Cyberwar and Peace

Hacking Can Reduce Real-World Violence

Thomas Rid

Cyberwar Is Coming!" declared the title of a seminal 1993 article by the RAND Corporation analysts John Arquilla and David Ronfeldt, who argued that the nascent Internet would fundamentally transform warfare. The idea seemed fanciful at the time, and it took more than a decade for members of the U.S. national security establishment to catch on. But once they did, a chorus of voices resounded in the mass media, proclaiming the dawn of the era of cyberwar and warning of its terrifying potential. In February 2011, then CIA Director Leon Panetta warned Congress that "the next Pearl Harbor could very well be a cyberattack." And in late 2012, Mike McConnell, who had served as director of national intelligence under President George W. Bush, warned darkly that the United States could not "wait for the cyber equivalent of the collapse of the World Trade Centers."

Yet the hype about everything "cyber" has obscured three basic truths: cyberwar has never happened in the past, it is not occurring in the present, and it is highly unlikely that it will disturb the future. Indeed, rather than heralding a new era of violent conflict, so far the cyber-era has been defined by the opposite trend: a computer-enabled assault on political violence. Cyberattacks diminish rather than accentuate political violence by making it easier for states, groups, and individuals to engage in two kinds of aggression that do not rise to the level of war: sabotage and espionage. Weaponized computer code and computer-based sabotage operations make it possible to carry out highly targeted attacks on an adversary's technical systems without directly and physically harming human operators and managers. Computer-assisted attacks

THOMAS RID is a Reader in War Studies at King's College London. His most recent book is *Cyber War Will Not Take Place* (Oxford University Press, 2013), from which this essay is adapted. Follow him on Twitter @RidT.

make it possible to steal data without placing operatives in dangerous environments, thus reducing the level of personal and political risk.

These developments represent important changes in the nature of political violence, but they also highlight limitations inherent in cyber-weapons that greatly curtail the utility of cyberattacks. Those limitations seem to make it difficult to use cyberweapons for anything other than one-off, hard-to-repeat sabotage operations of questionable strategic value that might even prove counterproductive. And cyber-espionage often requires improving traditional spycraft techniques and relying even more heavily on human intelligence. Taken together, these factors call into question the very idea that computer-assisted attacks will usher in a profoundly new era.

THE THIN CASE FOR CYBERWAR

One reason discussions about cyberwar have become disconnected from reality is that many commentators fail to grapple with a basic question: What counts as warfare? Carl von Clausewitz, the nineteenth-century Prussian military theorist, still offers the most concise answer to that question. Clausewitz identified three main criteria that any aggressive or defensive action must meet in order to qualify as an act of war. First, and most simply, all acts of war are violent or potentially violent. Second, an act of war is always instrumental: physical violence or the threat of force is a means to compel the enemy to accept the attacker's will. Finally, to qualify as an act of war, an attack must have some kind of political goal or intention. For that reason, acts of war must be attributable to one side at some point during a confrontation.

No known cyberattack has met all three of those criteria; indeed, very few have met even one. Consider three incidents that today's Cassandras frequently point to as evidence that warfare has entered a new era. The first of these, a massive pipeline explosion in the Soviet Union in June 1982, would count as the most violent cyberattack to date—if it actually happened. According to a 2004 book by Thomas Reed, who was serving as a staffer on the U.S. National Security Council at the time of the alleged incident, a covert U.S. operation used rigged software to engineer a massive explosion in the Urengoy-Surgut-Chelyabinsk pipeline, which connected Siberian natural gas fields to Europe. Reed claims that the cla managed to insert malicious code into the software that controlled the pipeline's pumps and valves. The rigged valves supposedly resulted in an explosion that, according to

Reed, the U.S. Air Force rated at three kilotons, equivalent to the force of a small nuclear device.

But aside from Reed's account, there is hardly any evidence to prove that any such thing happened, and plenty of reasons to doubt that it did. After Reed published his book, Vasily Pchelintsev, who was reportedly the KGB head of the region when the explosion was supposed to have taken place, denied the story. He surmised that Reed might have been referring to a harmless explosion that happened not in June but on a warm April day that year, caused by pipes shifting in the thawing ground of the tundra. Moreover, no Soviet media reports from 1982 confirm that Reed's explosion took place, although the Soviet media regularly reported on accidents and pipeline explosions at the time. What's more, given the technologies available to the United States at that time, it would have been very difficult to hide malicious software of the kind Reed describes from its Soviet users.

No known cyberattack has met Clausewitz's definition of an act of war.

Another incident often related by promoters of the concept of cyberwar occurred in Estonia in 2007. After Estonian authorities decided to move a Soviet-era memorial to Russian soldiers who died in World War II from the center of Tallinn to the city's outskirts, outraged Russian-speaking Estonians launched violent riots that threatened to paralyze the city. The riots were accompanied by cyber-assaults, which began as crude disruptions but became more sophisticated after a few days, culminating in a "denial of service" attack. Hackers hijacked up to 85,000 computers and used them to overwhelm 58 Estonian websites, including that of the country's largest bank, which the attacks rendered useless for a few hours.

Estonia's defense minister and the country's top diplomat pointed their fingers at the Kremlin, but they were unable to muster any evidence. For its part, the Russian government denied any involvement. In the wake of the incident, Estonia's prime minister, Andrus Ansip, likened the attack to an act of war. "What's the difference between a blockade of harbors or airports of sovereign states and the blockade of government institutions and newspaper websites?" he asked. It was a rhetorical question, but the answer is important: unlike a naval blockade, the disruption of websites is not violent—indeed, not even potentially violent. The choice of targets also seemed unconnected

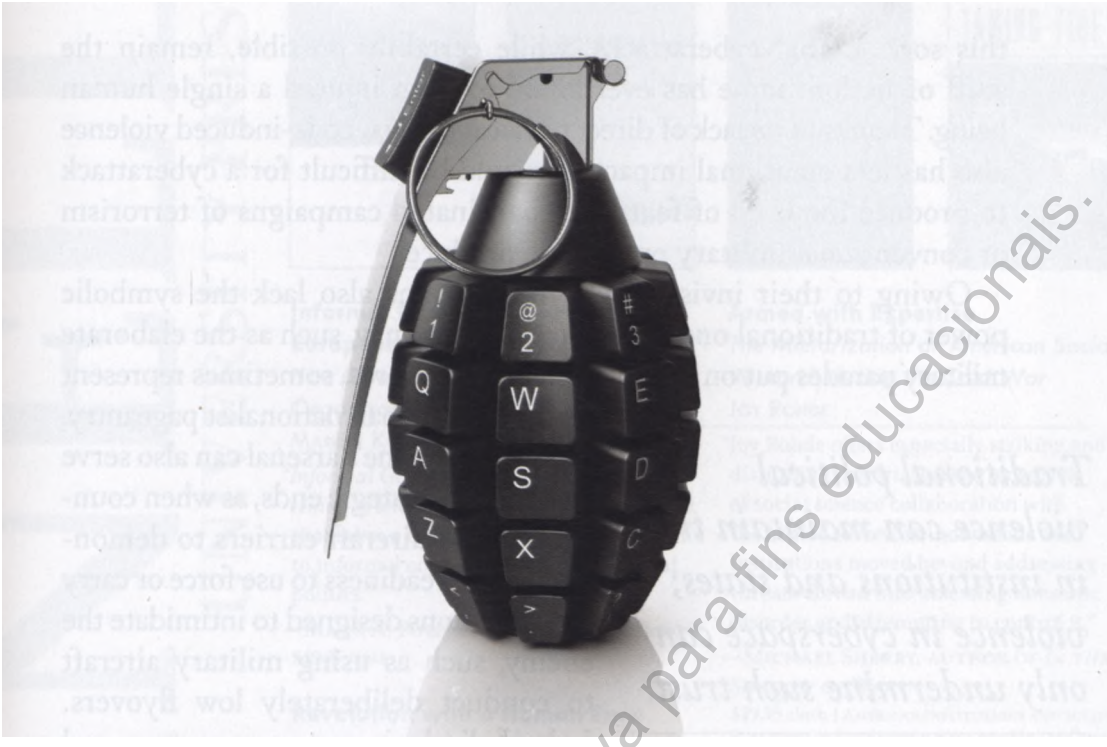
to the presumed tactical objective of forcing the government to reverse its decision on the memorial. And unlike a naval blockade, the attacks remained anonymous, without political backing, and thus unattributable.

A year later, a third major event entered the cyber-Cassandras' repertoire. In August 2008, the Georgian army attacked separatists in the province of South Ossetia. Russia backed the separatists and responded militarily. The prior month, in what might have been the first time that an independent cyberattack was launched in coordination with a conventional military operation, unknown attackers had begun a campaign of cyber-sabotage, defacing prominent Georgian websites, including those of the country's national bank and the Ministry of Foreign Affairs, and launching denial-of-service attacks against the websites of Georgia's parliament, its largest commercial bank, and Georgian news outlets. The Georgian government blamed the Kremlin, just as the Estonians had done. But Russia again denied sponsoring the attacks, and a NATO investigation later found "no conclusive proof" of who had carried them out.

The attack set off increasingly familiar alarm bells within American media and the U.S. national security establishment. "The July attack may have been a dress rehearsal for an all-out cyberwar," an article in *The New York Times* declared. Richard Clarke, a former White House cybersecurity czar, warned that the worst was yet to come: the Georgian attack did not "begin to reveal what the Russian military and intelligence agencies could do if they were truly on the attack in cyberspace." Yet the actual effects of these nonviolent events were quite mild. The main damage they caused was to the Georgian government's ability to communicate internationally, thus preventing it from getting out its message at a critical moment. But even if the attackers intended this effect, it proved short-lived: within four days after military confrontations had begun in earnest, the Georgian Foreign Ministry had set up an account on Google's blog-hosting service. This move helped the government keep open a channel to the public and the news media. What the Internet took away, the Internet returned.

IN CODE WE TRUST?

Perhaps the strongest evidence presented by advocates of the concept of cyberwar is the Stuxnet operation launched against Iran by the United States and Israel. Stuxnet, part of a set of attacks known as Operation Olympic Games, was a sophisticated multiyear campaign



Overblown: keyboard as grenade

to sabotage Iran's nuclear enrichment facility in Natanz by inserting a harmful computer worm into the software that ran the facility's centrifuges, causing them to overload. American and Israeli developers started designing the project as early as 2005, and it launched in 2007, growing more sophisticated until its discovery in 2010. The attack was groundbreaking in several ways. The developers built highly target-specific intelligence into the code, enabling the Stuxnet software to make autonomous decisions in its target environment. Most important, Stuxnet represented the first and only physically destructive cyberattack launched by one state (or, in this case, two states) against another.

Yet even cyberattacks that cause damage do so only indirectly. As an agent of violence, computer code faces a very basic limit: it does not have its own force or energy. Instead, any cyberattack with the goal of material destruction or harming human life must utilize the force or energy embedded in its target: for example, shutting down an air traffic control system and causing trains or planes to crash or disrupting a power plant and sparking an explosion. Yet besides Stuxnet, there is no proof that anyone has ever successfully launched a major attack of

this sort. Lethal cyberattacks, while certainly possible, remain the stuff of fiction: none has ever killed or even injured a single human being. Thanks to its lack of direct physical impact, code-induced violence also has less emotional impact. It would be difficult for a cyberattack to produce the level of fear that coordinated campaigns of terrorism or conventional military operations produce.

Owing to their invisibility, cyberweapons also lack the symbolic power of traditional ones. Displays of weaponry, such as the elaborate military parades put on by China and North Korea, sometimes represent nothing more than nationalist pageantry. But revealing one's arsenal can also serve tactical and strategic ends, as when countries deploy aircraft carriers to demonstrate their readiness to use force or carry out operations designed to intimidate the enemy, such as using military aircraft to conduct deliberately low flyovers. Indeed, displaying weapons systems and threatening to use them can prove more cost-efficient than their actual use. But cyberweapons are hard to brandish.

Traditional political violence can maintain trust in institutions and states; violence in cyberspace can only undermine such trust.

Perhaps the most crucial limitation of violence in cyberspace is its almost entirely destructive quality: unlike traditional political violence, which can maintain trust in institutions and states as well as undermine it, violence in cyberspace can do only the latter. Any established political order comes with a certain degree of inherent violence; consolidated states, after all, survive only if they maintain monopolies on the legitimate use of force. By encouraging trust in the ability of state institutions to protect property and safeguard citizens, this inherent violence buttresses a state's power and allows the state to establish the rule of law. But cyber-violence lacks this ability, since it does little or nothing to build up trust in institutions; indeed, it is very difficult to imagine how cyberattacks could be used to enforce rules or laws, either domestically or internationally. Digital surveillance presents a more complicated picture. In democracies, intelligence agencies tread a thin line between providing security and eroding public trust in the state, as demonstrated by the recent controversy over the U.S. National Security Agency's data-collection practices. In authoritarian countries, digital surveillance can assist the state's coercive use of force, but it cannot replace it.

Such limitations, however, should not lead anyone to dismiss the corrosive potential of cyberattacks. Indeed, such assaults can undermine social trust in a more direct way than traditional political violence. Cyberattacks are more precise; they do not necessarily undermine the state's monopoly of force in a wholesale fashion. Instead, they can be tailored to attack specific companies or public-sector organizations and used to undermine those groups' authority selectively. Stuxnet provides a good example of this dynamic. Putting aside the question of whether the attack was an act of war, its primary intention was to undermine the trust of the Iranian scientists in their systems and in themselves and the trust of the Iranian regime in its ability to build nuclear weapons. The original intention was to cause physical damage to as many Iranian centrifuges as possible. But the American and Israeli attackers knew that the physical effect could be exploited to unleash a much more damaging psychological effect. "The intent was that the failures should make them feel they were stupid, which is what happened," an American participant told *The New York Times.*

The Americans and the Israelis hoped that once a few machines failed, the Iranian engineers would shut down more machines because they distrusted their own technology or indeed their own skills. At the headquarters of the International Atomic Energy Agency, in Vienna, rumors circulated that the Iranians had lost so much confidence in their own systems and instruments that the management of the Natanz facility took the extraordinary step of assigning engineers to sit in the plant and radio back what they saw to confirm the instrument readings. "They overreacted," one of the attackers revealed to David Sanger of *The New York Times,* "and that delayed them even more." The Iranians also began to assign blame internally, pointing fingers at one another and even firing some personnel.

DIGITAL UNDERGROUND

Damaging though it may have been, Stuxnet, along with the cyber-scuffles in Estonia and Georgia, represents not a new form of warfare but something more akin to other, less lethal forms of aggression: sabotage and espionage. Unlike acts of war, these political crimes, which are often committed by nonstate actors, need not be violent to work. And although saboteurs and spies do act politically, they often seek to avoid attribution, unlike those who launch acts of war.

For those reasons, the cyber-era has been a boon for political crime. Consider sabotage. Before the computer age, saboteurs had trouble calibrating and controlling the effects of their actions. Sabotage had to target physical property and relied on physical violence, which often proves unpredictable. During postal and railway strikes in France in 1909 and 1910, for instance, saboteurs cut signal wires and tore down telegraph posts. Destroying property risked running afoul of public opinion, and the tactic ultimately divided the workers. The strikes themselves, as a form of sabotage, also ran the risk of leading to unpredictable violence: indeed, labor demonstrations often intensified into riots, making it easier for opponents to portray the strikers as uncompromising radicals.

It is much easier for saboteurs to avoid counterproductive side effects in the age of computer-assisted attacks, which can contain violence and generally avoid it altogether. Cyberattacks can maliciously affect software and business processes without interfering with physical industrial processes, remaining nonviolent but sometimes still causing greater damage than a traditional assault. A 2012 attack against the computer network of the oil company Saudi Aramco illustrates this potential. The attack physically harmed neither hardware nor humans. Yet by allegedly erasing the hard disks of some 30,000 computers, the attackers likely did much more monetary damage to Saudi Aramco than they could have through an act of traditional sabotage against machinery in one of the company's plants. The oil giant reportedly had to hire six specialized computer security firms to help with its forensic investigation and post-attack cleanup.

Despite such potential, it is also important to remember the inherent limitations of computer-assisted political crime and to note that human agents remain critical in the age of digital violence. Even Stuxnet, the most successful example of cyber-sabotage, demonstrates this fact. For the United States and Israel, the "holy grail," in the words of one of the attack's architects, was getting a piece of malicious software into the control system at Natanz. The Americans and Israelis needed fine-grained data from inside the Iranian plant to develop their weaponized code. The problem was that the control system was protected by an air gap: it was not connected to the Internet or even internal networks. As a result, the attackers had to deliver the malicious code via a removable hard drive such as a usb flash drive—delivered by a human hand.

To make this happen, U.S. intelligence operatives first obtained a list of the people who were visiting the targeted plant to work on its computer equipment and who could carry the payload there. "We had to find an unwitting person on the Iranian side of the house who could jump the gap," one planner later told Sanger. The list of possible carriers included engineers from the German company Siemens, who were helping their Iranian colleagues maintain the control system—work that required the Siemens engineers to bring portable computers into the plant. Precisely how the U.S.-Israeli team managed to exploit this vulnerability remains unknown. Suffice it to say that although "Siemens had no idea they were a carrier," in the words of one U.S. official quoted by Sanger, "it turns out there is always an idiot around who doesn't think much about the thumb drive in their hand."

SAFETY IN ONES AND ZEROS

If cyberattacks reduce the amount of violence inherent in conflict, and if they often take the form of sabotage or espionage, then many officials and commentators who have been warning about the dawn of cyberwar have been ringing false alarms. Digital violence does have implications for ethics and for national security strategy, however. Weaponized code, or cyberattacks more generally, can achieve goals that used to require conventional force. The most sophisticated cyberattacks are highly targeted, and cyberweapons are unlikely to cause collateral damage in the same way conventional weapons do. Therefore, in many situations, the use of computers would be ethically preferable to the use of conventional weapons: a cyberattack might be less violent, less traumatizing, and more limited.

A comparable dynamic applies to the ethics of cyber-espionage. Intelligence might be gained by infiltrating computer systems and intercepting digital signals, or it might be acquired by sneaking human spies, sometimes armed, into hostile territory at personal risk, or it might be got by interrogating suspects under harsh conditions. Depending on the case, computer espionage might be ethically preferable to any of the other options.

A cyberattack will not always be the strategically sound option, however. Indeed, even the celebrated Stuxnet operation was not necessarily a strategic success. The attack was designed to slow and delay Iran's nuclear enrichment program and undermine the Iranian government's trust in its ability to develop a nuclear weapon. The attack

might well have achieved those goals in the short term. But as soon as the malfunctions and delays were traced to sabotage, the psychological effect of the operation likely changed, as the Iranians could reassure themselves that they were not "stupid" and that they were faced with aggressive foreign adversaries. They now knew that the problem was not their own ineptitude; somebody else was doing this to them.

In an ongoing confrontation, such as the one over Iran's nuclear program, cyberattacks might yield valuable intelligence, but they likely possess very little coercive value. Consider that during the Cold War, the United States stationed hundreds of thousands of ground forces in West Germany and other areas bordering the Soviet bloc to communicate that Washington was alert and technically sophisticated, as well as serious about attacking if Moscow crossed a redline. A contemporary counterproliferation approach that relied on cyberattacks, by contrast, might send an altogether different message to the Iranians: that Washington is alert and technically sophisticated, but not really serious about attacking, even if Tehran does cross a redline. After all, a standalone cyberattack would not likely put the lives of U.S. personnel in peril, a fact that could signal a lower level of commitment.

THE WORST DEFENSE

Earlier this year, the Pentagon announced that it would boost the staff of its Cyber Command from 900 to 4,900 people, most of whom would focus on offensive operations. William Lynn, formerly the Pentagon's second-in-command, responded to critics of the move by assuring the public that the Department of Defense would not militarize cyberspace. "Indeed," Lynn said, "establishing robust cyberdefenses no more militarizes cyberspace than having a navy militarizes the ocean."

In a sense, Lynn is right: cyberspace has not been militarized, precisely because the U.S. government, along with many other governments, has not actually established robust cyberdefenses. Defending against cyber-sabotage means hardening computer systems, especially those that control critical infrastructure. But such systems remain staggeringly vulnerable. Defending against cyber-espionage means avoiding the large-scale theft of sensitive data from companies and government agencies. But as illustrated by the recent leaks of classified information regarding the National Security Agency's domestic surveillance, Western intelligence agencies are only now beginning to

understand digital counterespionage and the proper role of human informants in a digitized threat environment.

What has been militarized is the debate about cyberattacks, which is dominated by the terminology of warfare. What appears as harmless inconsistency—constantly warning of cyberwar's dangers while neglecting to protect against them—masks a knotty causal relationship: for a number of reasons, loose talk of cyberwar tends to overhype the offensive potential of cyberattacks and diminish the importance of defenses. First, it encourages the false idea that two states exist: cyberwar and cyberpeace. In fact, the threat of a cyberattack is ever present and will not go away. Second, when U.S. military officials hype cyberwar, it leads the public to believe that the Pentagon is in charge of dealing with the threat. In fact, companies and individuals need to take responsibility for their own security. And finally, advocates of the concept of cyberwar often suggest that the best defense is a good offense. That is not the case: consider, for example, that designing the next Stuxnet will not make the U.S. energy grid any safer from digital attacks. To avoid further distorting the issue, the debate over cyberattacks must exit the realm of myth.

Fonte: Foreign affairs, New York, v. 92, n. 6, p. 77-87, nov./ dec. 2013.