BLOG@CACM

The Ethics of Cyberwar

By John Arquilla
July 2, 2015
Comments

All over the world, there is a growing sense that conflict is spreading from the physical realm to the virtual domain. The 2007 cyber attacks on Estonia, the military use of cyberwar techniques in the 2008 Russo-Georgian War, and the act of "cybotage" committed against Iran's nuclear program using the Stuxnet worm are but a few of the most salient signs of a growing trend. And these likely form just the tip of an iceberg, as cyber attacks and counter-attacks ongoing between combatants can be observed in many other places, from Ukraine to the Middle East, and on to East Asia and beyond. Thus it is high time, as this new mode of conflict diffuses in breadth and deepens in intensity, to think through the ethics of cyberwar.

Under what conditions should one engage in cyberwar? How should such a conflict be waged? These questions speak to the classical division in ethical thought about warfare that addresses first the matter of going from peace to war justly, then ponders how to fight one's battles honorably. Ideas about "just wars" go back many centuries and derive from diverse cultures. In terms of going to war justly, there are three commonly held principles: *Right purpose,* which refers mostly to acting in self-defense; *Due authority* seeks authorization from a national or supra-national body; and *Last resort,* which is self-explanatory. Ideas of fighting justly cluster around: *Noncombatant immunity,* i.e., a focus on military v. civilian targets; and *Proportionality,* avoiding excessive force.

Right purpose has always been a very fraught element of just-war theory – and practice. As Napoleon once said, "I had to conquer Europe to defend France." Many military adventures follow a similar logic, justifying acts of aggression as pre-emptive or preventive defensive actions. Stuxnet would fall in the ethically dodgy area of prevention, and one can easily see how cyber attack, such a seemingly usable, low-risk option, may move nations ever more in the direction of pre-emptive and preventive action. Not good.

Due authority, until the Information Age, was fairly neatly confined to nations, coalitions, or even transnational bodies like the United Nations. For example, NATO made choices to intervene militarily in Kosovo in 1999, and in recent years in Libya. The U.N. authorized action to repel invading North Korean forces in 1950. And so on. This category includes and allows ethical choices to go to war made by individual nations as well – even when a choice might well have been made in error (like the American war against Iraq in 2003, whose justification was the mistaken belief of some that Saddam Hussein had, or soon would have, weapons of mass destruction). In the realm of cyberwar, "due authority" suffers terribly because field armies, navies, and air forces are not necessary; just malicious software and skilled hackers. "Authority" loses meaning in a world where aggressive networks, or even highly adept individuals, can wage cyberwar.

Last resort typically has referred to a requirement, before going to war, to pursue diplomatic efforts until it is clear they will not resolve a given crisis. This aspect of just-war theory has also proved a bit nebulous, as it seems that sometimes war is resorted to because one or another party to a dispute just gets tired of negotiating. The July Crisis of 1914 that led to World War I falls in this category. The Japanese-American talks

in the fall of 1941 were frustrating enough to Tokyo that the choice was made to attack Pearl Harbor even before diplomatic talks had ended. When it comes to cyberwar, its fundamentally covert, deniable nature may mean that it will be used even *during* negotiations – which was clearly the case with the use of Stuxnet.

Noncombatant immunity is the principle that calls for avoiding the deliberate targeting of civilians. Over the past century, it has been outflanked by those technologies – aircraft and missiles – that allow for the innocent to be struck directly, without the prior need to defeat the armed forces that protect them. Thus World War II saw the deliberate burning of many cities – and nuclear attacks on civilians in Japan as soon as the atomic bomb became available. During the Korean War virtually every building in Pyongyang was flattened, and a greater weight of bombs fell on North Vietnam in "the American War" than were dropped on Hitler's Germany. How will this principle play out in an era of cyberwar? With far less lethal harm done to noncombatants, but no doubt with great economic costs inflicted upon the innocent.

Proportionality has proved a less difficult principle to parse over the past century or so. By and large, nuclear-armed nations have refrained from use of ultimate weapons in their wars against others not so armed. Korea stayed a conventional conflict; Vietnam, too, even though the outcomes of both for the nuclear-armed United States were, in the former case an uneasy draw, in the latter an outright defeat. A more recent example would be of the military skirmishing between India and Pakistan over Kashmir, where neither side has shown any inclination to act in a disproportionate manner. In the case of cyberwar, the principle of proportionality may play out more in the type of action taken, rather than in the degree of intensity of the action. Thus a cyber counter-attack in retaliation for a prior cyber attack will, generally, fall under the proportionality rubric. When might a cyber attack be answered with a physically destructive military action? The United States and Russia have both elucidated policies suggesting the possibility they might respond to a "sufficiently serious" cyber attack by other-than-cyber means.

Overall, it seems that classical ideas about waging war ethically remain quite relevant to the emerging strategic and policy discourses on cyberwar. That said, it is clear that conflict in and from the virtual domain should impel us to think in new ways about these principles. In terms of whether to go to war at all, the prospects may prove most troubling, as cyber capabilities may encourage pre-emptive action, and may also erode the notion of "war" as a tool only of last resort. But when it comes to strictures against targeting civilians – so often violated in traditional war-fighting – cyberwar may provide a means of causing costly disruption without killing many, perhaps not even any, civilians. Yet there are other problems, as when networks of non-state actors can easily outflank the "authority" principle, and when frustrated nations might deliberately employ disproportionate physical force in response to a virtual attack.

Back in 1899, when advances in modern weapons technologies made many leaders wary of the looming costs and dangers of war, a conference was held at The Hague to codify the ethics and laws of armed conflict. It was then followed up with a subsequent meeting on the same subject in 1907. Perhaps it is time to go back to The Hague again, given that a new realm of virtual conflict has emerged. Even if we cannot fully live up to the ethical ideals that might be set and agreed upon in such a gathering, it is imperative that the world community should make the effort. Now.

No entries found