

DOI:10.1145/2001269.2001287

**Expect more cyberwarfare on the conventional battlefield and less against civilian infrastructure ...assuming containment is possible.**

BY JOHN ARQUILLA

# From Blitzkrieg to Bitskrieg: The Military Encounter with Computers

WARFARE IS NOT just a matter of hurling mass and energy at one's enemies; it is also about gaining an "information edge." In ancient times the emergence of writing allowed for battle orders that could guide subordinates at a distance, making possible greater operational complexity and enhancing the importance of skillful generalship. In the Middle Ages the Mongol Arrow Riders, a Pony-Express-like messenger system,

coordinated movement of armies across vast distances and contributed to the startling victories that created a "nomad empire" from East Asia to Central Europe. In the Napoleonic era, 1790–1815, the British Navy's Popham signaling system allowed transmission and receipt of more, and far more complex, information than opposing fleets could muster. During the period from the American Civil War through the German wars of unification and on to World War I, telegraphy supported the deployment choreography of masses of rail-mobile troops.

A generation later in World War II, maturing radio capabilities played a key role in coordinating the German armored blitzkrieg on land and the U-boat wolf packs at sea, the latter nearly starving Britain into submission. In that conflict, fast-moving panzer divisions and far-flung submarine squadrons, each guided to their objectives and commanded in battle from great distances, completely revolutionized fighting doctrine. Radio reports by spotter planes also played a key role in empowering aircraft-carrier operations, allowing some naval battles to be conducted without opposing ships ever coming into visual range of each other.

Early computers also debuted during World War II, helping enable breakthroughs in many areas, including ballistics, but made their most important contribution in codebreaking.

## » key insights

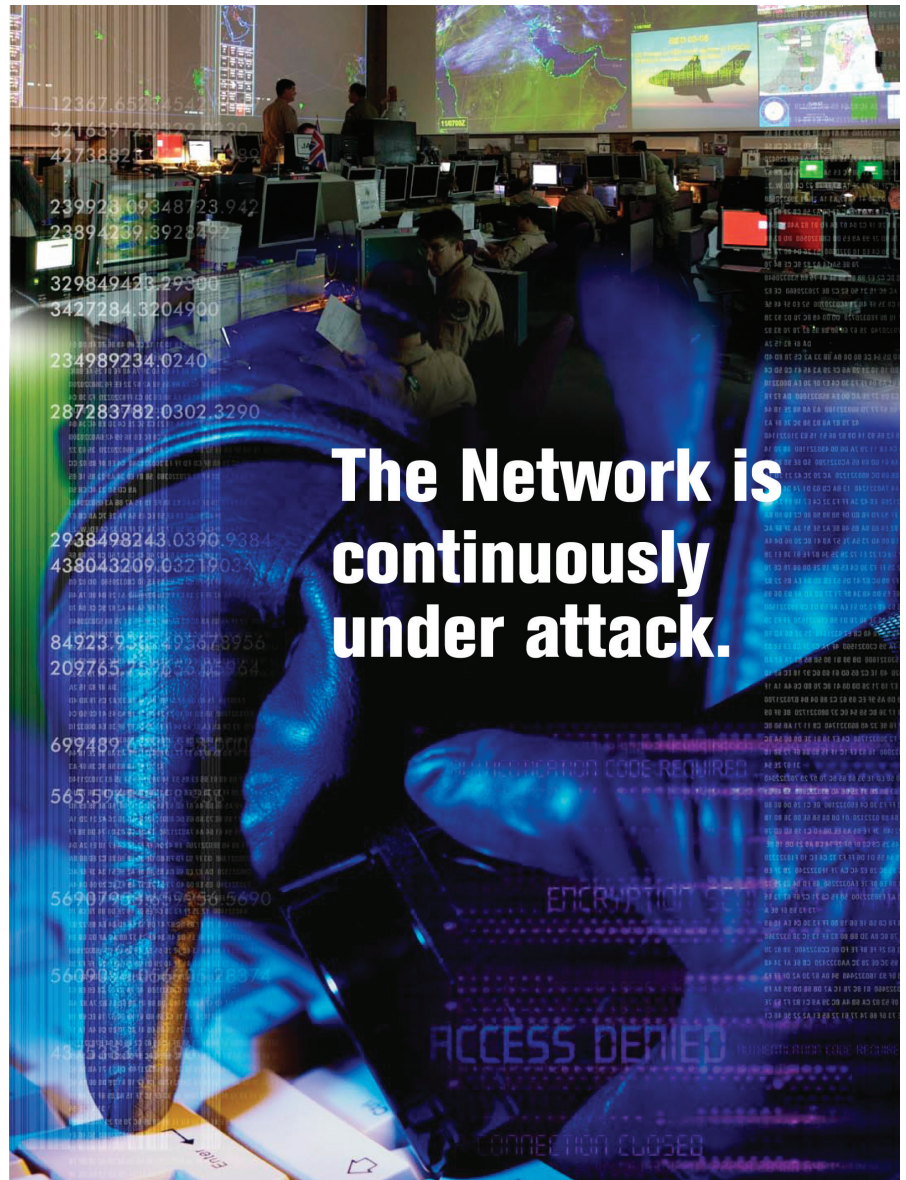
- **Militaries have been greatly empowered by a range of advanced information systems but are so dependent on them their disruption would have crippling effects.**
- **The rise of cyberwarfare should impel a reexamination of classical just-war ethics, given its relative ease of use as a "first resort" and the tempting prospect of being able to achieve national aims with less-bloody use of force.**
- **To head off a virtual arms race, behavior-based cyber arms control should be explored, including multilateral agreements to refrain from targeting civil infrastructures and pledging "no first use" of such tactics.**

Indeed, the ability of Britain's "Ultra" and its American counterpart "Magic" to decipher, respectively, German and Japanese codes made all the difference in the first few years of the war when the Allies often had to engage Axis forces from a position of material inferiority. Later, when the tide had turned, codebreaking enabled Allied victories with fewer casualties due to foreknowledge of enemy intentions.

The age of computers in battle that has unfolded over the past 70 years has proved similar to earlier eras in military history, with these new informational tools pointing to new practices. Today, computers serve not only to guide weapons and break codes but also to winnow vast amounts of battle-related information in the search for insight while facilitating lateral communications, or contact with fellow field units, not just with distant commanders. It is this super-empowerment of those who actually conduct the fighting that most distinguishes our era of informational advances from earlier ones.

An example is the triumph enabled by some 200 American Special Forces soldiers in Operation Enduring Freedom they and local allies conducted in Afghanistan in late 2001. The Green Berets rode and fought in the immediate company of a few thousand friendly Afghans, part of a larger nominal force of perhaps as many as 40,000 fighters—until then, on the losing end of a civil war in which 95% of the country had been ceded to the Taliban.<sup>37</sup> The Special Forces and those accompanying them were opposed by upward of 70,000 Taliban and Al Qaeda fighters who had already shown resilience in the face of a month of American-led aerial bombing.<sup>7</sup> But "the 200" had a secret weapon: the tactical Web page.

Originally designed with the idea of simply allowing these soldiers to order supplies, the Web page quickly became their preferred means of communicating timely, targetable information among themselves. The resulting effect was that the teams could act more swiftly and knowledgeably



Poster created by U.S. Department of Defense Cyber Strategy.

and give attack aircraft supporting them far greater potency, due to what has been described as their "faster, unfiltered flow of data."<sup>9</sup> In just a few weeks the enemy was driven from power and out of the country by an omnidirectional assault best described as a "swarm." That this success was eventually squandered, allowing the Taliban to mount an insurgency of its own, is more a function of the return to traditional command arrangements and concepts than of any fundamental flaw in network-style operations.

Several years after the initial take-down of the Taliban, another kind of military network emerged, this time in Iraq, where vicious insurgent action was under way. While senior American generals and Pentagon officials

were having difficulty mastering this challenge, junior officers doing most of the actual fighting crafted a way to share their "lessons learned" and best practices. Through a Web site called [companycommand.com](http://companycommand.com), initially open only to company commanders, good ideas were quickly diffused throughout the force, sharply improving counterinsurgent practices.<sup>5</sup> Sadly, out of ostensible security concerns, the Web site was soon subjected to high-level oversight that had a chilling effect on the willingness of junior officers to freely share their thoughts. Still, another aspect of the power of IT-enabled networking had been demonstrated.

Every day it grows clearer that networks, best described by philosopher-technologist David Weinberger's el-

egant phrase, “small pieces, loosely joined,” comprise the organizational form most empowered by computers, the Internet, and the Web. Their strength comes from their great lateral connectivity and the kind of “collective intelligence” that arises when many share their thoughts and build on one another’s ideas. Over the past two decades the world has seen networks rise, with civil-society movements toppling authoritarian regimes in a series of social revolutions, most recently in the “Arab Spring” of 2011. But terrorists and transnational criminals, the principal “uncivil society” actors of our time, have benefited from networking, too, demonstrating that the new tools may serve the darkest of purposes, as Al Qaeda has shown the world. Which of networking’s Janus-like faces will prevail in the future?

### The Path Since the 1970s

Given the wide-ranging effects of the computer revolution on the larger issues of society and security, it is not surprising that military affairs are also profoundly affected by computerization and networking. But this reshaping has emerged only in fits and starts, with halting progress. Difficulties in Afghanistan following the initial triumph enhanced by a tactical Web page and the fate of [companycommand.com](http://companycommand.com) are

dramatic examples of the problem. But so, too, was the notion that electrons transmitted through information systems no longer simply communicate, but were becoming actual weapons. This idea, introduced by Thomas Rona, a science advisor to the Defense Department, in his seminal 1976 think piece, “Weapons Systems and Information War,”<sup>31</sup> was a breakthrough concept. Yet for the next 20 years, Rona’s notion was simply folded into existing strands of strategic thought, leading to information warfare being equated with either strategic air power or nuclear war.

At this time, defense researchers, still steeped in Cold War military doctrines, became deeply attracted to the idea of mounting crippling attacks on adversaries without first having to engage and defeat their sea, air, and land forces. To the extent there was debate, it was about whether “strategic information warfare,” as it would come to be called,<sup>25</sup> would look more like the sustained aerial-bombardment campaigns of World War II and later Korea and Vietnam or be thought of in terms of the massive effects that would accompany nuclear exchanges or widespread use of chemical and biological weapons, as international security expert Walter Laqueur argued in the 1990s.<sup>22</sup> That such “mass disruption”

could be achieved without significant loss of life made strategic information warfare irresistible.

Around the same time (early-1990s) my RAND Corporation colleague David Ronfeldt and I introduced our concept of “cyberwar,” which was far less about using computer viruses to attack other societies than about gaining an information edge over adversary military forces in battle.<sup>2</sup> Our view was based on the belief that information warfare as a form of strategic attack would have as poor a record of success as aerial bombardment, which has seldom achieved its hoped-for goals.<sup>28</sup>

Instead, advanced information systems had simultaneously empowered and imperiled modern militaries, opening new operational possibilities but at the same time making armies, fleets, and air forces vulnerable to disruption. Small but better-informed forces could thus defeat larger, less-well-informed, enemies, much as the heavily outnumbered U.S. naval forces outfought the Imperial Japanese fleet at Midway in 1942 by knowing more about their adversary’s dispositions and intentions. Fanatical courage, luck, and timing were important factors in this battle, but the ambush of the Imperial Japanese Fleet could not have happened without an initial information edge. So a key defense research agenda was identified, one aimed at understanding the material effects of “knowing more.”

### Doctrinal Debate

Conflict between the two major competing concepts—strategic information warfare as launching “bolts from the blue” and cyberwar as doing better in battle—was inevitable. Since the 1990s, a kind of “war of ideas about the idea of cyberwar” has been waged, with each side landing telling blows. The military proponents of what journalist James Adams once called the “strategic attack paradigm”<sup>1</sup> have been dominant in the discourse, skillfully using the threat of this kind of assault—in the hands of hostile nations and/or networks—to drive national-security debates in countries around the world and generate huge budgetary support for protection of their “critical information infrastructures.” Much as the still-frightening specter of nuclear



**U.S. sailors assigned to Navy Cyber Defense Operations Command at Joint Expeditionary Base, Little Creek-Fort Story, VA, responsible for monitoring, analyzing, detecting, and responding to unauthorized activity within U.S. Navy information systems and computer networks.**

U.S. NAVY PHOTO BY MASS COMMUNICATION SPECIALIST 2ND CLASS JOSHUA J. WAHL/RELEASED

strikes sparked the rise and persistence of myriad well-funded ballistic-missile defense initiatives, the notion of a “digital Pearl Harbor,” mounted perhaps by cyberterrorists, has ensured the future of an entire industry devoted to thwarting a massively disruptive virtual attack.

The alternative emphasis, on exploring the implications of the information revolution for battle, has gained less traction. In part this is the result of a military mind-set still steeped in the Powell Doctrine of “overwhelming force” and its aerial homunculus, “shock and awe” bombing. Commanders much prefer to flatten enemy forces with brute force if at all possible, fearing that subtler approaches enabled by advanced information systems will either have less effect or be too difficult to implement.

The same commanders express concern that growing dependence on such systems could have crippling effects should they be disrupted, whether by logic bombs or well-placed physical bombs. This last worry—about kinetic weapons—is a subtle echo of early reservations, largely dispelled, as to whether computers would ever actually be rugged enough to function in the field.<sup>6,17</sup>

Despite such old habits of mind, attempts have been made to articulate innovative ideas that would improve military effectiveness. The best known is the concept championed by the late Vice Admiral Arthur Cebrowski, “network-centric warfare.” Cebrowski, a Vietnam-era fighter pilot with an advanced degree in computer science from the Naval Postgraduate School, envisioned an interconnected, lattice-like set of “sensor and shooter grids” that would share information swiftly and widely with the largest possible number of combat elements. Introduced in 1998, this notion has sparked much discussion but has not been implemented widely or systematically.<sup>11</sup> Another senior naval officer, Admiral William Owens, propounded his own views of a highly networked “system of systems” intended to function in similar fashion.<sup>27</sup>

In the late-1990s, while Cebrowski and Owens focused on organizational redesign along networked lines, Ronfeldt and I, interacting with them regularly at the time, shifted our own

focus to developing the kind of battle doctrine implied by a force that would have better access to information than ever before. We came up with the notion of “swarming,” or simultaneous assault from many directions, as the most effective means by which a well-informed network comprised of many small units could strike at its foes, whether large and traditional or small and irregular.<sup>3</sup>

As with Cebrowski’s network-centric warfare and Owens’s system of systems, swarming has been embraced only fitfully. Today it languishes in a virtual purgatory alongside “autonomous” combat systems, or weapons wielded by artificial intelligence, since swarming has been branded as best-suited to application by silicon-based intelligence.<sup>34</sup> As for autonomous systems, the notion of unleashing robotic weapons has been seriously studied since the 1980s,<sup>4</sup> a period of major technical advances in the field. Nevertheless, there remains a high barrier to change here, posed largely by human self-interest (such as pilots’ fear of and resistance to replacement by robots) that slows their progress. Other concerns have to do with the possibility that robots would unwittingly inflict serious collateral damage, making it more difficult to fulfill the ethical imperative to always do one’s best to wage war “justly.” But now, with a swarming doctrine to guide field operations, military commanders have at least a vision of how a skillfully blended future force of humans and intelligent machines could operate effectively and ethically. All that may be necessary to make this leap would be to overcome tradition-bound organizational inertia. Given the great strains on U.S. service members from repeated deployments over the past decade, robots may soon be more welcome in the force.

### The Offense-Defense Balance

In a period in which battlefield-based cyberwar has made only isolated gains, the bureaucratic triumph of the strategic attack paradigm has spawned what can only be called a “cyber defense initiative,” an information-age counterpart to the Strategic Defense Initiative missile-interceptor program introduced by President Ronald Reagan in 1983. While the mix of institutional

actors involved is more diverse than in the nuclear realm, the U.S. military still plays a central role in thinking through the problems associated with ensuring the continued functions of its forces in the field and the infrastructures upon which its citizens depend. The same is true with regard to infrastructure protection in many other developed countries, where several military cyber corps have sprung up.

A key problem that has plagued cyber defense is that there was, and continues to be, far too little debate over alternative paradigms. The dominant view was, and still is, tethered to a kind of preclusive security based on firewalls capable of distinguishing friendly “self” from hostile “other.” The problem with this Maginot-Line-like approach is that firewalls are, for the most part, capable of recognizing only things they already know, whether hostile or friendly. They are not as good at dealing with new wrinkles.

There have been repeated serious intrusions into sensitive defense information systems in the years immediately before, as well as since, the 9/11 attacks on America, little of which can be discussed openly. These events, known to the public under such names as “Moonlight Maze,” which may be linked to Russia, and “Titan Rain,” which may involve China,<sup>39,40</sup> provide stark proof of the limitations of the Maginot Line mind-set. This is not only true of the military “infosphere”; commercial firms tend to follow the military model of preclusive security. Here, too, the news is troubling, if even more difficult to obtain in detail. But the reality is that leading corporations around the world are hemorrhaging intellectual property, as hackers tap their creative veins and bleed them of their precious information resources.

The alternative to a primarily firewall-dependent information-security model is to accept that intruders will almost always access the system, no matter how nominally secure, but by strongly encrypting the data within, a defender can deny the attacker/exploiter the advantage of having gotten inside. Dorothy Denning, a leading computer scientist and professor of defense analysis at the Naval Postgraduate School, has summed up the case for defense dominance via encryption: “If the

key length is sufficiently long, it is not feasible to test each and every key. In practice, the strength of a system needs only to be commensurate with the risk and consequence of breakage.”<sup>15</sup>

Those who believe “data at rest is data at risk” envision the additional security option of breaking encrypted data into pieces and sending them out into “the cloud,” or into cyberspace beyond one’s own system, ready to be called back and reassembled at a keystroke. Strong crypto and the cloud are gaining attention, but the firewall-based model remains dominant, especially with military- and national-security-related information systems.

Thus the fear of a crippling “bolt from the blue” cyberattack is great, and the U.S. military’s frenetic efforts to cope with such a possibility have sparked a return in some military circles to the classic question of whether offense or defense is “dominant.” In every period of major technological change there has been sharp debate about the properties of the new tools of war, and the conclusions drawn have quite often been wrong.<sup>29</sup> For example, before World War I, most Western generals believed machine guns and high-explosive artillery would favor the offense. They were tragically wrong. Some millions of soldiers marched shoulder to shoulder to slaughter in that war.<sup>35</sup>

A generation later, at the outset of World War II, the prevailing belief, except within small circles of military mavericks, was that defense was dominant. This mind-set led to such initiatives as the massive investment in the French Maginot Line. Wrong again. Aided by mechanization, the Germans simply went around the wall and scored one of history’s signal military victories in the spring of 1940. It seems that figuring out the state of the offense-defense balance, in light of the latest technological changes, has generally proved quite difficult. Today is no exception.

### Security System, Attack Tool

Assessing the balance of power in battle is just as difficult to parse in the virtual realm as it has been in the physical realm. To date, the school of thought associated with notions of offense dominance in cyberwar has been

ascendant, feeding the frenzy to craft defenses.<sup>12</sup> But articulate dissenters have also been heard from, in particular the RAND Corporation’s Martin Libicki, who believes it will be difficult for cyberspace-based offensives to achieve strategic effects. As he sees it, cyberwarfare “is still largely theoretical. People have seen the detritus left behind by small-scale hacker attacks, but no one has ever seen it work at the scale often claimed for it.”<sup>23</sup>

Even so, a theoretically superior defensive concept can still lead to wrong-headed implementation, engendering great vulnerabilities. A case in point is the Navy Marine Corps Intranet (NMCI), a classic preclusive security attempt—in the form of the world’s largest intranet—to make intrusions into the sea services’ information systems virtually impossible. From the outset, NMCI proved vulnerable to a range of threats, none openly acknowledged, beyond admission that one particular computer virus, a variant of MS/Blast, made its way into and throughout much of the system.<sup>30</sup>

Viral attacks, based on malicious software that attaches to programs or documents, have grown in sophistication and stealth, as have “worms,” self-replicating programs that can even cause disruptive effects in the physical world. A recent and very troubling example of the latter is the Stuxnet worm, malicious software specifically designed, it appears, to exploit vulnerabilities in Siemens industrial control systems components in Iranian high-tech (possibly nuclear-weapons proliferation-related) equipment.<sup>10,32</sup>

Stuxnet is especially interesting in that it has apparently succeeded in disrupting systems not connected to the Internet, suggesting insertion of the worm may have occurred via any of a range of components, possibly through something as simple as an infected USB drive. If so, the “reach” of cyber-weaponry may have to be reckoned as far greater than previously thought. The implication is that a vast range of technical components—many of them “off-the-shelf” imports—should be seen as potential conduits for attackers. Awareness of this threat has grown and, in the American case, led the military to develop a significant capacity for ensuring “supply chain security.”<sup>21</sup>

This discussion—from Libicki’s analysis to the Stuxnet example—suggests the offense-defense balance in this era may be characterized by an action-reaction cycle in which one or the other mode of war becomes temporarily ascendant. It may be much like technical and tactical developments in traditional military affairs, often favoring the attacker or defender when introduced, but which are eventually countered. For example, the World War II German U-boat wolf-pack offensive was ultimately defeated by a mix of skillful codebreaking and improved direction-finding equipment, unmasking the attackers’ positions and giving the edge to the defense.

Likewise, viruses, worms, and new forms of “semantic attack” on information systems will likely be subject to technical countermeasures that will diminish, if not dispel, the threats they pose, particularly if firewall-oriented “Maginot Line mind-sets” give way to greater emphasis on strong cryptography and data being moved around much more, not just deposited for long periods in fixed locations.

### Recent Cyberwars

In April and May 2007 a series of widespread cyberattacks was mounted anonymously against Estonia, sparked by removal of a World War II monument to Soviet soldiery (commemorating the Russian military campaign and its casualties suffered driving the Nazis from the country) from a prominent place in the capital, Tallinn. Outrage among Russians at this action was followed by massive cyberattacks thought to have been perpetrated, or at the least encouraged, by Russian leaders against the Estonian government and civil society. Huge disruptions ensued for a short period, with the attackers using simple tools in distributed denial-of-service attacks.<sup>8</sup> It was a clear example of the “strategic attack paradigm”; a scaled-up version of this sort of campaign launched against, say, the U.S. or other developed country would have inflicted enormous economic losses.


In August 2008 the Russian military launched an invasion of the trans-Caucasian Republic of Georgia, a U.S. ally whose security forces had been nurtured, trained, and equipped along

lines amenable to the Pentagon. Unlike the difficulties they had experienced fighting in nearby Chechnya, Russian troops this time sliced through Georgian defenses. (The Russians were joined in the field by Ossetian irregulars, though they did not form the advance shock troops in this particular war.) Among the factors contributing to Russian success were skillful cyberattacks mounted in conjunction with field operations, making this a battle-oriented cyberwar rather than a stand-alone virtual strategic offensive against infrastructure. The degree of disruption to Georgian command-and-control systems achieved by hackers (use of cyberattacks has still not been acknowledged by Moscow) was startling. Again, were similar effects scaled up against a U.S.-size military, they would likely achieve catastrophic levels of disruption.


The Estonian and Georgian cyberwars both seem to support the notion that we are entering an era of offense dominance. Whether the intent is to use computers and cyberspace for mounting strategic attacks on other societies or to provide “virtual supporting fire” in force-on-force battles in the field, preventing such assaults is likely to prove problematic. They may also prove difficult to contain, at least for a while. One implication is these events could herald a period of constant cyber conflict in which cyberwars are always under way somewhere; another is that the ease of mounting such attacks will be offset by retaliatory threats or mutual agreements to refrain from doing so. Indeed, both notions of “controlling cyberwar” have been considered in recent years.

### **Deterrence and Arms Control**

It is interesting, and somewhat ironic, that the Russians appear to be on the cutting edge of cyberwarfare, as both a form of strategic attack and mode of battle. The irony comes from the fact that, at least since the mid-1990s, Russia has been trying to make the world less permissive of this kind of conflict by bringing older concepts of deterrence and arms control into the information age. For example, an early, and very blunt, Russian attempt at deterrence came in 1995 in the form of an alarming statement from information



**Strong crypto and the cloud are gaining attention, but the firewall-based model remains dominant, especially with military- and national-security-related information systems.**



warfare expert V.I. Tsymbal, as reported by military analyst Tim Thomas: “Moscow’s only retaliatory capability [to cyberattacks] at this time is the nuclear response.”<sup>38</sup>

Tsymbal’s formulation spoke to what is called the “punitive” dimension of deterrence, or the belief that, even when defenses are poor, a capacity for devastating retaliation can prevent attacks from being mounted in the first place. An early nuclear strategy, the Eisenhower-era U.S. doctrine of “massive retaliation” with atomic weapons against any form of aggression, even on a small scale, is a classic example of the punitive approach. However, the exceedingly disproportionate nature of the threat undermined its credibility from the outset, causing the policy, in the phrasing of strategic analyst and Nobel laureate Thomas Schelling, to be “in decline almost from its enunciation in 1954.” However, its successor concept, advanced in the 1960s, “mutual assured destruction” (MAD)—all-out retaliation in the event of a nuclear attack—has fared better and remains, even today, the foundation of American strategic-deterrent thought.

In the cyber realm, it seems that some informal variant of MAD may already be in place to deter strategic attacks on infrastructure, the twist being that the concept is now “mutual assured disruption,” not destruction. Where many advanced militaries are hardly likely to be deterred from waging cyberwar in the field against their adversaries, developed countries are clearly aware that their information systems are and will remain vulnerable to attack, so considerable circumspection is the apparent norm when it comes to the strategic-attack paradigm. To be sure, many cyber-spying intrusions occur worldwide on a daily basis but are not attacks per se and do little or no damage to operating systems.

Key problems for cyber deterrence are that attacking nations may keep their identities secret, and not all attacks emanate from other nations. On the latter point, nations may be attacked by networks of non-state actors (such as terrorists and transnational criminal syndicates) or even super-empowered individuals. When it comes to cyberwarfare of this strategic sort,

a network could easily slip the bonds of mutual deterrence simply because it proves difficult, if not impossible, to figure out against whom to strike a retaliatory blow. The same is true if networks ever get their hands on nuclear weapons, though for now the notion of a network having its own “nuclear Napoleon” remains just a far-off possibility. It is the imminent threat posed by hacker networks (and perhaps terrorist groups) that already possess or are developing capacities for mounting mass disruptive cyberattacks that demands attention. Against them, the only measure likely to work will be based on the notion of what experts call “denial deterrence,” the ability to convince malefactors that they are wasting their time with such attacks, as the likelihood of success is low.<sup>26</sup>

Given the great edge conveyed by being able to launch cyberattacks from behind a veil of anonymity, denial-based deterrence is to be preferred when confronting the threat from networked actors. But when it comes to other nations, the hope remains that they can be identified when they perpetrate attacks, and that punitive retaliatory threats can work to stop them.<sup>24</sup> However, the ambiguity as to the perpetrator(s) of the Stuxnet attack suggests the veil of anonymity may remain difficult to pierce.<sup>19</sup> Thus, uncertainty abounds, leading to efforts to cultivate another Cold War concept: arms control. Though clear that almost all information technologies can be “weaponized” for cyberwarfare, and trying to control their spread is futile, there is some hope of fostering a behavior-based norm of restraint by “emphasizing dialogue with like-minded nations,” as former CIA director General Michael V. Hayden explained earlier this year.<sup>20</sup>

This notion, called “operational arms control,” reflects success in both the biological and chemical weapons conventions, formally adopted in 1975 and 1997, respectively, that have done much to limit development and use of these mass-destructive weapons. The question today is whether such behavior-based controls can make a similarly beneficial contribution, inducing those nations, perhaps even some networks, to refrain from using them, at least against civilian infrastructures.



## The Estonian and Georgian cyberwars both seem to support the notion that we are entering an era of offense dominance.



However, as with deterrence, it is difficult to see how such controls would be imposed on the battlefield, given that cyberwar applied in a military-on-military fight would likely convey an advantage to the better practitioner, bringing about a swifter, less-bloody end to the fighting. The answer to the question about cyber arms control and cyberwarfare is perhaps to be found in the ethical domain.

### Just, Unjust Cyberwars

Classical ethical formulations about conflict address both going to war justly (acting in self-defense or fighting only as a last resort) and waging war morally (using force only in proportionate ways and refraining from inflicting harm on noncombatants).<sup>41</sup> Cyberwarfare puts considerable strain on both aspects of just-war ethics. The very ease of offensive action encourages redefining “defense” in preemptive or even preventive terms<sup>a</sup> and makes going to war in this way attractive as an early option rather than as a last resort. In terms of fighting justly, cyberwarfare, with its disruptive rather than destructive effects, hardly seems likely to qualify as “disproportionate,” either as a form of strategic attack or on the battlefield.

However, no one is able to predict effects across cyberspace, and the prospect of inflicting collateral damage is likely to be high. Think of Stuxnet, which may have targeted a specific Iranian nuclear-proliferation program but which also apparently “escaped” and spread. Thus it has inflicted damage on information systems in many other countries, and, now that it is out in the world, may be reengineered by others for their own, potentially unjust, uses.

In the realm of cyberwarfare on the battlefield, as opposed to its application as a form of strategic attack, a curious new ethical nuance emerges: acting early and aggressively might cripple an opponent in ways that sharply reduce physical casualties and overall

a Preemption refers to attacking when under imminent threat of attack, with Israeli actions at the outset of the 1967 Six Day War often referred to as a clear example. Prevention means striking before the enemy poses a serious threat, the rationale some policymakers used for the U.S.-led invasion of Iraq in 2003.

war costs. In essence, devoting more attention to disrupting enemy forces, even, or especially, with early surprise attacks, might be ethically acceptable due to the reduced destruction that would ensue.

The paradox is that the rise of cyberwarfare techniques in battle may make the traditionally unethical notion of starting a war attractive, yet at the same time cyberweaponry could improve the efficiency, and thus the morality, of the war-waging process itself. The logical terminus of a world replete with cyberwarfare would be an era with more uses of force, though they would be shorter and less destructive than traditional conflicts.

A key problem with this line of reasoning is that it does not deal adequately with escalation. A nation whose military is quickly debilitated on the battlefield due to cyber strikes may, instead of standing down or surrendering, respond with whatever weapons of mass destruction it has. Indeed, some nations might respond to their own perceived vulnerability to cyber disruption by seeking to acquire nuclear, biological, or chemical arms. The threat to use them might be subject to deterrent counterthreats by the war initiator; but those who have been attacked first generally hold the somewhat higher moral ground when it comes to retaliatory escalation. The best example of this is the decades-old NATO policy of reserving the right to use nuclear weapons in response to a conventional Russian invasion of Western Europe. A similar policy might well emerge in future efforts to cool the ardor of cyberwar enthusiasts, as in the new U.S. policy of threatening to respond to cyberattacks with conventional military means.<sup>18</sup>

### Conclusion

The military encounter with computerization is playing out against a backdrop that includes many traditional concepts—strategic attack, battlefield close support, deterrence, arms control, and “just war” ethics—exposed now to troubling new wrinkles. But for all the complexities that have emerged, there are still reasonable paths forward. One could lead to more cyberwarfare on battlefields but few, if any, direct cyberattacks on societal infrastructures. This runs coun-

ter to the current emphasis among military leaders from nations around the world on the “strategic attack paradigm” but is a shift that might have profound practical (and ethical) benefits. It is also gaining traction among leading scholars, two of whom, Peter Sommer and Ian Brown, of the London School of Economics and the Oxford Internet Institute, respectively, took a clear position against the strategic-attack paradigm but acknowledged the importance of cyber operations on the battlefield: “Pure cyberwar... is highly unlikely. [But] in nearly all future wars... policymakers must expect the use of cyberweaponry...in conjunction with more conventional kinetic weaponry.”<sup>36</sup>

However, carrying out this battle-oriented vision places huge demand on the cultivation of cyber-adept military service members of the highest caliber.

National governments and their military leaders might also have to choose between deterrence and arms control. During the decades of the Cold War and for some time after the dissolution of the Soviet Union, these concepts were viewed as moving hand-in-hand. But the information revolution and the rise of cyberwarfare may have gravely undermined deterrence, placing ever-greater weight on the need to emphasize behavior-based arms control, as by, say, entering into mutual agreements to refrain from being the first to mount cyberattacks against another country’s civilian infrastructure. Against non-state networks, defense-oriented “denial deterrence” would likely prove of greater value than reliance on punitive threats.

Civilian and military decision makers thus have two preferred pathways: limiting cyberwar to battlefield use and embracing behavior-based arms control. If pursued, the paths could enable the information age to unfold in a more peaceful manner. Indeed, they offer the world community its best chance to use advanced information technology to spread prosperity and continue the intellectual improvement of all humanity. □

### References

1. Adams, J. *The Next World War*. Simon & Schuster, New York, 1998.
2. Arquilla, J. et al. Cyberwar is coming! *Comparative Strategy* 12, 2 (Apr.–June 1993), 141–165.

3. Arquilla, J. et al. *Swarming & the Future of Conflict*. RAND Corp. Santa Monica, CA, 2000.
4. Barnaby, F. *The Automated Battlefield*. Free Press, New York, 1986.
5. Baum, D. Battle lessons. *The New Yorker* (Jan. 2005).
6. Bellin, D. *Computers in Battle*. Harcourt, 1987.
7. Biddle, S. *Afghanistan & the Future of Warfare*. Strategic Studies Institute, Carlisle, PA, 2002.
8. Blank, S. Web War I. *Comparative Strategy* 27, 3 (Apr.–June 2008).
9. Briscoe, C.H. et al. *Weapon of Choice*. Combat Studies Institute, Fort Leavenworth, KS, 2004.
10. Broad, W. et al. Israel tests called crucial in Iran nuclear setback. *The New York Times* (Jan. 16, 2011).
11. Cebrowski, A. et al. Network-centric warfare. *Naval Proceedings* (Jan. 1998).
12. Clarke, R. *Cyber War*. HarperCollins, New York, 2010.
13. Clayton, M. Computer worm as guided missile? *The Christian Science Monitor* (Oct. 4, 2010).
14. de Landa, M. *War in the Age of Intelligent Machines*. MIT Press, Cambridge, MA, 1991.
15. Denning, D. *Information Warfare and Security*. Addison-Wesley, Boston, 1999.
16. Dixon, N. et al. *Company Command*. West Point, NY, 2005.
17. Dunnigan, J. *Digital Soldiers*. St. Martin’s Press, New York, 1996.
18. Gorman, S. et al. Cyber combat: Act of war. *The Wall Street Journal* (May 31, 2011).
19. Gross, M. A declaration of cyberwar. *Vanity Fair* (Apr. 2011).
20. Hayden, M.V. The future of things ‘cyber’. *Strategic Studies Quarterly* 5, 1 (Spring 2011).
21. Hoover, J.N. Air Force to tackle supply-chain security. *InformationWeek* (Aug. 20, 2010).
22. Laqueur, W. Postmodern terrorism. *Foreign Affairs* 75, 5 (Sept.–Oct. 1996).
23. Libicki, M.C. *Conquest in Cyberspace*. Cambridge University Press, New York, 2007.
24. Libicki, M.C. *Cyberdeterrence and Cyberwar*. RAND Corp., Santa Monica, CA, 2009.
25. Molander, R. et al. *Strategic Information Warfare*. RAND Corp., Santa Monica, CA, 1996.
26. Morgan, P. *Deterrence*. Sage Publications, Thousand Oaks, CA, 1977.
27. Owens, W. *Lifting the Fog of War*. Farrar, Straus and Giroux, New York, 2000.
28. Pape, R. *Bombing to Win*. Cornell University Press, Ithaca, NY, 1996.
29. Quester, G. *Offense and Defense in the International System*. Wiley, New York, 1977.
30. Robinson, B. Love/hate relationship with NMCI. *Federal Computer Week* (Sept. 10, 2007).
31. Rona, T. *Weapons Systems and Information War*. Boeing, Seattle, 1976.
32. Sanger, D. et al. Iran fights malware attacking computers. *The New York Times* (Sept. 26, 2010).
33. Schelling, T. *Arms and Influence*. Yale University Press, New Haven, 1966.
34. Singer, P.W. *Wired for War*. Penguin, New York, 2009.
35. Snyder, J. *The Ideology of the Offensive*. Cornell University Press, Ithaca, NY, 1989.
36. Sommer, P. and Brown, I. *Reducing Systemic Cybersecurity Risk*. Organization for Economic Cooperation and Development, Paris, France, 2011.
37. Stanton, D. *Horse Soldiers*. Scribner, New York, 2009.
38. Thomas, T. The threat of information operations: A Russian perspective. In *War in the Information Age*, R. Pfaltzgraff and R. Shultz, Eds. Brassey’s, London, 1997.
39. Thornburgh, N. The invasion of the Chinese cyber spies. *Time* (Aug. 29, 2005).
40. Vistica, G. We’re in the middle of a cyberwar. *Newsweek* (Sept. 20, 1999).
41. Walzer, M. *Just and Unjust Wars*. Basic Books, New York, 1977.

### Acknowledgments

I would like to thank the reviewers and editors for their insightful critiques of earlier drafts of this article and for their thoughtful suggestions regarding revisions to it.

**John Arquilla** (jarquilla@nps.edu) is a professor of defense analysis at the U.S. Naval Postgraduate School, Monterey, CA; he was, 2005–2010, director of the Department of Defense Information Operations Center for Excellence, also located in Monterey, CA.