Cyberwars Already Underway With No Geneva Conventions To Guide Them

By **Peter Fowler** at 14 Oct 2010

A University at Buffalo military ethicist says we have good reason to worry about an escalation in Cyberwars, because cyber attacks are almost entirely unaddressed by traditional morality and laws of war.

Cyber attacks of various sorts have been around for decades. The most recent, and very dangerous, escalation in the past few years has been marked by countries launching attacks against other nations, such as Stuxnet, the nuclear plant-disrupting worm the Iranians have blamed on Israel and the U.S., while others are pointing the finger at Russia.

University at Buffalo military ethicist Randall R. Dipert, PhD, one of the founders of the National Center for Ontological Research at UB, says cyber attacks are not covered by an convesntions of law.

"The urge to destroy databases, communications systems and power grids, rob banking systems, darken cities, knock manufacturing and health-care infrastructure off line and other calamitous outcomes are bad enough," says Dipert.

"But unlike conventional warfare, there is nothing remotely close to the Geneva Conventions for cyberwar. There are no boundaries in place and no protocols that set the standards in international law for how such wars can and cannot be waged," he says.

"In fact," he says, "terms like 'cyber attack,' 'cyberwarfare' and "cyberwar,'" -- three different things with different characteristics and implications -- are still used interchangeably by many, although they are three distinct entities."

Dipert points out that while the U.S. isn't the only target, it is a huge target and "our massive systems offer the biggest payoffs for those who compromise them."

Dipert, C.S. Peirce Professor of American Philosophy at UB and a former West Point philosopher, examined many aspects of this issue in his paper "Ethical Issues of Cyberwarfare," first published on the website of the Consortium for Emerging Technologies, Military Operations and National Security, or CETMONS.

CETMONS is a multi-institutional organization concerned with the ethical, rational and responsible understanding and management of complex issues raised by emerging technologies, their use in military operations and their broader implications for national security. He presented a more comprehensive paper at the U.S. Naval Academy, which is due to be published soon by the Journal of Military Ethics.

Dipert points to a few of the many fronts on which the war has already begun: on components of U.S. defense cyber-infrastructure; cyber attacks by Russia on Estonia and Georgia; recent probable attacks by China, North Korea and Iran on U.S. defense and economic targets, well-organized attacks by China on corporate targets, Google and Gmail; and this month, the suspected Stuxworm attacks.

"There has been intentional cyberharm for decades," he says, "including damage perpetrated by apolitical and anarchic ("black") hackers and economically motivated industrial cyberespionage agents."

We think we have some idea of what "can" happen, but Dipert says, but there is a large array of possible scenarios for which there do not exist obvious moral reasoning or even straightforward analogies that could guide us.

"For instance," he says, "traditional rules of warfare address inflicting injury or death on human targets or the destruction of physical structures. But there are no rules or restrictions on 'soft-' or 'cyber-' damage, damage that might not destroy human beings or physical structures as objects.

"But," he says, "intentional destruction or corruption of data and/or algorithms and denial-of-service attacts could cause tremendous harm to humans, machines, artificial systems or the environment -- harm that could make entirely civilian systems that are necessary for the well being of the population inoperable for long periods of time.

"Second," he says, "I am disturbed by the extent to which, through easy Internet access, much of our economic and defense informatics infrastructure is vulnerable to cyber attack.

"This is due, in part," Dipert says, "to our departure from the relatively secure Arpanet (one of the networks that came to compose the global Internet) for use in defense operations to a wide-open Internet that doesn't have one relatively secure hard-wired Ethernet portal, but a variety of possible portals accessible by numerous international routes.

"Third," Dipert says, "Gen. Keith Alexander, director of the National Security Agency, who also heads Cyber Command, a new full command instituted by the U.S. Department of Defense, has indicated that serious thought is being devoted to the development of cyberwarfare policy and strategy.

"To date, however, this has been shrouded in secrecy," he says, "which is a serious problem because if they are to have a deterrent effect, it is absolutely necessary to make some policy elements public."

Finally, Dipert points out that cyberwarfare is such a new and difficult domain that traditional ethical and political theories with which we frame disputes -- utilitarianism, Kantian theory or natural rights theory -- cast little light on this particular one.

"It has been my working assumption that to fully understand the moral constraints of warfare requires us to understand certain conclusions from game theory and work them into traditional thinking about war," Dipert says.

He points out that similar reasoning in game theory guided the nuclear powers through the earlier years the Cold War, when there was little idea of how to use these weapons defensively or offensively.

What we need today, he says, and what scholars, military personnel and governments are trying to come up with, are policies, doctrines and strategies that cover cyberwarfare; an understanding of Just War Theory for cyberwarfare; new concepts and principles of morality for cyberwarfare; and some agreement as to whether and how such warfare is subject to international and customary law.

"I would predict that what we face today is a long Cyber Cold War, marked by limited but frequent damage to information systems, while nations, corporations and other agents test these weapons and feel their way toward some sort of equilibrium," Dipert says.

The University at Buffalo is a premier research-intensive public university, a flagship institution in the State University of New York system and its largest and most comprehensive campus. UB's more than 28,000 students pursue their academic interests through more than 300 undergraduate, graduate and

CATEGORIES

- US Politics and Govt
- Business
- SciTech
- Sports
- World
- Entertainment
- USA News
- Weather
- Media
- Gulf Oil Spill
- News Content For Sale

professional degree programs. Founded in 1846, the University at Buffalo is a member of the Association of American Universities.

Categories: Computers and Internet General SciTech General US News Military SciTech USA News

Tags: Cyberwars Cyber attacks Cyber Cold War Stuxnet