Rogue cyberwars don't follow rules

Posted By Patricia Donovan-Buffalo On October 14, 2010 @ 3:11 pm In Society & Culture | 1 Comment

U. BUFFALO (US) — Because cyber attacks are almost entirely unaddressed by traditional morality and laws of war, their recent escalation is particularly concerning, according to a new report.

"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 Randall Dipert, professor of American philosophy at the University at Buffalo. [1]

"But unlike conventional warfare, there is nothing remotely close to the Geneva Convention 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."

"In fact, 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."

While the U.S. isn't the only target, the country's "massive systems offer the biggest payoffs for those who compromise them."

Dipert's paper was first published on the Web site of the Consortium for Emerging Technologies, Military Operations and National Security, or CETMONS. [2]

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 in the *Journal of Military Ethics.* [3]

The war has already begun on several fronts, Dipert says, including 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, the nuclear plant-disrupting worm the Iranians have blamed on Israel and the U.S., while others are pointing the finger at Russia.

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

Experts have some idea of what could happen, but there is a large array of possible scenarios for which obvious moral reasoning or even straightforward analogies don't exist, Dipert says.

"For instance, 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, intentional destruction or corruption of data and/or algorithms and denial-of-service attacks 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.

"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, to the 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, 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," Dipert 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."

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—offer few answers.

"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."

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."

More news from University at Buffalo: http://www.buffalo.edu/news/ [4]

URLs in this post:

[1] University at Buffalo.: **http://www.buffalo.edu/news/11862**
[2] CETMONS.: **http://cetmons.org/**
[3] Journal of Military Ethics.: **http://www.tandf.co.uk/journals/journal.asp?issn=1502-7570&linktype=5**
[4] http://www.buffalo.edu/news/: **http://www.buffalo.edu/news/**