c|net NEWS.COM http://www.news.com/

Perspective: The first 'e-war'

By Declan McCullagh
http://news.com.com/2010-12-983077.html

Story last modified February 3, 2003, 6:20 AM PST

WASHINGTON--Not long ago, I had dinner with a former military officer who participated in information warfare "what-if" exercises that the Pentagon and the White House ran in the late 1990s.

"If Saddam ever attacks the U.S. through the Internet and takes out a telecommunications firm, we'll be in a state of war," my dinner companion told me. "All bets are off. The Fourth Amendment is on hold. If EarthLink is attacked, the Army could show up and seize control of their servers."

That was news to me. Might a shadowy corps of U.S. hacker-soldiers be ready to defend my e-mail in-box from an angry Saddam Hussein seeking revenge for a strike on Iraq? Would using the military to defend U.S. companies even be legal? Or was this a bad knockoff of a Tom Clancy novel?

It turns out that the best thinking about cyberwar remains in flux, even after military wonks and nicely compensated Beltway contractors have spent the better part of a decade noodling over it. The reason: We're still waiting for the first real cyberwar between nations to take place.

Public discussions go back at least as far as 1995, around which time Richard Aldrich, an Air Force staff judge advocate, wrote a paper called "The International Legal Implications of Information Warfare." Aldrich pointed to how the staid Law of Armed Conflict, formalized in the 1949 Geneva Conventions, doesn't jibe well with communications that are ephemeral, global and difficult to trace.

For example, a nation violates international treaties by falsely claiming to surrender. "Suppose Iraq sent a bogus e-mail message to low-level (U.S.-led) coalition force commanders in the Gulf purporting to be from the commander of all coalition forces indicating that Iraq has surrendered and all hostilities are to cease immediately," Aldrich wrote. "If a commander acted on this message believing it to be real, and suffered heavy casualties from an Iraqi force he thought was surrendering but was actually attacking, would Iraq be guilty of violating the Law of Armed Conflict?"

Another implication is that it may not be permissible for a nation to deploy blunt offensive tactics like the recent Sapphire worm that snarled Microsoft SQL servers. Unless the creature was crafted to disable only legitimate enemy targets, it might violate international law.

Since those early discussions, the Pentagon has done what it does best: It has institutionalized and bureaucratized the study of computer warfare, making it a part of the larger field of information warfare. The Navy's Fleet Information Warfare Center has, for example, added "computer network defense" to its charter, and the Naval Postgraduate School conducts "red team" intrusion exercises for students.

The Pentagon has institutionalized and bureaucratized the study of computer warfare, making it a part of the larger field of information warfare.

The Air Force runs a "battlelab" that invented early-warning systems to alert operators when a network attack is about to take place and a "Software Agent for Operations Security" that scours dot-mil sites for classified documents. (Perhaps it works: There has been no verified report of classified files leaking through the Web.) Information warfare has even crept, oddly, into a "hazard list" compiled by Florida's Division of Emergency Management--alongside civil disorders, riots and various weapons of mass destruction.

"Kill Americans and you're in trouble," a Defense Department spokesman told me on Friday. "Whether it's treated as a felony, an act of terrorism or an act of war, you're in for serious consequences. Of course, behind the scenes, we would be having a spirited policy discussion of the relevant laws before a decision was reached."

One serious problem that governments face when responding to electronic assaults is that, because their origin may be unknown, the appropriate response depends on whether the culprit is a malicious hacker, a terrorist network--or the dictator of Iraq keyboarding furiously from a bunker deep below Baghdad. Depending on the source and the intent, the same type of intrusion could be a criminal offense or a declaration of war.

It's worth noting here that, as my colleague Robert Lemos has explained, the threat of so-called cyberwarfare may be overhyped: True, it's possible for electronic intruders to damage infrastructure and threaten physical harm, but seizing control of systems from the outside is extremely difficult--often impossible--and typically requires inside knowledge. Remember, it's always easier to bomb a target than to hack a PC.

Still, how would the Pentagon respond to a serious electronic attack on U.S. infrastructure? "It's yet another one of those issues where you would have to decide what the Internet is like," says Eugene Fidell, president of the National Institute of Military Justice. "The law often moves by analogy. Is the Internet like newspapers, like the water supply or like the power grid? Is it like the banking system? Issues like these have not been seriously explored, at least in terms of the law of war."

Robert Turner, the associate director of the Center for National Security Law at the University of Virginia, says President George W. Bush and the executive branch would have broad authority to respond to electronic onslaughts. "We're really in a gray area here," Turner says. "The theory of the Constitution was we don't like war. Before the president can make a decision to go from peace to war, he needs to have the permission of both houses of Congress. But if we are attacked, as commander of chief, the president wields executive power and does not need approval from Congress (to initiate a defense)."

Translation: If things get bad enough, say goodbye to civil liberties for a while, including the Fourth Amendment's protection against "unreasonable searches and seizures." Turner adds: "The Supreme Court has always held that what is reasonable depends on context. If you're in a situation where people are being killed and you're trying to save lives, you can be more intrusive...Protecting the state is a higher duty. To say otherwise is to sacrifice the ends to the means. If you're unwilling in times of crisis to depart from the law, and you lose your freedom, you've done no service to anyone."

The threat of so-called cyberwarfare

That's the conventional wisdom among military officers and Washingtonians. But even though a successful electronic attack is implausible, we should still remember

may be overhyped. to remain skeptical about governmental overreaching in times of apparent crisis. Once gained, additional surveillance power is not readily relinquished, and new data-mining centers like the one Bush announced last week bear close scrutiny.

Besides, at the same time that al-Qaida was plotting its successful suicide hijackings, the top U.S. spooks were busy fretting about the dire threat of Fidel Castro hacking our computers. In February 2001, Adm. Tom Wilson, head of the Defense Intelligence Agency, warned Congress: Castro's armed forces could initiate an "information warfare or computer network attack" that could "disrupt our military."

We're still waiting.