2013-05-04

Cyber Security Hall of Famer Dorothy Denning discusses the ethics of cyber warfare

Stewart, Kenneth; Naval Postgraduate School Public Affairs Office

Monterey, California: Naval Postgraduate School

Cyber Security Hall of Famer Dorothy Denning Discusses the Ethics of Cyber Warfare

Article By: Kenneth A. Stewart

The United Nations Charter prohibits the use of force by one state against another. But in the cyber world, where are the borders and what constitutes force? Naval Postgraduate School (NPS) Defense Analysis Distinguished Professor Dorothy Denning is an icon in the field of information security, but has spent the last several years adding the ethics of cyber warfare to her fields of exploration.

Denning teaches a class titled, "Conflict in Cyber Space" that attempts to address the legal and ethical issues raised by cyber warfare. Her students include members of NPS' recently inaugurated Master of Science in Cyber Systems Operations (CSO) degree program, as well as members of the Joint Information Operations program and others on campus. The CSO program is training the Navy's first generation of cyber warriors.

"We focus on the law of armed conflict as well as issues related to censorship, privacy and surveillance … It is a required course in the CSO program," said Denning.

Denning helps her students to navigate the murky waters of cyber ethics, where battlefields may consist of layers of code rather than the mountains, seas and planes that have historically defined combat areas of operations.

Despite the legal ambiguity of some questions, Denning makes a seemingly powerful case for both the legality and the moral imperative to seek cyber approaches to conventional warfare objectives.

"If you can achieve the same effects with a cyber weapon verses a kinetic weapon, often that option is ethically preferable … If an operation is morally justifiable, than a cyber route is likely preferable, because it causes less harm," said Denning.

Denning and fellow NPS Assistant Professor Bradley Strawser make the argument in a recent paper addressing cyber ethics.

In "Moral Cyber Weapons," Denning and Strawser argue, "At least with some kinds of cyber weapons, not only can they adhere to the principles of just war theory but that a positive duty to employ them can arise, at least in certain contexts … The reason for this moral obligation is that cyber weapons reduce both the risk to one's own military and the harm to one's adversary and non-combatants. Overall, cyber weapons are more humane, less destructive, and less risky than kinetic weapons for achieving certain military effects."

Denning insists that cyber attacks are not as new as they may appear; pointing out that cyber operations have been used in the past in conjunction with kinetic operations.

"When Israel bombed Syria's nuclear facility [in 2007], they used a cyber operation to shut off Syria's missile defense systems," she notes.

Still, Denning notes that the red line in the realm of cyber warfare – which, if crossed, could lead to kinetic warfare – has not been breached.

Distinguished Professor Dorothy Denning has built a legendary resume in the information security arena, but has spent the last several years examining, and teaching, about the ethical challenges of cyber warfare.

"We haven't crossed the threshold where a cyber attack has initiated a kinetic response," said Denning. "What we are seeing primarily is espionage, and we have never responded with military force to espionage."

Much of the espionage that Denning refers to centers on business and economic interests, but Denning is quick to point out that in our global economy, there are limits to what state actors can do without harming their own interests.

"Our interconnected economies serve as a deterrent to cyber sabotage that would damage the economy. I think that a state would be very cautious about damaging another nation's economy because it would likely damage their own economy in the process," said Denning.

The conversation that researchers like Denning and Strawser have initiated at NPS will no doubt continue. The U.S. military and both its allies and foes have made tremendous human and economic capital investments into the burgeoning arena of cyber defense. What will come of these investments remains to be seen, but their ethics and conformity with international law is already an area of particular emphasis within the cyber operations community at NPS.

Posted May 4, 2013