cyberwarfare) into a joint analysis of military battles. Because pundits have been focusing on the broad geopolitical implications of cyberattacks, the strategic literature lacks a systematic and detailed campaign analysis of these acts. This joint analysis would frame cyberattacks as offensive or defensive military engagements in the process of a larger naval, air, or land campaign. Based on the findings of this research, cyberattacks should be considered a subset of an offensive, a means of *denial* rather than a means of *punishment*. They aim at attaining an intermediate goal for the attacker.

Consequently, as long as cyber operations are launched by actors with broader objectives than

exclusively dominating channels of communication, there is legitimate doubt over whether a cyberwar could occur without an extension to other traditional military domains.

As a necessary word of caution, this article explicitly excludes cases of cyber-espionage whose aim differs from cyberattacks: while the former tries to steal and exploit information from an enemy (eg, the daily attempts of intrusion into the servers of the Defense Department), the latter are defined here in strict military terms to directly or indirectly destroy or disrupt targeted infrastructures. In other words, cyberattacks should be narrowly considered at the battle level as a component of the forces used by the attacker.

This article has three sections. The first section assesses the fundamental divide of the strategic debate on cyber-defense. I show that although many efforts have been dedicated to understanding the strategic dimensions of cyberspace, a rift prevails between two camps: one predicts the emergence of cyberwarfare while the other characterizes such events as no more than cases of 'cyber-annoyance'. In the second section, I explain that this protracted clash of views comes mainly from the use of two misleading analogies for cyberwarfare: nuclear warfare and strategic bombing. The article then demonstrates in a third section that a middle way to implement a military policy in cyberspace can be found by understanding cyberattacks as a subset of broader military operations. To that end, I employ the tools of campaign analysis to make an appraisal of events such as the cyberattacks against Georgia prior to its August 2008 war against Russia. Finally the article's conclusion explores the implications of my findings for future research.

Cyberwar or cyber-annoyance? The fundamental divide of the strategic debate

In spite of obvious efforts (such as the 2009 60-day *Cyberspace Policy Review*, led by Melissa Hathaway, former Senior Advisor to the US Director of National Intelligence), the Obama administration has not tackled the fundamental dispute over the strategic implications of cyberattacks. Currently in Washington, two opposing views compete with each other: the alarmist voices (and indeed the most vocal ones) who predict the advent of cyberwarfare as a revolutionary form of conflict, and the skeptical voices who acknowledge the "annoying" vulnerabilities of US civilian and military infrastructures but who do not see such attacks as the constituents of a pattern for potential new major conflicts.

This divide has existed since the middle of the 1990s, when the US Department of Defense and military-related think tanks started issuing reports and articles on the strategic implications of cyberspace. Although the cyber realm and information warfare have significantly evolved since then, the terms of the divide have been noticeably constant all along. Starting in the 1990s, an impressive proportion of the strategic studies literature focused on the so-called "Revolution in Military Affairs", of which the optimal exploitation of electronic interfaces was only one of many components. From the futurists Alvin and Heidi Toeffler, and their famous "third wave" characterization of the information revolution,[1] to the iconoclast colonel Richard Szafranski and his fuzzy concept of "neocortical warfare", people inside the Defense Department started to read and write about warfare in the information age.[2] This led to the now famous but still-ambiguous concept known as "information warfare".[3]

The starting point for emerging conceptual debates could be marked in 1993, when John Arquilla and David Ronfeldt, two researchers at the RAND Corporation, published an article titled "Cyberwar is Coming!" in the journal *Comparative Strategy*.[4] Behind this emblematic title, the two

scholars argued that cyberwar - defined as a war centered on information flowing through electronic interfaces - was to provoke a fundamental bottom-up review of military organizations.

Yet straight away, ideas about a war in cyberspace sounded at best farfetched, at worst spurious. After all, was it not a term - cyberspace - taken from a science fiction book?[5] Some researchers saw this conflation of concepts and ideas as an eventual march toward the establishment of a coherent field of studies. For instance, the late Laurent Murawiec, a scholar from the Hudson Institute, observed in 2001 that

> As presently constituted, the field seems to cover a bewildering array of subsets: psychological warfare, deception, cyberwar, critical information protection, computer network attack, computer network exploitation, netwar, and more. The confusion is normal. When people started building automobiles, hundreds, if not thousands of attempts were made which bore the name of "automobile", and other names too. The variety of shapes, methods, materials, solutions proposed to the various problems of a self-propelled vehicle, was equally bewildering. It took time and experience, much competition and failures, to winnow, to rationalize, to weed out. We can only expect the same to hold true in the field of "information warfare" as opened up by the digital revolution of the last quarter century.[6]

But contrary to Murawiec's faith, ten years later, the confusion still remains. Moreover, this decade-long divide has deepened since 2007 as cyber-defense has been put at the forefront of the political-military agenda following the cyberattacks against Estonia in 2007, the use of cyberspace during the military campaign between Russia and Georgia in 2008, and lastly the Stuxnet worm that targeted the Iranian nuclear plant in Natanz in 2010.

Counted among the alarmist voices are recently retired US officials such as Richard Clarke, former Special Advisor to the President on Cybersecurity, and Mike McConnell, former Director for National Intelligence. Mr. Clarke explains in his book, *Cyberwar: The Next Threat to National Security and What to Do About It*, that what states "are capable of doing in a cyber war could devastate a modern nation".[7] In February 2010, Mr. McConnell explicitly titled a much-discussed op-ed from the *Washington Post*, "How to win the cyberwar we're losing".[8]

More specifically, these voices frequently compare the current debate on the scope of cyberwarfare with the age of nuclear strategy in the 1950s. For instance, Mr. McConnell asserts that "the cyber-war mirrors the nuclear challenge in terms of the potential economic and psychological effects".[9] Following this comparison, they call for a doctrine of cyber-deterrence. Moreover, General Kevin Chilton, the head of US Strategic Command, supports the idea of a combined deterrence based on nuclear weapons, missile defense systems, and cyberwarfare capabilities.

In a US Air Force journal, Chilton wrote that "the deterrence impacts of such uncertainty over the potential impacts of a cyberspace attack would be a function of the nature of the attacker's goals and objectives. A competitor's concerns about unintended consequences could enhance the effects of our deterrence activities if it wishes to control escalation or fears blowback from its cyberspace operations".[10] This fairly resembles the Cold War's MAD (Mutually Assured Destruction) doctrine. Originally emerging at the end of the Kennedy administration, MAD was a doctrine that assured that a full-scale use of nuclear weapons by two opposing sides would effectively result in the destruction of both the attacker and the defender.[11] Can such an argument be replicated into cyberspace? So far, it is hardly conceivable.

As a matter of fact, one year prior to Chilton's article, a suggestion from a US military officer was already raising similar questions. In May 2008, Colonel Charles Williamson from the US Air Force

wrote a widely criticized article in the *Armed Forces Journal* on the potential build-up of military botnets that could be used for offensive purposes.[12] For Williamson,

> America needs a network that can project power by building an af.mil robot network (botnet) that can direct such massive amounts of traffic to target computers that they can no longer communicate and become no more useful to our adversaries than hunks of metal and plastic. America needs the ability to carpet bomb in cyberspace to create the deterrent we lack.[13]

In other words, Williamson was not only acknowledging an on-going arms race in cyberspace, he was advocating it. But Williamson was only adding another argument to the idea that cyberspace in itself is a new and separate domain of warfare. This idea had grown in earnest several months before his article, when Estonia experienced cyberattacks against its governmental servers. Following the attacks, the US Secretary of the Air Force, Michael Wynne, stated that "Russia, our Cold War nemesis, seems to have been the first to engage in cyber warfare".[14] Jaak Aaviksoo, Estonian Minister of Defense, went further, evoking "the first unnoticed third world war".[15]

But even while these voices are urging for a new posture toward cyberwarfare, skeptical voices—among them Howard Schmidt, the current Cybersecurity Coordinator for the Obama Administration—are vigorously opposing their conclusions. Although such thinkers recognize the need for improving information system security, they understand the concept of cyberwarfare as deeply flawed. For instance, Schmidt stated during an interview at the RSA Security Conference in San Francisco in March 2010: "There is no cyberwar [...] I think that is a terrible metaphor and I think that is a terrible concept".[16]

All in all, both postures (the alarmist and the skeptical) fuel the debate in Washington, both in the government and in think tanks. This rift has two consequences: first, the US military still remains uncertain precisely what cyberwarfare, cyberconflict or, indeed, any other term given to describe the political use of attacks in the cyberspace actually stands for. Second, this tension logically affects the credibility of the national security architecture, leading to official disagreements on the threat level (e.g. Howard Schmidt stating publicly that 'there is no cyberwar'[17]) or even interservice rivalries (the Air Force having claimed since 2005 to be the one to 'fly and fight in cyberspace'[18]). But the rift between these two antagonistic views can and should be overcome. This is the aim of the next two sections, starting with how the confusion is produced by two analogies—nuclear warfare and strategic bombing—that too often frame the debate on cyber military policies.

The problems of current analogies for cyberwarfare

Balancing the equation between the alarmists and the skeptics of cyber-threats requires a critical examination of the terms of the debate, and more specifically of the frequently used analogies. The study of new phenomena in international affairs is often dependent on analogical reasoning. Analogies provide guideposts on the assumption that new issues can be understood within the framework of older, more familiar ones. Regarding cyberspace, two analogies have been extensively used, both explicitly and implicitly: cyberwarfare as nuclear warfare, and cyberwarfare as strategic bombing. Each is misleading.

The analogy with nuclear warfare is often used to emphasize the low level of existing knowledge on the strategic implications of cyberattacks. Within that logic, the same could be said of the early nuclear literature published in the 1950s and 1960s. At that time, no one denied the potentialities of

nuclear weapons, as they were dramatically demonstrated at Hiroshima and Nagasaki. But equally, no one could accurately appraise how nuclear forces and their diffusion would alter the balance of power in the context of the Cold War. It took years and some risky and bold analysis from Bernard Brodie, Herman Kahn, and Albert Wohlstetter to build a more coherent understanding of nuclear strategy.[19] People needed to "think the unthinkable", to cycle through numerous ideas and concepts in order to finally build a coherent intellectual framework for nuclear policy analysis.[20]

The comparison with cyberwarfare, however, cannot be stretched further. While nuclear weapons remain the single most lethal asset available to armed forces, in terms of military applications, cyberattacks do not have any direct lethal effect. In terms of force employment, the cyberattacks perpetrated in recent years have tended to be used in support of combined operations (the Russia-Georgia war of 2008) with low-intensity effects, or to achieve a modest political outcome (the intimidation of Estonia in 2007). By contrast, nuclear warfare—at least since the widespread acceptance of the MAD doctrine—has been understood to carry the real risk of escalation to a Clausewitzian absolute conflict that shifts the strategic calculus of conventional warfare. Deterrence in the nuclear field is relevant because of its absolute character. Cyberattacks can disrupt the command and control systems of an enemy, but they do not annihilate his population.

Furthermore, computer scientists underline that technical limitations prevent the victim of a cyberattack from identifying their attacker in cyberspace, which results in an inability to deter a potentially anonymous aggressor. Indeed, with the current state of technology, cyberattacks deny the technological possibility to trace their origins. The use of botnets implies the hijacking of computers that can be located in other countries, or even on other continents. Therefore, authorities do not have any certainty with which to attribute an attack to a terrorist organization or to a state. For instance, cyberattacks on Estonia in spring 2007 were partly originating from computers physically located in California. Therefore, for all these reasons, cyberattacks can barely be compared to nuclear strikes.

The second analogy refers to strategic bombing, a theory of coercion based on the exploitation of massive air attacks that emerged at the end of the First World War and that has, for much of the period since, constituted a dogma of the US Air Force in its claims for the independent effectiveness of airpower. As Caroline Ziemke wryly observed: "Strategic bombing is not mere doctrine to the USAF; it is its lifeblood and provides its entire *raison d'être*. Strategic bombing is as central to the identity of the Air Force as the New Testament is to the Catholic Church".[21] In other words, the fact that strategic bombing is USAF's *raison d'être* demonstrates how the US armed forces can acquire technological obsessions as a product of their strategic culture, even when the empirical evidence does not systematically support their position.

The presumed similarity between cyberattacks and strategic bombing has already led several pundits to argue for an explicit cyberpower doctrine, recalling directly the long and intractable debate over the independent effects of airpower.[22] Institutionally, this analogy can be explained as a product of the US Air Force's sunk investment in cyberspace expertise. But more particularly, this analogy emphasizes the persistently technology-centered nature of US strategic culture.[23]

In other words, the analogy is based on the idea that technological capabilities (whether air strikes or cyberattacks) can compel the enemy to do our will without ever launching a massive and costly ground offensive.[24] But in spite of certain thinkers' enduring faith, there is little evidence that strategic bombing has ever decisively determined victory in war.[25] Regarding cyberattacks, there is even less proof that they have been decisive in any military context.

The best example of this misleading analogy is the contemporary debate surrounding the Stuxnet attack against the Iranian uranium-enrichment plant in Natanz. After rumors spreading in the summer of 2010, the authorities in Tehran acknowledged in November that the control systems of its nuclear facilities had been targeted by a cyberattack that caused significant physical damage. There is clear evidence from the reports issued by the International Atomic Energy Agency that the cyberattacks targeting the centrifuges delayed for about a week Iran's nuclear program. Nevertheless, Stuxnet did not decisively stop Tehran's ambition, it only hindered the pace of its fulfilment.[26] Thus, the exaggerated statements on Stuxnet and the advent of cyberwar *per se* come from this same belief about strategic bombing and its decisiveness.

Consequently the analogy is not applicable, not strictly because cyberattacks lack the lethality of air strikes (they actually could resemble air strikes in terms of disruptive effects), but because the analogy is biased by the fundamental assumption that strategic bombing can be decisive and so cyberattacks could as well.

Although the errors vary for the respective different comparisons with nuclear warfare or strategic bombing, one common conclusion can be drawn: as of today, cyberattacks do not amount to a distinct field of warfare with its own rules and processes. Both analogies should therefore be avoided if we are to get the conceptual framework for the analysis of cyberattacks right. Therefore, we need to strictly understand the history of the phenomenon within the context of military operations.

A middle way for a military posture in cyberspace

The political science literature dedicated to campaign analysis can provide precious insights on how to articulate a robust strategic analysis of cyberattacks that avoids both the fads of "cyberwarmongers" and the reductionist arguments of "cyberskepticals". Campaign analysis looks at the operational level of military activity by combining an appraisal of the objectives, the military balance (quantity, quality, joint capabilities), the terrain, the duration of the campaign and its evolution (breakthrough, maneuver).[27] Going beyond a simple compilation of military resources and technologies, this methodology allows us to get a better grasp of how these assets are used *during* the campaign, what Stephen Biddle calls the "force employment" factor.[28]

So far, campaign analysis has rarely looked at cyberattacks. The most obvious reason is the lack of sufficient available data (due to the classification issue) that would be needed. Nevertheless, based on the first lessons learned from the cyberattacks released to the public (mostly about the Estonian and the Georgian cases), cyberwarfare cannot be described as an independent field of warfare. There cannot be war in cyberspace like there are instances of wars in the air, on the seas, or on land. Cyberattacks can only be conceived as a component by-product of a larger military campaign. In other words, a cyberconflict has to be defined as a proxy conflict aimed at attaining an intermediate goal for an attacker, thereby functioning as a subsidiary addition to conventional kinetic military operations. Cyberattacks are means of denial, not of punishment: they can block an enemy's ability to use its information systems as part of their war effort, but they are rarely designed to achieve political outcomes in their own right by inflicting an unbearable cost on the defender.[29]

On that matter, the lessons learned from the cybercampaign against Georgia during the war in Russia in August 2008 are instructive. Georgia experienced early cyberattacks in late July, including an attack on the presidential website on July 19. Due to a distributed denial of service attack, the

website remained unavailable for twenty-four hours.[30] After a two week pause, cyberattacks targeting Georgian government and media websites started by late August 7 following President Mikheil Saakashvili's decision to attack South Ossetian separatist forces that night. But the wave of attacks substantially increased on August 8, the day the Russian armed forces entered Georgia, when cyberwarriors began to block and deny access to Georgian govermental websites, and moved on to expand the list of targets to include financial institutions.[31]

Experts from the US Cyber Consequences Unit (US CCCU) surmised that the attackers were civilians recruited through electronic social networks. However, more significantly, the authors of the report concluded that there was a clear convergence between the Russian armed forces' campaign and the hackers' actions: "The organizers of the cyber attacks had advance notice of Russian military intentions, and they were tipped off about the timing of the Russian military operations while these operations were being carried out".[32] Consequently, this illustrative case of cyberwarfare clearly demonstrates the integration of such practices into a larger military campaign. By themselves, cyberattacks function as proxy components of a strategic offensive. Indeed, one could argue that the use of cyberattacks during the conflict between Russia and Georgia pointed away from the use of autonomous cyberwarfare in itself, and instead illustrated that there are combined operations that can exploit cyberattacks in the same way that theater air campaigns have been performed for decades.

Interestingly, this also happens to be the way that Chinese strategists conceive the exploitation of cyberspace. In spite of misleading speculations regarding Chinese capabilities (mainly a consequence of the alarm generated by the best-selling book *Unrestricted Warfare*, written in 1999 by PLA colonels Qiao Liang and Wang Xiangsui), the People's Liberation Army (PLA) does not conceive cyberspace as an autonomous military domain.[33] Rather, the Chinese military has explicitly adopted a posture including the concept of "integrated network electronic warfare", which aims at controlling the flow of information in the adversary's system and at maintaining the PLA's information superiority on a traditional, physical battlefield. Moreover, the seminal Chinese documents, *The Science of Military Strategy* and *The Science of Campaigns*, both underline the decisive role of information superiority in air and sea warfare.[34] Such strategic thought clearly integrates cyberattacks into classic military campaigns. In short, even thinkers in the United States' principal future great power rival only see cyber as a subcomponent of modern conventional conflicts.

In spite of all the political exaggerations regarding cyberwarfare, modern cases (Estonia in 2007, Georgia in 2008, the revelations over a so-called 'GhostNet' operating against Tibetan authorities) display evidence that there are no truly independent or even autonomous cyberwars *per se*.[35] In all of these instances, cyberattacks were a component by-product of a larger campaign (political intimidation in the Estonian and Tibetan cases, military intervention in the Georgian case).

As a result, our assessment renders debate on the future of deterrence in cyberspace irrelevant. Of course, this does not mean that hackers cannot inflict significant damage that could severely disrupt the vital infrastructure of a country but so too, still, could bombers and tanks. Even worst-case scenarios involving cyberattacks do not suggest that the United States or other major powers could be severely coerced, let alone existentially threatened, by such cyberattacks alone.

The belief that disruptions in cyberspace could defeat a country is flawed—and dangerous. The idea that cyberwarriors could become the principal combatants of a future war without physical implications remains science fiction *à la* William Gibson. It might be the role of strategic futurists to explore such narratives, but policy-makers that need to base analysis on present-day objective facts have to acknowledge this evidence: taking into account recent international events and known

technological trends, cyberattacks cannot be compared to nuclear warfare. The actual analogy that should be explored, if such analogical reasoning is cognitively necessary to conceptualize and understand the emergence of cyberattacks, is electronic warfare. It may be less strategic and more technical, but it is also more relevant.

◆ ◆ ◆

Policy-makers and military planners should neither overestimate the strategic scope nor underestimate the operational effectiveness of cyberattacks. The protracted battle over their significance has not only intellectual implications but policy ones as well. The inability of the Obama administration to bridge this decade-long gap between these two distinct views of cyber-defense extends the institutional dysfunction into the current system. Alarmists and skeptics are dispersed in all levels of the chain of command (in the White House, the Department of Homeland Security, the Department of Defense, the National Security Agency or the Department of State) without anyone prevailing. As a result, final decisions are still taken as a product of bureaucratic tactics, rather than on the back of cautious strategic threat-assessment.[36]

Therefore, getting the strategic appraisal right should be the priority when designing the relevant military posture. As I explained in this article, there is a middle ground between dismissing the military significance of cyberattacks and overestimating their reach. Cyberattacks certainly represent a cost-effective tool to support classic land, sea and air campaigns, and consequently their military added-value should be assessed in the context of joint operations. But they do not represent a new and revolutionary class of military operation in their own right.

In the coming years, the challenge will be precisely to measure this added-value, whether in offense or in defense, and at both the national armed forces level and the joint international level. Policy makers and strategic analysts should then increase their efforts on the exploitation of two techniques helpful to adapt a military posture in cyberspace:

- First, thorough campaign analysis of recent cyberattacks can provide precious assessments of the "force employment" factor in cyberspace and its effectiveness on the battlefield. It will permit the US military to shift its focus from cybertechnology as the decisive assets to a posture based on an optimal exploitation of these weapons in the context of combined operations to achieve strategic objectives;

- Second, scenario-based exercises should look at how US armed forces can operate in a *degraded* cyber environment.[37] Exploring specific contingencies where cyberattacks would disrupt the conduct of an operation, these exercises should not only involve national servicemen but also the militaries from NATO members as well as from traditional allies (Japan, South Korea). This will provide new evidence and ideas on how to integrate these engagements as an additional contributory element to a broader military campaign.[38]

This adaptation process could well represent the key to both defensive resilience and offensive edge when confronting future cyber-threats.

About the Author

Jean-Loup Samaan is a policy advisor at the French Ministry of Defense (Directorate for Strategic Affairs) and an adjunct lecturer in international security at the French Institute for Political Studies, Sciences Po. A former visiting scholar at the RAND Corporation and Duke University, he holds a PhD in Political Science from the University of Paris. The views expressed in this article are his only, and do not necessarily reflect those of the French government.

Notes

1 Alvin Toffler, *The Third Wave*, (New York, NY: Bantam Books, 1980).

2 Richard Szafranski, 'Neocortical Warfare? The acme of skill' in John Arquilla, David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, (Santa Monica CA: RAND Corporation, 1997), pp.395-416.

3 Although the term was initially conceived by Thomas Rona in a corporate document from the Boeing Company, in 1973. See Thomas P. Rona, *Weapon Systems and Information War*, (Seattle, WA: Boeing Aerospace Co., 1976).

4 John Arquilla, David Ronfeldt, 'Cyberwar is Coming!', *Comparative Strategy*, (Vol.12, No.2, Spring 1993), pp.141-165.

5 William Gibson, *Neuromancer*, (New York: NY, Ace Hardcover, 1994).

6 Laurent Murawiec, *Aristotle in Cyberspace: toward a theory of information warfare*, (Santa Monica, CA: RAND Corporation, 2001), p.26.

7 Richard Clarke, Robert Knake, *Cyberwar: The Next Threat to National Security and What to Do About It*, (New York: NY, HarperCollins, 2010), p. 31.

8 Mike McConnell, 'How to win the cyberwar we're losing', *Washington Post,* 28 February 2010.

9 *Ibid.*

10 Kevin Chilton, Greg Weaver, 'Waging Deterrence in the Twenty-First Century', *Strategic Studies Quarterly*, (Vol.1, No.3, Spring 2009), p.40.

11 Among others, Alan Parrington, 'Mutually Assured Destruction Revisited: Strategic Doctrine in Question', *Airpower Journal*, winter 1997; Henry Sokolski, *Getting Mad: Nuclear Mutual Assured Destruction, its Origins and Practice*, Strategic Studies Institute, 2004.

12 Charles Williamson, 'Carpet bombing in Cyberspace', *Armed Forces Journal*, May 2008.

13 *Ibid.*

14 Rebecca Grant, *Victory in Cyberspace*, Air Force Association, 2007.

15 Estonian Ministry of Defense news release, 'Internet : XXI Century Battlefield', 16 June 2007.

16 Ryan Singel, 'White House Cyber Czar: There Is No Cyberwar', *Wired.com*, 4 March 2010. Accessed 6 0ctober 2010. http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/

17 Ryan Singel, "White House Cyber Czar: 'There Is No Cyberwar'", *Wired*, 4 March 2010.

18 See Sebastian Convertino, Lou Anne DeMattei, Tammy Knierim, *Flying and Fighting in Cyberspace*, (Alabama, Air War

College, Maxwell Paper No.40, 2007).

[19] Fred Kaplan, *The Wizards of Armageddon*, (New York, NY: Simon and Schuster, 1983).

[20] Herman Kahn, *Thinking about the Unthinkable*, (New York, NY: Horizon Press, 1962).

[21] Caroline Ziemke, 'Foreword' in TILFORD Earl, *Setup: What the Air Force Did in Vietnam and Why*, (Maxwell, Air University Press, 1991), p. ix.

[22] See Rebecca Grant, *Victory in Cyberspace*; Frank Kramer, Stuart Starr, Larry Wentz, *Cyberpower and National Security*, (Washington D.C.: NDU Press, 2009).

[23] On this debate, see Russell Weigley, *The American Way of War: A History of United States Military Strategy and Policy*, (Indiana: IN, Indiana University Press, 1977); Antulio Echevarria, *Toward An American Way of War*, (Washington, Strategic Studies Institute Monograph, 2004); Colin Gray, *Irregular Ennemies and the Essence of Strategy: Can the American Way of War Adapt ?*, (Washington, Strategic Studies Institute Monograph, 2006); Arthur Cebrowksi, Thomas Barnett, 'The American Way of War', *Proceedings*, January 2003.

[24] On this belief, see the literature following the Desert Storm campaign: Christopher Bowie, David Ochmanek, Fred Frostic, Kevin Lewis, John Lund, Philip Propper, *The New Calculus: Analyzing Airpower's changing role in joint theater campaigns*, Santa Monica, RAND Corporation, 1993; Eliot Cohen, 'The Mystique of U.S. Air Power', *Foreign Affairs*, (Vol.73, No.1, 1994);

[25] See Robert Pape, *Bombing to Win: Air Power and Coercion in War*, (Ithaca: NY, Cornell University Press), 1996 and one of its critics, Barry Watts, 'Ignoring reality: Problems of theory and evidence in security studies', *Security Studies*, (Vol 7, No.2., Winter 1997-1998), pp. 115-171

[26] On the assessment of the Stuxnet attacks, see International Institute for Strategic Studies, "Stuxnet: targeting Iran's nuclear programme", Strategic Comments, February 2011; James Farwell, Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival*, (Vol.53, No. 1, February-March 2011), pp.23-40; Isaac Porche, "Stuxnet is the world's problem", *Bulletin of the Atomic Scientists*, 9 December 2010; Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier*, Symantec, February 2011.

[27] Among others, see John J. Mearsheimer, "Why the Soviets Can't Win Quickly in Central Europe," *International Security*, (Vol. 7, No. 1, Summer 1982), pp.139-175; Barry R. Posen, *Inadvertent Escalation*, (Ithaca, N.Y.: Cornell University Press), pp. 68-128.

[28] See Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle*, (Princetion : NJ, Princeton University Press, 2004).

[29] See for instance the distinction made by Martin Libicki between strategic cyberattack and operational cyberattack while exploring the scenarios of a China-US contingency in Martin Libicki, *Chinese Use of Cyberwar as an Anti-Access Strategy*, (Santa Monica, CA: RAND Corporation), January 2011.

[30] Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, Liis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified*, Cooperative Cyber Defence Centre of Excellence, Estonia, 2008, p.36.

[31] Ronald Asmus, *A Little War That Shook The World*, (New York, N.Y.: Palgrave, 2010), p.166; John Bumgarner, Scott Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia In August of 2008*, US-CCU Special Report, US Department of Defense, August 2009, p.5.

[32] Bumgarner, Borg, *Overview by the US-CCU*, p.3.

[33] Qiao Liang, Wang Xiangsui, *Unrestricted Warfare*, (Panama, Pan American Publishing Company, 2002).

[34] Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*,

Report from Northrop Grumman to the US-China Economic and Security Review Commission, October 2009, pp.6-7; Gurmeet Kanwal, 'China's Emerging Cyber War Doctrine', *Journal of Defence Studies*, (Vol.3, No.3, July 2009), pp. 14-22.

[35] Information Warfare Monitor, *Tracking Ghostnet : Investigating a Cyberespionnage Network*, March 2009.

[36] For a cautious analysis of the US reforms in cyberdefense, see CSIS Commission on Cybersecurity for the 44th Presidency, *Cybersecurity Two Years Later*, (Washington: DC, Center for Strategic and International Studies), February 2011.

[37] Noticeably, the new *US National Military Strategy* released in February 2011 acknowledges the need to better apprehend the conduct of operations in "degraded environments".

[38] An illustration of such valuable scenarios is provided by Martin Libicki, *Chinese Use of Cyberwar as an Anti-Access Strategy: Two Scenarios*, (Santa Monica: CA, RAND Corporation, 2011).