Defense Horizons
Number 68
A publication of the
Center for Technology and National Security Policy
National Defense University
September 2009

Cyberspace and the "First Battle" in 21st-century War

by Robert A. Miller and Daniel T. Kuehl

Overview

Wars often start well before main forces engage. In the 19th and early 20th centuries, combat often began when light cavalry units crossed the border. For most of the 20th century, the "first battle" typically involved dawn surprise attacks, usually delivered by air forces.[1] While a few of these attacks were so shattering that they essentially decided the outcome of the struggle or at least dramatically shaped its course—the Israeli air force's attack at the opening of the June 1967 Six-Day War comes to mind—in most cases the defender had sufficient strategic space—geographic and/or temporal—to recover and eventually redress the strategic balance to emerge victorious. The opening moments of World War II for Russia and the United States provide two examples.

The first battle in the 21st century, however, may well be in cyberspace.[2] Coordinated cyber attacks designed to shape the larger battlespace and influence a wide range of forces and levers of power may become the key feature of the next war. Early forms of this may have already been seen in Estonia and Georgia. Control of cyberspace may thus be as decisive in the network-dependent early 21st century as control of the air was for most of the 20th century.

In the future, cyber attacks may be combined with other means to inflict paralyzing damage to a nation's critical infrastructure as well as psychological operations designed to create fear, uncertainty, and doubt, a concept we refer to as *infrastructure and information operations*. The cyber sphere itself is, of course, a critical warfighting domain that hosts countless information infrastructures, but the rise of network-based control systems in areas as diverse as the power grid and logistics has widened the threat posed by network attacks on opposing infrastructures.

Given the increasing dependence of the U.S. military and society on critical infrastructures, this cyber-based first battle is one that we cannot afford to lose. And yet we might.

First Battles in American History

Historically, time and space to recover have often proven essential in overcoming losses in an opening battle. The United States frequently has fared poorly in the opening battles of past conventional wars—the other side, usually authoritarian or totalitarian, spends more time preparing the initial blow. As Charles Heller and Bill Stofft point out in their classic study of America's first battles, there's a pattern here.[3] In many cases, especially those in which the United States was engaged with a technologically advanced peer competitor, our first engagements have been disastrous. Only because America had sufficient (sometimes barely sufficient) strategic space—geographic and/or temporal depth—were we able to recover from our first defeats.

World War II provides examples across all three of that war's operational domains and with several combatants in different theaters. At sea, our initial efforts at submarine and carrier warfare, which became indispensable components of our victory in the Pacific, were hesitant and marked by faulty equipment, ineffective doctrine, and a steep learning curve for personnel.[4] In the air, we discovered that one of the keystones of our prewar airpower doctrine—the efficacy of unescorted precision strategic bombing—was sadly in error, and the lack of fighter escorts for our bombers in 1943 cost us hundreds of bombers and thousands of crewmen. It was not until 1944 that German exhaustion and the arrival of the P–51 gave us air superiority in Europe, without which the victories of 1944–1945 would have been simply impossible. On land, our initial encounters with the Wehrmacht went poorly, as shown by the disaster at Kasserine Pass and the difficulties encountered throughout the North African and Italian campaigns. Not until the advance across France in the summer of 1944

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyberspace and the 'First Battle' in 21st-century Was (Defense Horizons, Number 68, September 2009)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Center for Technology and National Security Policy,300 5th Avenue SW,Washington,DC,20319-5066**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**6**	

did our skill at conducting combined arms maneuver warfare begin to match that of our German adversary. In all three examples, the time gap between the opening failures and the eventual victories was measured in months to years.

Even today, as we have most recently seen in Iraq, it has taken time and many casualties to change course and implement a strategy based on what seems to be more effective counterinsurgency principles.

We have been lucky to have had the time, space, and resources to correct these early problems. The question we face now is whether our luck will continue to hold in different operational conditions of the cyber age. Will that all-important time gap between early defeats and final victory be there for us now and in the future if we are faced with an enemy who is adept in and has planned for warfighting in the emerging fifth dimension of cyberspace, and who has avoided self-imposed and organizationally and programmatically based constraints on its operational concept for cyberspace operations?[5] The Chinese, for example, have been writing since the 1990s about the evolving "networked and informationized" battlefield, and one gains a clear sense that their approach to cyberwarfare is different than U.S. concepts.

Evolving Threats

Twentieth-century warfare was dominated by mass struggles of so-called conventional forces, created and sustained by the productive power of the industrial state and shadowed by the specter of weapons of mass destruction. The mushroom cloud and carpet bombing were its symbols, set-piece battles between symmetrically conceived forces its hallmark.

These 20th-century images have not yet left us, but they have been joined by new apparitions. The most visible, of course, is the kind of struggle that U.S. forces now find themselves fighting in Iraq and Afghanistan. Half war and half pacification campaign, these fierce struggles would once have been called "low intensity conflicts" or (more distantly) "irregular campaigns." No longer.[6]

But while our attention has been fixed on the conflicts in the Middle East, a different kind of national security threat has also emerged in recent years.

Military forces since time immemorial have tried to confuse their enemies and disrupt their plans, cut their communications, and throw them off balance.[7] However, the advent of the cyber age has changed things in some significant ways. Two factors increase the stakes of the cyber struggle. Tactically and operationally, the increasing dependence of modern technologically advanced forces (especially U.S. forces) on networks and information systems create new kinds of exploitable vulnerabilities. Second, as modern societies—including the militaries that mirror them—have continued to evolve, they have become ever more dependent on a series of interconnected, increasingly vulnerable "critical infrastructures" for their effective functioning. These infrastructures not only have significantly increased the day-to-day efficiency of almost every part of our society, but they have also introduced new kinds of vulnerabilities. The increasing exposure of nations such as the United States to well-coordinated attacks on critical infrastructures creates a situation that we have labeled "strategic fragility."[8] The evolution of Russian strategic thinking throughout the 1980s and 1990s incorporated the potential to degrade national economic systems and communications networks as a means of breaking the enemy's will to resist and inflicting military and political defeat, at low cost and without the need to occupy territory.[9]

These interconnected and interdependent infrastructures represent new kinds of strategic targets. Take them down, and societies are effectively paralyzed. And yet successful action against them does not depend, as it once would have, on massive destruction of the physical infrastructure. In many cases, effective paralysis can be achieved by other cheaper and subtler means. In short, it is now possible to create chaos without carnage, disruption without destruction.[10]

"Weapons of Mass Disruption"

The chances of creating nondestructive chaos have been immeasurably increased by a second, related development—the increased dependence of the other infrastructures on the information infrastructure as a control mechanism. Most of the critical infrastructures that daily life relies on—electricity, communications, money, and transportation, to cite just four—now use cyberspace and the Internet to exchange information and directions. If this traffic, or the underlying data that are transmitted, is interrupted or tampered with, confusion and disorder will quickly break out.[11]

Attacks on the cyber infrastructure are one variant of what the military refers to as "information operations," and these attacks have been going on in one form or another for some years now.[12] So far, however, they have been in the nature of probes rather than strategic attacks designed to disable major infrastructures or affect the overall balance of military forces.[13] In the one case in which actual conflict included cyber activity—Russia's operations against Georgia in 2008—the Georgian infrastructure was simply not sufficiently sophisticated to be vulnerable to a cyber attack.[14]

We think that this is about to change.

The Opening Shot

It seems increasingly probable that the first battles in any future conflict involving technologically advanced adversaries will be electronic and waged in/via cyberspace.[15] Strategic cyber attacks will likely have multiple objectives:

- to disrupt enemy communications and supply lines
- to distract and confuse enemy command and control
- to impair the movement of military forces
- to create opportunities for strategic attacks on enemy infrastructures
- to deny similar capabilities to the enemy
- to weaken and distract social cohesion and political will, perhaps even before the conventional start of a conflict
- to shape global perceptions of the conflict.

First battle cyber attacks are likely to use a combination of approaches. These could include attempts to deny services critical to military capability, from logistics support to actual warfighting systems, and might include rapid, coordinated attacks to deny network connectivity. Attacks that deny data are the most obvious use of

Dr. Robert A. Miller and Dr. Daniel T. Kuehl are Professors in the Information Resources Management College at the National Defense University. They can be reached at millerr@ndu.edu and kuehld@ndu.edu.

the new capabilities. Additionally, because of our heavy and growing dependence on what can be termed *dual-use infrastructures*—those owned and operated by the private sector that both society itself and military forces depend on for daily functioning of critical capabilities—the target of those attacks may not be prepared or resourced to withstand the kind of pressure that could be brought to bear by a coordinated and nation-state–sponsored series of attacks. A potential target list might include:[16]

- telecommunications
- space-based sensors and relays
- automated aids to financial and banking networks
- power production and distribution
- media to shape public perceptions.

In addition, we may also see attempts to manipulate the content of stored information through such means as injecting spurious information (attacks on data integrity). Modern military forces, and modern societies in general, rely on large databases of information that are essential for daily life and effective operations. If these databases become unreliable, the likely result is bedlam. So we should also expect to see attempts to reduce the adversary's confidence in the reliability of his networks and systems (attacks on confidentiality). As one senior Air Force leader observed at a symposium hosted at Air University in July 2008, the threat of data denial was much less worrisome than that of data manipulation.[17] Evidence of this threat extends as far back as Operation *Desert Shield*, the logistics and force deployment buildup to Operation *Desert Storm*, during which the intrusions into nearly three dozen American computer networks and databases by the so-called Dutch Hackers forced the delay of elements of the deployment because of the necessity to verify the contents of the databases that had been affected.

While the cyber events in Estonia (2007) and Georgia (2008) may not have reached the level of cyberwar, the targeted functions in both countries bore striking similarity to those listed above. In Estonia, effects were felt across the financial and media sectors; in Georgia, the cyber effects were also accompanied by an actual shooting war, although the less developed state of Georgia's use of cyberspace limited the cyber impact.[18]

Estonia 2007/Georgia 2008

The past two summers have seen examples of what the future may hold, albeit on a less developed scale. In the spring of 2007, the world witnessed what may have been the first major cyber-based assault on a nation-state, one that was perhaps particularly vulnerable because of its heavy use of and dependence on cyberspace. Estonia, although a small and relatively lightly populated country (about 1.3 million, roughly the same as urban Stockholm, Sweden), is one of the most highly connected countries in the world; citizens often refer to their country as "eStonia." Both the public and private sectors are heavily dependent on cyberspace.

The details that caused the cyber incident are less important than what happened. To protest a perceived insult and injustice to Russia, someone launched a persistent but technologically simple distributed denial of service attack against a range of Estonian targets, coupled with some Web site defacements. Some were against the public sector (for example, Estonia's Parliament and Office of the President), while some were against key infrastructure elements in the private sector (banks, telecommunications, and media). The peak of the attacks came between May 4–8, 2007, but they did not present any technologically new features, and the largest ones presented all the signs of a botnet, whose use had been purchased for a limited and specified period of time. Estonian internal coordination and mitigation actions were successful in minimizing the impact of these assaults, and the perpetrators have never been identified. While the common belief is that the Russians did it, no one has ever been able to perform any digital forensics linking the attacks to the Russian government. Perhaps ethnic Russians who were displaying their anger using the new medium of cyberspace were to blame, but the only person formally charged with any offense was an Estonian.[19] While the incident prompted widespread and sometimes breathless "Cyberwarfare is Under Way!!" headlines, it had no impact on the Estonian military forces or national security apparatus. It was, however, a bit of a wakeup call.

That wakeup call was repeated even more loudly the following year, in August 2008, against the small country of Georgia, deep in the Caucasus region between Russia and Turkey/Iran to the south. But the differences between the Estonia situation and the one faced by Georgia were pronounced. Estonia is a heavily "wired" and connected society, whereas Georgia is at the opposite extreme.[20] The 2007 incident was completely cyber, except for some minor civil disturbances, and completely civilian, with no impact on Estonian military systems or sites. In Georgia, on the other hand, the cyber incidents went hand in hand with a significant conventional military operation by Russian forces, with rocket attacks into Georgian territory and an incursion by armored forces. Cyber actions against Georgian political leaders began well before the crisis blew up into military operations, with attacks on/defacement of Georgian President Mikheil Saakashvili's Web site 3 weeks before the start of combat operations. Because of Georgia's much lower use of (and thus lower dependence on) cyberspace for the control and use of key infrastructures, the cyber attacks conducted against Georgia concentrated primarily on blocking its ability to access the outside world and tell its side of the evolving story. Targets included President Saakashvili, the Foreign Ministry, and the Defense Ministry. Once again, claims that a second cyberwar was under way had to be measured against the unresolved question, "What is a cyberwar?"[21]

Both incidents raise a series of unanswered questions. What, for example, constitutes a sufficiently aggressive or damaging cyber event to involve the North Atlantic Treaty Organization? While most discussion has focused on Articles 4 (the need for consultation) and 5 (collective self defense against an "armed attack"), Article 6, which delineates what constitutes an "armed attack," seemingly limits that to actions against territory, forces, vessels, or aircraft. What are the limits and requirements for neutrality in cyberspace? Shortly after Russian tanks moved against Georgia and its governmental Web sites were defaced and taken over by unknown attackers, an ethnic Georgian expatriate in the United States who owned Tulip Systems in Atlanta began hosting the Georgian sites on Tulip servers. Since the legal status of the Russian-Georgian incident was unclear—was an "armed conflict" under way?—it cannot be firmly argued that Tulip violated any neutrality laws, but the question remains interesting.[22]

Given the potential stakes, it is worth speculating what a full-scale cyberwar would look like (see sidebar).

A Plausible Scenario?[1]

The opening phases of the Cyber War of 20XX began in ways that surprised most of the world, especially Lusitania's forces and its political/military leadership. Even before actual hostilities began, certain steps had been taken by the Ruritanians over the course of many months that culminated on X-Day with a rapidly unfolding series of cyber incidents. Even though Lusitania's cyber experts had been warning for months—indeed, years—that many of their critical national systems and infrastructures had been penetrated by unknown operatives, Lusitania's citizens were shocked to wake up on X-Day to find that for some reason, many of their basic infrastructures had either stopped functioning, had slowed to a crawl, or else were unreliable. Automatic bank tellers no longer worked, many media outlets went dark, and even the traffic lights often blinked out. The financial sector found that its trading floors were paralyzed.

The electricity blackouts started the first afternoon. Though not everywhere, rolling blackouts afflicted large parts of the country, but at no time did the entire country "go dark." Nobody knew why they started, or for that matter why they stopped, although everyone was certainly glad they did.

It actually took some time before the Lusitanians even realized that what was going on was not merely an unconnected series of glitches in the central nervous system. As the examination of the failures got under way, Lusitania's political and military leadership discovered other, even more disquieting problems. Supposedly secure logistics databases turned out to be unreliable—someone had fiddled with the data. Supervisory Control and Data Acquisition systems controlling the power grid and certain oil refineries and pipelines went on the blink; the energy infrastructure had suddenly become quite shaky. Further complicating the situation was the often discussed problem of attribution—just exactly *who* was doing this? Some of the intrusions were traced back to computers in Africa and South America, but others came from inside Lusitania itself. Without the confident ability to point a finger at someone, how would the Lusitanian cyber-security forces respond?[2]

Later that day, the problems afflicting the infrastructures mysteriously cleared up. Television and radio came back on and soon were filled with horror stories about the "collapse of the nation's infrastructures." Enterprising reporters soon found, and endlessly rebroadcast, film of chaos in the streets, most of it captured by "citizen journalists" using their cell phones and digital imaging devices. Bloggers and users of the new social networking systems soon amplified these stories (some were later found to have been false, planted by "parties unknown"), coupled with rumors about how the authorities were covering up even worse stories. Amid rising signs of confusion and incipient panic, law enforcement found that many of its communications assets were compromised as well.

Meanwhile, Lusitanian military forces, heavily dependent on network-centric capabilities, found that their communications were unreliable, and even worse, many of the databases needed for mobilization and force generation were untrustworthy. These problems worsened over the next 5 days, but it was on day six, "Y-day," that Ruritanian forces made their first overt moves against their small neighbor, Zenda, with whom tensions had reached a boiling point after years of nearly continuous confrontation. The same problems that Lusitania had been experiencing now exhibited themselves in Zenda's systems and networks, but far more extensively and destructively. Anything that supported Zenda's military forces and ability to defend itself, resist attack, and communicate with the outside world came under attack. What seemed to be a warning to Lusitania only a week earlier became a full-fledged assault against Zenda, whose populace, long fearing their much larger neighbor, began to panic.

The panic became full fledged on Y+1, when Ruritanian forces began to aggressively exploit the advantages provided by their cyber offensive by extending it into a powerful attack. Zenda's air defenses were negated due to a deeply flawed and completely inaccurate air picture, caused by a devastating intrusion into its computerized radar controls. Intrusions also severely degraded Zenda's view of its maritime approaches, which were totally unreliable. Zenda's efforts to prevent Ruritanian amphibious and airborne forces from occupying key sites were completely ineffective, and the Ruritanian cyber blockade, imposed by its virtual seizure of Internet access controls, led to a global news blackout at the most critical moment. The only scenes widely accessible to the world came via Ruritania, which provided a broad multimedia information offensive that consisted of crowds of supposed Zendans welcoming the Ruritanian forces while those same forces ensured that food, water, and medical care were readily available to the Zendan population.

Zenda used special communications links to appeal for help from Lusitania, but that effort ran into two formidable obstacles. One was an intense and broad-spectrum strategic communications and influence campaign that aimed at several objectives, especially to convince the world that Ruritania's offensive was legally and ethically justified and to convince the Lusitanian population that any misguided desire to aid Zenda was not worth the risks and potential severe costs of a wider conflict. Interestingly, most of the more direct efforts against Ruritania came from Zendan expatriates who quickly mounted a noisy, albeit uncoordinated and strategically ineffective, series of "patriotic hacking" efforts aimed at Ruritania, which had its own increasingly vulnerable cyber dependent infrastructures. For a while, these counter-network attacks only served to muddy the situational awareness of all parties until it became clear that the attackers had no government affiliations.

The other and far more important obstacle was a focused series of cyber attacks that sought to significantly degrade the Lusitanian military capability to generate and move forces, albeit for a limited time. The series of computer attacks experienced the previous week intensified and concentrated on those databases, networks, and systems necessary to support military efforts to aid Zenda. It was obvious that the groundwork and intelligence preparation for these attacks had been laid over the course of several years. Their targeting principles were cleverly designed to eliminate human casualties as much as possible, especially in the civil sector, and thus avoid provoking the Lusitanian population while simultaneously limiting Lusitania's military capability to intervene on behalf of Zenda until it was too late. Plans to mobilize reserve forces and initiate deployment operations had to be halted in the face of unreliable databases, broken communications links, and widespread infrastructure failures.[3]

And this was exactly how the scenario played itself out. Future historians would have ample ground to plow in exploring how the Ruritanians were able to exploit cyberspace as the decisive domain in this conflict. The Ruritanian campaign in Zenda was militarily complete within 4 days, and by Y+4, the Zendan government had not only capitulated but also agreed to the incorporation of Zenda as Ruritania's 33^{d} province; they were even allowed to remain in office to lead the process of incorporation. Casualties in Zenda had been remarkably light, in part due to Ruritania's disruption of Zendan military communications

and control capabilities, and Ruritania's strategic communications forces had been quick to show the rest of the world how little physical damage had been done and the popular acceptance of the new situation.

In Lusitania, the Ruritanians had cleverly combined their demonstrated yet understated threat to a wide range of national infrastructures with an attack that on the surface looked more like malfunctions than a long-planned and prepared military operation, at least not until it was long over. Furthermore, the suppression of rapid Lusitanian military action until after the Zendan campaign was over and the fact that intense diplomatic maneuvers and negotiations were under way meant that the Lusitanian government had to react to a fait accompli and a total change in the geopolitical situation from what had been the basis for all previous planning. Given the facts on the ground, it seemed clear that a war with Ruritania would likely accomplish nothing, and diplomacy soon returned the situation between Ruritania and Lusitania to what it was ante bellum.

Only after the situation was resolved was it was apparent that the first battle of this war had been waged in cyberspace, and the Ruritanians had won a decisive victory. Although Lusitanian military and cyber strategists had been calling attention to the writings and analysis of both Chinese and Russian information warfare theorists for nearly two decades, and had the experience of the Estonian and Georgian crises to provide real-world empirical evidence to validate the theories, the reality was worse than the predictions. Ruritanian joint and integrated kinetic and cyber operations against Zenda put into practice, on a grand scale, lessons and insights that should have been gained from the Russia-Georgia conflict. Meanwhile, the Ruritanians' precise and focused cyber operations against Lusitania generated real and critical military advantages while simultaneously avoiding the kind of apocalyptic society-wide damage that many theorists predicted.

Notes

[1] The protagonists in this futuristic scenario are not intended to represent any real countries or reflect current planning exercises, certainly not Russia, Georgia, and the United States.

[2] See Jason Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," in *Culture Mandala* 8, no. 1 (October 2008), 56, on the problems of attribution.

[3] Ibid., 69.

Information and Infrastructure Operations

In the 1990s, it became fashionable in American military circles to speak of a "revolution in military affairs," arising from a combination of technological breakthroughs, changes in the geopolitical balance due to the end of the Cold War and the collapse of the Soviet Union, and the growing conventional military superiority of the United States and its allies. As many theorists pointed out, all of these factors suggested that future conflicts—at least those involving U.S. forces—were likely to become "asymmetric," as others tried to figure out ways to counter U.S. predominance in conventional and nuclear military power.[23]

As we have seen in Iraq and Afghanistan—mirroring lessons learned from many previous insurgencies—lightly armed insurgents can have a considerable degree of success against conventional forces, especially if they use tools of the cyber age as force multipliers.

For the reasons discussed above, it seems likely that we are seeing the beginnings of a new kind of military operation, which could be referred to as information and infrastructure operations (I2O). I2O warfare could:

- combine with other types of operations
- be largely fought in cyberspace. Special operations and limited kinetic efforts directed at key infrastructure targets, single points of failure, and chokepoints are also likely.
- have strategic as well as operational/tactical goals
- offer important asymmetric advantages against a society/military dependent on networked systems and capabilities
- offer important advantages to the first mover. Combined with the relative ease of initiating such I2O, this provides powerful incentives to a hostile (or merely nervous) potential adversary to initiate actions.
- be limited through resilience strategies and, perhaps, be deterred by the development of retaliatory capabilities
- delay counter actions because of the inherent difficulty in obtaining high-confidence attribution of attacker identity
- drive other military forces to exploit cyber capabilities regardless of the United States doing so
- be decisive in achieving war aims.

Command and Control Issues

The U.S. Government, and particularly the military, has been paying increased attention to cyber threats in recent years.[24] As yet, however, much of this effort has seemed, at least from a distance, somehow dissociated from broader strategic and operational concerns—as if the cyber struggle will be confined to a series of "exploits" that will be pursued in their own realm with little contact with other events. In particular, the possibility of I2O as an element of a larger military and national security strategy has received little attention in the United States.

The Cyber Battle

We predict that in any future conflict, strategic infrastructures will be a major, and perhaps decisive, battleground, and I2O will be *the* critical set of operations in that battleground. We also expect that cyberspace will be the major theater for the conduct of such operations, if only because it offers a fast, relatively inexpensive, and effective way to assail and degrade critical but vulnerable infrastructures.[25]

As a consequence, we also expect that the struggle for cyberspace dominance will be a difficult one, fought at the beginning of hostilities

and probably begun long before. Since modern military operations have already become cyber dependent, and are rapidly increasing this dependence for operations and logistics, this cyber struggle for mastery will have significant consequences for a nation's ability to deploy, support, and fight, especially in a conflict of short duration aimed at focused and limited objectives. Winning that future *war*—defined in Clausewitzian terms as the attainment of strategic political objectives—thus may depend on successfully waging and winning the "first battle in cyberspace."

Notes

[1] Examples of the latter include the German attack on Poland in 1939, Japanese attack on Pearl Harbor, Israeli attack on Egypt at the start of the 1967 war, and coalition attack on Iraq in 1991, although the latter was a surprise only in a tactical sense.

[2] This is obviously a hypothetical construct because the 21st-century's first battles have already been waged in Afghanistan and elsewhere.

[3] Charles E. Heller and William A. Stofft, eds., *America's First Battles, 1776–1965* (Lawrence: University Press of Kansas, 1986).

[4] This was also true for early operations in the Battle of the Atlantic, during which U.S. shipping was so badly ravaged by German U-boats that their crews called this period (early 1942) the "happy times." However, a significant cause of this was the stubborn refusal of senior U.S. Navy leadership, especially Admiral Ernest King, to adopt the convoy system, rather than an across-the-board problem.

[5] The definition of *cyberspace* is still evolving. The Department of Defense uses the definition that originated with the Deputy Secretary of Defense in mid-2008 and has been codified into doctrine. *Cyberpower and National Security* (NDU Press and Potomac Books, 2009) offers a slightly different definition, emphasizing the role of the electromagnetic spectrum. The distinctions are more than merely semantic; how one defines an environment defines how one will use it.

[6] This is at the heart of the growing debate over the future direction of U.S. military doctrine and force structure. Secretary of Defense Robert Gates seems to emphasize irregular warfare as seen in Iraq and Afghanistan, while his sharpest critics seem to emphasize the need to be ready to fight the "big war" against a near/peer nation-state competitor. If both eventualities must be guarded against, can we afford both force structures? One of the axioms of military preparedness is that the next war will almost assuredly not look like the last war. If this is true, basing our preparedness for the next war on the insurgency/counterinsurgency model could be disastrous.

[7] If this sounds like the classic treatise on Chinese warfare by Sun Tzu, *The Art of War*, the resemblance is intentional. It also closely mirrors the Palestine Campaign waged by Field Marshal Edmund Allenby in 1918.

[8] See Robert A. Miller and Irving Lachow, Defense Horizons 59, *Strategic Fragility: Infrastructure Protection and National Security in the Cyber Age* (Washington, DC: NDU Press, 2008).

[9] Paul M. Joynal, "The Brave New World of the 5 Day War: Russia-Georgia Cyberwar, Where Cyber and Military Might Combined for War Fighting Advantage," available at <www.nationalstrategies.com/pdf/publicSafety_GovSec_5DayWar_Joyal.pdf>.

[10] For a somewhat dated but still useful examination of non-U.S. concepts and capabilities, see Charles Billo and Welton Chang, "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States" (Hanover, NH: Institute for Security Technology Studies, November 2004), which examines six countries' capabilities, including Russia and China.

[11] See Elgin M. Brunner and Manuel Suter, *International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Information Infrastructure Protection Policies* (Zurich: Centre for Security Studies, 2008). About every 2 years, this Swiss think tank publishes an extensive and thoroughly researched survey and analysis of national Critical Information Infrastructure Protection efforts. While each nation defines differently what constitutes a *critical infrastructure*, there are two that all 25 countries agree on: electricity and telecommunications.

[12] See Joint Publication 3–13, *Joint Doctrine for Information Operations*, for definitions of the various "core competencies" included under the umbrella of information operations.

[13] American practice distinguishes between computer network attacks and exploitation probes; the latter can be thought of as reconnaissance efforts looking for weak spots and trying for stray bits of useful information. Although the exact number, nature, and source of any of these efforts are classified, it is clear that their number and sophistication have steadily increased in recent years. As the U.S. military becomes more dependent on network-based operations, cyber attacks on it will inevitably become more attractive to others.

[14] Eneken Tikk et al., "Cyber Attacks Against Georgia: Legal Lessons Learned," presentation at the NATO Cooperative Cyber Defence Centre of Excellence, August 2008.

[15] Ibid. The timing of cyber actions, which occurred perhaps coincidentally with Russian military operations during the incursion into Georgia in the summer of 2008, suggests this possibility. Although Georgian military capability was in no way dependent on that nation's rather limited cyber-based infrastructures, Georgia's ability to inform the outside world of events there was certainly degraded.

[16] Joynal.

[17] This conference was hosted by Lieutenant General Robert Elder, then-commander of 8th Air Force, and included a panel led by Major General Bill Lord, then-commander of Air Force Cyber Command (Provisional).

[18] For an interesting discussion of the Estonian and Georgian situations, as well as an exploration of a notional future cyberwar scenario, see Andrew F. Krepinevich, *Deadly Scenarios: A Military Futurist Explores War in the 21st Century* (New York: Bantam Books, 2009), especially 232–237.

[19] Analysis taken from Eneken Tikk, "Cyber Attacks: Estonian Lessons Learned," presentation at the George Mason University Critical Infrastructure Protection Project, 2008; and Tikk, "Legal Lessons Learned from the Georgia and Estonia Events," *Cyber Warfare 2009*, London.

[20] While Estonia ranked 33d in the world in terms of Internet penetration with 57 percent, Georgia did not even register with only 8 percent penetration. See <www.internetworldstats.com/top25.htm>.

[21] Tikk et al.; and Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* 38, no. 4 (Winter 2008–2009).

[22] Korns and Kastenberg.

[23] This follows work done in the former Soviet Union in the 1980s on what had been termed the "military-technical revolution." Both seem to be responsible for much of the gene pool on which current concepts of "transformation" are based.

[24] The Obama administration creation of a task force on cyber security is evidence that this issue has reached the highest levels of the U.S. Government. The publication in early 2009 of two Chatham House studies—one focusing on "Cyberspace and the National Security of the United Kingdom," the other on "Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks," both edited by Paul Cornish—are evidence that the importance of this issue is recognized. Both reports are accessible at <www.chathamhouse.org.uk/research/security/>.

[25] A series of recent major U.S. strategy and policy documents have referred to cyberspace as a "theater of operations" and part of the "global commons," reflective of the growing realization that cyberspace is and will continue to be a vital, perhaps decisive, environment for military operations.

Defense Horizons *is published by the Center for Technology and National Security Policy. CTNSP publications are available online at http://www.ndu.edu/ctnsp/publications.html.*

The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Department of Defense or any other department or agency of the Federal Government.

Center for Technology and National Security Policy

Hans Binnendijk
Director