Do we need a Geneva convention for cyber warfare?

By Olivia Solon | 15 October 2010 | Categories: Culture

Related

UK Internet is now a £100 billion 'industry'

BICS 2010: A very British Comic Con

Modder creates Portal t-shirt

We should worry about the fact that cyber wars are not dealt with by traditic morality and laws of war, according to military ethicist Randall R. Dipert, Ph the University of Buffalo.

Cyber attacks are nothing new. In 1982, the US reportedly sabotaged the Sibe pipeline through a logic bomb planted in software, causing an explosion. Mo recently we have seen the likes of Stuxnet, the nuclear plant worm that the Iranians have blamed on Israel and the US.

Similarly there have been cyber attacks by Russia on Estona and Georgia, an well-organised attacks by China on corporate targets including Google.

Dipert said: "The urge to destroy databases, communications systems and power grids, rob banking systems, dar cities, knock manufacturing and health-care infrastructure offline and other calamitous outcomes are bad enough unlike conventional warfare, there is nothing remotely close to the Geneva Conventions for cyber war. There are boundaries in place and no protocols that set the standards in international law for how such wars can and canno waged," he says.

Dipert argues that intentional cyberharm stirs up a range of possible scenarios which don't have any obvious mo reasoning or analogies that could guide us. Traditional rules of warfare address inflicting injury or death on hum

or the destruction of physical structures, but there are no rules on "soft" or "cyber" damage that might not destro humans or physical structures.

However, intentional destruction or corruption of data or algorithms and denial-of-service attacks could cause "tremendous harm to humans, machines, artificial systems of the environment" that could render civilian system necessary for people's wellbeing redundant for long periods of time.

He was also concerned about how vulnerable economic and defence systems are to cyber attack, due in part to th shift in global connectivity from the relatively secure Arpanet (a legacy precursor to the internet) to the open inte

Because cyber warfare is such a new domain, the political theories with which we frame disputes -- utilitarianism Kantian theory or natural rights theory -- shed little light on this issue.

Dipert is operating under the working assumption that we need to understand certain conclusions from game the and work them into traditional thinking about war. He points out that similar reasoning in game theory guided t nuclear powers through the earlier years of the Cold War, when there was little idea of how to use these weapons defensively or offensively.

He is keen to get scholars, military personnel and governments to drive policies and doctrines that cover cyber warfare and to agree how such warfare is subject to international law.

Dipert predicts "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".

He examined these issues in his paper, entitled *Ethical Issues of Cyberwarfare*, first published on the website of the Consortium for Emerging Technologies, Military Operations and National Security, or CETMONS.

CETMONS aims to understand the ethical issues raised by emerging technologies, their use in military operations and the broader issues for US national security.

PHOTO CREDIT: Flickr CC: West Point Public Affairs | **ONLINE EDITOR:** Duncan Geere

TAGS: Military | US | Cyber wars | Cyber security | Ethics

Comment

Post comment

NAME

EMAIL ADDRESS