

Cyberwar goes mainstream

Alix Paultre, Editor-in-Chief



Once upon a time thoughts of computer warfare were restricted to science fiction stories. The role of the computer in warfare, both traditional and non-conventional, has grown and expanded as technology enhanced capability. Now cyberwar has matured to the point where a recent virus attack on the Iranian nuclear program resulted in as much damage and even more confusion and disruption to their efforts as a bombing strike with high explosives would have.

In the beginning computers in warfare were only used as force multipliers in military support areas such as logistics coordination, artillery fire-table calculation. Significant time savings and efficiencies were realized and the military was better able to address threats. For a long time, that's how it stayed. As computers migrated from the basement to the desktop, cyberwar expanded to cipher creation and code-breaking, using the computer to analyze and decrypt enemy callsigns and communications.

In the area of action, the odd "sneak in and download stuff" attack occurred, using mechanisms from quislings to break-ins. There was also passive infiltrative electronic espionage, snooping on poorly-shielded enemy computer systems as an expansion of signals intelligence. Add to that the management of advanced optical surveillance, radio intercept, and jamming systems in the water and on the land as well as in the air and space of both manned and unmanned types, and you have the primary roles of computers in warfare through the end of the cold war.

With the advent of the internet as a medium of communications and data exchange, a whole new world of surveillance opened up. In addition, a whole new realm of cyberwar opened up in the area of viruses, aggressive software agents that can act as electronic soldiers in the field. The ability to directly impact the physical world by manipulating the computers involved changed everything. Hackers morphed from a role of little more than telephone pirates getting over on Ma Bell to deadly computer warriors who could shut a corporation's operations down at the drop of a hat.

This recent attack by the Stuxnet worm on Iranian centrifuges demonstrated that computer warriors can do more than just damage a target's communications

Cyberwar goes mainstream

Published on Electronic Component News (<http://www.ecnmag.com>)

infrastructure through actions like denial-of-service (DoS) attacks. In the case of the Stuxnet attack, the virus changed the operation of hundreds of uranium centrifuges to cause negatively-resonant operation in their motors. This irregular operation caused the motors to render themselves nonfunctional, which turned the centrifuges into expensive doorstops.

Such direct-action attacks have positive repercussions that go beyond simply achieving the goal of interfering with the Iranian nuclear effort. No explosions means no public outrage at collateral damage, no physical presence means no captured soldiers or downed aircraft, and a room full of otherwise-fine machinery presents novel problems to people who would otherwise simply bulldoze and rebuild. A facility was rendered useless without a drop of blood being spilled. (I dare say the bill was significantly lower than the cost of a squadron of F-18s as well.)

This is not to say that DoS attacks are passé. The many followers of Julian Assange who shut down major web sites like PayPal, Visa and MasterCard (it takes stones and skill to mess with the banks) demonstrated that the weapon remains extremely effective. Just as victory on the real battlefield depends on proper use of all the combat arms supporting one another, success in the cybernetic theater of war will also depend on proper integration of all weapons and intelligent addressing the specific obstacles and opportunities the terrain of the battlefield involved.

The analogy of the web as battlefield can only go so far because the web is a place where the mouse can truly vanquish the lion if the mouse is smart and fast enough (in modern parlance, "has mad skilz"). The web expands and mutates every frontier in every facet of every application it touches, and the area of conflict is no exception. A jungle or ocean mentality may be a better comparison. In the sea of data we swim, information aggregators and crowd-sourced social exchanges like Twitter are the reefs where our new society grows, expands, evolves, and of course preys upon one another. The shark may command respect, but a little worm in either world can bring it down.

(Why not take a look at my book [Cyberchild](#) [1], a novel that deals with some of these issues.)

Source URL (retrieved on 03/26/2015 - 11:46pm):

http://www.ecnmag.com/blogs/2011/01/cyberwar-goes-mainstream?qt-recent_content=0

Links:

[1] <http://www.amazon.com/Cyberchild-ebook/dp/B001NMSRY0>