The Computer Mouse that Roared: Cyberwar in the Twenty-First Century

John Arquilla
Professor
U.S. Naval Postgraduate School

Scholars have long sought to understand the persistence and prevalence of conflict in world affairs. They have theorized that wars arise from imbalances of power, challenges to declining empires or nations, ethnic or religious antipathy, and even attempts to divert attention from troubles at home. However, none of these explanations has proved to be particularly valid: great conflagrations have resulted when power was "in balance;" empires and nations have acted with the greatest belligerence when they were waxing rather than waning; cultural and religious diversity has regularly been embraced without strife; clashes *within* civilizations have been as common as those that have arisen *between* them; and true diversionary wars are exceptionally rare. Now into the mix comes cyberwar: an emergent mode of conflict enabled by and primarily waged with advanced information systems, which are in themselves both tools and targets. It may be that this new way of war—possibly quite potent on the battlefield, but also able to strike at others' homelands without the need to defeat their military forces first—is showing the world that outbreaks of conflict may be primarily driven by the state of play in technology. Today, this state of play is one that makes attacking seem easy and defending oneself hard. A world replete with cyberwars appears to loom ahead.

How will the growing potential to sever or disrupt military communications and disable infrastructures with computer worms and viruses affect the balance of world power? Will cyberwar fit into established explanations of the causes of war or will it be inexplicable like other new fighting concepts of earlier eras? Finally,

John Arquilla is a professor of defense analysis at the U.S. Naval Postgraduate School. From 2005 to 2010, he was director of the Department of Defense's Information Operations Center for Excellence. His latest book is *Insurgents, Raiders, and Bandits: How Masters of Irregular Warfare Have Shaped Our World.*

will this technology really imply a new age of conflict for the world? We must answer these questions because wars may indeed arise as these new weapons make conflict more conceivable. If so, attacks that come at the click of a mouse—that is, within easy reach of nations, networks, and even individuals—may give new life to the old Hobbesian notion of wars of "all against all."

One defense analyst who thought deeply about this possibility was George Quester. In the 1970s, he advanced the argument that the frequency of war is a function of the perceived dominance of either offensive or defensive means. Quester wrote that war is most likely to occur when "the environment may suggest great advantages for launching an attack."[1] Without such advantages—that is, with high costs and risks associated with offensive action—peace will be more robust. For example, the marriage of gun and sail in European naval affairs ramped up violence across the globe during the sixteenth century. These heavily armed, long-range sailing vessels sparked centuries of colonial expansion and control, reshaping the world system.[2] A more modern example—one that helped reverse the tide of imperialism during the twentieth century's "wars of liberation"—was the emergence of the exceptionally durable and light AK-47. This assault rifle proved to be a weapon "so deadly, yet so simple to use, that every able-bodied person [became] worth having as a soldier."[3]

When defensive means were dominant, stability and security resulted. The *trace italienne*—a military design style that created fortifications of sufficient strength to withstand sieges, artillery bombardments, and ground assaults—helped tamp down martial ardor and stabilize European power politics during the Renaissance and the Enlightenment. At the dawn of the twentieth century, barbed wire, machine guns, and high-explosive artillery gave even greater advantages to the defense. However, the failure to accurately perceive that defense was dominant led great empires to engage in catastrophic war-making against one another in 1914. Thus, the outbreak of World War I provides "negative proof" of offense-defense theory. According to the theory, the superiority of the defensive should have kept the peace. However, it did not and millions died in failed offensives undertaken because of the mistaken belief that massed frontal assaults by brave men could somehow break through against automatic weapons and high-explosive artillery.[4]

In the 1940s, after the brief flowering of German *blitzkrieg* armored warfare concepts, nuclear weapons came along. Once these weapons of mass destruction started spreading beyond American control, they offered another twist on the defense dominance idea. Even seven decades into the nuclear age, there are still no reliable ways to intercept intercontinental ballistic missiles armed with nuclear warheads. But the sheer destructive capacity of these weapons and the likelihood of devastating retaliation in response to an attack have resulted in "the equivalent of the primacy of the defense," as the noted political scientist Robert Jervis observed.[5] Thus, the Cold War never got hot, validating Quester's theory.

Cyberwar is yet another mode of conflict in the long line of military history's new operational concepts, current debate about which has yet to resolve whether it will favor offense or defense. President George W. Bush's one-time "cyberczar" Richard Clarke said that cyberwar constitutes a grave threat, in part because of the ease with which its weaponry—computers, even quite small ones—can be acquired and networked into large attacking formations, such as robot networks ("botnets"). Clarke sees cyberwar as almost "undeterrable," the same term that George Quester used to describe the potency of guerrilla warfare.[6] Martin Libicki ("The Nature of Strategic Instability in Cyberspace," p. 71) a top cyberexpert at the RAND Corporation, has argued the opposite: the myriad problems associated with offensive cyberwarfare are problematic enough to warrant skepticism about its ultimate efficacy.[7]

Interestingly, both those who believe in the tremendous offensive potential of cyberwar as well as the skeptics feel a strong need to emphasize defenses: the former because they see a technology-dependent world as extremely vulnerable to disruptive cyberattacks; the latter because of the belief that taking early protective measures can reduce the threat to modest levels. This has led to a convergence in policy circles emphasizing defense, which in turn has driven the technical and academic discourses along similarly defense-minded lines. Still, there has also been an increase in investment and research in offensive cybercapabilities, though much of it remains classified. The extra benefit of this kind of research, most defense analysts and information technology experts believe, is that a deeper understanding of offensive cyberwarfare will aid the development of ever more robust defenses. But there is another reason for such research—one seldom discussed openly. It is the belief that taking the cyberoffensive might be profoundly advantageous, both for national and global security. It is because of this less openly discussed possibility that cyberoffensives should be closely considered.

The Two Faces of Cyberwar

When David Ronfeldt and I introduced the concept of cyberwar 20 years ago, we thought of it primarily in terms of gaining and exploiting a "knowledge advantage" over one's battlefield opponents.[8] In our view, modern militaries were growing so dependent upon secure, timely flows of massive amounts of information that their disruption would quickly have a crippling effect on the ability to fight. The implication was that the optimal use of offensive means would be to target those information systems that were most closely associated with the command and control of military forces in the field, at sea, and in the air. In this respect, we were describing a new way of providing "close support" to those engaged in battle. An enemy force unable to control its own units or track their locations would be unable to sustain a battle or campaign. Thus, future military offensives that effected such disruption would lead to swift victories with less attrition on both sides—echoing the early years of *blitzkrieg* tactics.

But we were skeptical about the prospects for conducting cyberattacks directly against national information infrastructures—along the lines of what one expert labeled the "strategic attack paradigm."[9] Yet, as the academic and policy discourse began to unfold, it became increasingly clear that the vast majority were thinking about cyberwar primarily in terms of attacking infrastructure—a kind of information age analog to strategic bombing. Indeed, one of the leading scholarly studies of cyberwar devoted an entire chapter to the examination of American strategic air power theories as a means of understanding the potential for taking conflict into the virtual domain.[10] Others sought to draw similarities between cyberwar and nuclear war, even though the former is, at best, going to have only "mass disruptive" effects, while the latter's primary stock in trade is mass destruction.[11] The association of the cyberoffensive with nuclear attack is problematic, but it has encouraged useful thinking about issues of deterrence and forms of arms control rooted in mutual agreements to refrain from certain behaviors—both of which are intriguing ideas that might have some utility.[12]

While theorists and policy makers supportive of the strategic attack paradigm have drawn liberally from ideas about aerial bombing and nuclear war, in practice senior military and political leaders have drawn more inspiration from notions of irregular warfare. They view cyberattack in the same light as special operations: as a tool capable of resolving—or at least temporarily defusing—a major international crisis without the need to go to war. This is the realm of the "strategic special operation," a phenomenon studied and so named by the scholar and former State Department official Lucien Vandenbroucke.[13] For example, the Stuxnet computer worm attack on Iranian nuclear enrichment processes may have temporarily slowed down Tehran's weapons proliferation efforts. Regardless of whomever released Stuxnet, this "virtual raid" in which centrifuges were made to run at self-destructively fast rates resonates with both the concept of strategic special operations and, because of the ambiguity about who was responsible for it, covert action. Indeed, cyberattacks of this sort may be seen as giving a "green light" to *Mission: Impossible* sorts of secret strikes—a practice that had somewhat fallen into disrepute in the wake of the Cold War.[14]

If the Stuxnet episode speaks to the possibility of employing cyberattacks for preventive purposes—as the Israeli air raid on the Osirak nuclear reactor outside of Baghdad prevented nuclear proliferation in 1981—such means should also be considered in preemptive roles as well. While preventive measures involve a strike before an adversary becomes a serious threat, preemption refers to the disruption of an imminent attack. For example, Israeli air and ground attacks in the 1967 Six-Day War were launched preemptively because Arab forces appeared to be making final preparations to invade and overrun the country. Now, cyberattacks have the potential to serve as preemptive weapons that could cripple a massing force preparing to attack. Cyberattacks might even be employed to keep two bickering parties from moving to open conflict. In these ways, cyberwar techniques could breathe new life into preemption. This might be how the strategic attack paradigm would cede center stage to the more battlefield-oriented concept of cyberwar that Ronfeldt and I introduced two decades ago.

> **Cyberattacks have the potential to serve as preemptive weapons that could cripple a massive force preparing to attack.**

Practical and Ethical Considerations of Strategic Cyberattack

Proponents of the strategic attack paradigm have not sufficiently considered its serious limitations. In the long discourse about whether to emphasize the cyberoffensive as a means of striking at civilian infrastructures or instead focusing on doing better in battle against other militaries in the field, proponents of strategic attack have generally not been willing to acknowledge the low likelihood that temporarily disabling a power grid or an oil pipeline might actually break the will of an enemy populace. There is simply too much historical evidence of societal resilience under sustained aerial bombardment for us to believe that cyber-induced disruption will prove effective.[15] Aerial bombing, for all its destructiveness, has seldom worked. Future cyberattacks against civilian infrastructure targets will likely fare even worse—with the exception of the aforementioned forms of preventive or preemptive operations. Certainly, the brief period of disruption and the swift recovery of Estonia in the face of sustained "hack attacks" in April and May of 2007—likely launched by Russia or pro-Russian elements—challenge the notion of the strategic attack paradigm's effectiveness as a tool of force and statecraft.[16]

Nonetheless, there will still be campaigns aimed at disrupting information infrastructures and the systems they control, such as power and water supplies. Just as strategic air power advocates felt compelled to try out their theories during World War II, their intellectual descendants feel the same impulse today. But future instances of infrastructural warfare will also likely be complemented by special cyberoperations aimed at disrupting proliferation, terrorism, and other illicit activities, in acts of what I call "cybotage." Besides these, there will indeed be wartime cyberstrikes that target military command and control systems, particularly highly automated programs of advanced militaries like the U.S. Armed Forces' troop deployment and "air tasking" systems. But even far less sophisticated command systems can be targeted to great effect: Russian cyberattacks on Georgia's communications, skillfully blended with Russian field operations, proved an important tool in the short war between the two nations in August 2008.[17]

We live in a time when the ethical demands of waging cyberwar need to be considered.

Clearly, we live in a time when the ethical demands of waging cyberwar need to be considered. A "just war" requires a "right purpose" as well as "due authority," and can only be entered into as a last resort. Further, there must be more than simply a just cause, like self-defense; one must also fight justly. Doing so requires showing care for the safety of civilians and using no more force than the absolute minimum required to achieve one's aims. Such values hold across cultures and have endured over time.[18] Traditionally, "right purpose" has extended beyond just self-defense to include preemption. "Due authority" has meant approval by some governmental entity. In the modern era, these might include transnational bodies such as the United Nations. The meaning of "last resort" is self-evident.

Now comes cyberwar, which shreds the classical notions of war ethics. For example, if networks or even individuals can wage cyberwar, what kind of "due authority" oversees them or sanctions their actions? The answer: none. And if an act of "cybotage" can stem or slow a great threat like illicit nuclear proliferation, why wait to employ it as a last resort? The weapon of mass destruction might be fully developed, or nearly so, before an act of "last resort" takes place. As to the immunity of non-combatants, strategic attack via cyberspace—while it might not kill many, or even any, in a civil populace unlike strategic aerial bombardment, which has always caused substantial civilian deaths—is built around the notion of depriving that populace of its power, water, and other infrastructural requirements. Is the immunity of the non-combatant still upheld if a way of war is designed to inflict much suffering, albeit largely nonlethal? These are all complicated issues, and the early evidence, from Estonia to Stuxnet, suggests that those with cyberwar-waging capabilities are unlikely to use worms, viruses, logic bombs, and other virtual weaponry only as "last resorts." Hacker groups like Anonymous and LulzSec have made it clear that governments and transnational bodies will not be sought out to regulate the cyberwar-making waged by informal networks. Finally, in Estonia, inflicting pain on non-combatants was the principal effect sought by the cyberattackers in 2007. It was not something they strove to avoid.

The principle of proportionality will likely hold up best in an era of cyberwarfare. After all, bits and bytes are unlikely to kill, so as uses of force go, "virtual war" seems more palatable than its bloody predecessors. However, a cyberattack may spark escalation to more lethal forms of war. Indeed, the United States has made it clear that virtual attacks, depending on the severity of their effects, may result in a retaliatory response consisting of physical force.[19] If this sounds troubling, consider the position of V.I. Tsymbal, a Russian cyberwar expert who avowed back in the 1990s that "Moscow's only retaliatory capability [to cyberattacks] at this time is the nuclear response."[20] Both formulations are eerie echoes of the United States' "massive retaliation" doctrine of the 1950s, which called for using nuclear weapons in response to any act of aggression—seemingly without regard for how small. It quickly proved impractical and was "in decline almost from its enunciation in 1954."[21]

The current American effort to define cyberwar as an act of "real war," allowing physical force to be used in response, will founder, much as the massive retaliation doctrine did.[22] The sheer escalatory risk seems hardly worth any satisfaction that might be gained by retaliating for virtual attacks with physical means. What if the cyberaggressor is a major military power—perhaps even a nuclear-armed one—that has a range of responses ready? And what if the aggressor is a band of hackers? "Shock and awe" bombing is hardly likely to work against a network distributed around the world. There is also the possibility that an actual perpetrator might try to "finger" some innocent party as the culprit, with the very idea in mind of sparking a larger conflagration begun by a mistaken military

Bits and bytes are unlikely to kill, so as uses of forces go, "virtual war" seems more palatable than its bloody predecessors.

strike on some innocent third party. The point here is that the practical and ethical "firewalls" between cyberwarfare and more traditional modes of conflict should almost certainly remain robust, crossed only in the instances of using cyberattacks either to preempt a physical war or to improve troop performance on an actual battlefield.

Conclusion

Some 15 years ago, I co-led a U.S. team of cyberexperts that met with our Russian counterparts to discuss the looming threat of war in and from the virtual domain. These talks were thoughtful and wide-ranging, and culminated in a Russian request that we consider adopting a behavior-based set of constraints on the practice of cyberwar (e.g., not targeting civilian infrastructures). The approach was to be modeled on the chemical and biological weapons conventions, signatories to which could easily acquire such capabilities but who agreed to refrain from developing or using them. I was very supportive of this notion. The U.S. government was not, largely because of the belief that the United States was far ahead of Russia in the cyberarena and should not be slowed down. Thus, when Russia advanced its notion in the UN—soon after the meeting and at regular intervals in the years since—it was (and continues to be) opposed by U.S. policy makers.[23] The irony of the situation is that there is a global consensus among cyberexperts today that the Russians have become extremely capable cyberwarriors.

We now live in a world of emerging cyberwars. Indeed, the resounding message of cyberspace-based acts of disruption in Estonia, Georgia, and Iran is that conflicts will now be regularly waged in and from the virtual domain. The record of the past several years reflects the emergence of the global atmosphere George Quester considered the most unstable: a world in which taking the offensive is attractive. In addition, senior leaders in a number of countries have adopted the point of view that cyberwarfare is a very practical option in a crisis. This may be so, but in a world full of rich and inviting targets, allowing the spread of an attitude permissive of cyberwar is probably the last thing we need.

As one of the progenitors of cyberwar, I am mortified by the eagerness of many to use this mode of conflict against other societies. David Ronfeldt and I based our original vision of cyberwar on the belief that the role of advanced information technologies was growing to the point that skillful disruption would make it difficult for a military to fight at all—especially with any kind of real power or cohesion. Thus, wars in which a decisive "information edge" was achieved would be shorter and less bloody—a seemingly good development. The reality, however, is that cyberwar as a form of strategic attack on national infrastructures quickly overshadowed our original vision. The idea of using "cybotage" as a tool of "strategic special operations" emerged as a complement to the larger notion of waging infrastructural warfare. To date, efforts to engage in any kind of arms control have been opposed, principally by the United States. The attempt again led by the United States to deter virtual attacks by means of threats of retaliation in the physical world, will either founder from the outset or exert undue escalatory pressure in crisis and conflict.

The emerging picture of a world bedeviled by cyberwars is a dark one. However, it can be brightened by good sense and circumspection, and by the willingness to work toward the aforementioned behavior-based cyberarms control regime. It will only take one willing U.S. president to start the process of changing course. But such a move would prove most beneficial in reining in other nations that might be growing eager, or at least willing, to conduct acts of cyberwar. A behavior-based arms control agreement would not solve all outstanding problems—nor would it prevent battlefield uses—as such a treaty would be aimed primarily at nations. Networks will prove harder to deal with or deter from engaging in such acts, but not impossible if our overall approach to diplomacy eventually goes beyond traditional statist constructs.

Indeed, since social networks have risen to considerable power at the same time as the emergence of cyberwar, it is now incumbent upon world leaders to learn how to work with them. Networks, whether they are of civil or "uncivil" society, have few of the vulnerabilities or constraints that nations do. The greater freedom of action that networks enjoy should thus impel nation-states to provide models of good behavior when it comes to cyberwar. If instead nations take a permissive view of cyberwar in general, or encourage "sharp practices" like the Stuxnet attack, then an era of massive and costly disruption to advanced information systems and the infrastructures they control will soon be upon us.

Notes

1. George H. Quester, *Offense and Defense in the International System* (New York: John Wiley and Sons, 1977), 2.
2. The best study of this remains Carlo M. Cipolla, *Guns, Sails, and Empires: Technological Innovation and the Early Phases of European Expansion, 1400–1700* (New York: Pantheon Books, 1965).
3. Paul A. Colinvaux, *The Fates of Nations: A Biological Theory of History* (New York: Simon & Schuster, 1980), 353.
4. Jack L. Snyder, *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914* (Ithaca, NY: Cornell University Press, 1984).
5. Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2 (1978): 186.

6. Richard A. Clarke and Robert Knake, *CyberWar: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010); George H. Quester, "Guerrilla Revolution: Undeterrable War," in *Offense and Defense in the International System* (New York: John Wiley and Sons, 1977).

7. Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 101.

8. Our original discussion of cyberwar came in a RAND paper we began writing in 1991 that was circulated in 1992 and later appeared as: John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (Spring 1993): 141–165.

9. James Adams, *The Next World War: Computers are the Weapons and the Front Line is Everywhere* (New York: Simon & Schuster, 1998), 97.

10. Gregory J. Rattray, "Development of U.S. Strategic Airpower, 1919–1945: Challenges, Execution and Lessons," in *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001).

11. Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, CA: RAND Corporation, 1996).

12. Given that most information technology can be used to conduct acts of cyberwar, attempts to control the spread of these "weapons" would be futile. However, behavior can be controlled (e.g., with a pledge of "no first use" of strategic cyberattacks against civilian infrastructure).

13. Lucien S. Vandenbroucke, *Perilous Options: Special Operations as an Instrument of U.S. Foreign Policy* (New York: Oxford University Press, 1993).

14. On the declining utility of such operations near the Cold War's end, see: Gregory F. Treverton, *Covert Action: The Limits of Intervention in the Postwar World* (New York: Basic Books, 1987).

15. Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca, NY: Cornell University Press, 1996).

16. On this conflict, see: Stephen Blank, "Web War I: Is Europe's First Information War a New Kind of War?" *Comparative Strategy* 27, no. 3 (May 2008): 227-47.

17. John Markoff, "Georgia Takes a Beating in the Cyberwar with Russia," *New York Times,* August 11, 2008.

18. For an excellent overview of Just War Doctrine, see: Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, rev. ed. (1977; repr., New York: Basic Books, 2006).

19. Siobhan Gorman and Julian E. Barnes, "CyberCombat: Act of War," *Wall Street Journal*, May 31, 2011.

20. Cited in Timothy Thomas, "The Threat of Information Operations: A Russian Perspective," in *War in the Information Age*, ed. Robert Pfaltzgraff and Richard Shultz (London: Brassey's, 1997), 6-7.

21. Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), 190.

22. "Cyberwar: War in the Fifth Domain," *The Economist*, July 1, 2010.

23. These events have been described in John Markoff and Andrew E. Kramer, "U.S. and Russia Differ on a Treaty for Cyberspace," *New York Times*, June 27, 2009.