James C Sanders
COMP 395, RAM
Dr.Goeller

September 25, 1996

Information Warfare

Why is it that, with every advance in technology, someone invents a more destructive warfare? Artificial fire kept us warm and cooked our food, but allowed our arrows to scorch villages. Splitting the atom provided energy, but also brought us the atomic bomb. Such is the case with information technology. Information technology allows us to keep a geographically separated family together, share ideas, automate remedial jobs, and solve complex problems However, like fire and atomic energy, information technology has worked itself into the battlefield with a dogtag stamped Information Warfare (IW).

Reto E. Haeni, in his essay "Information Warfare," defines IW as "action taken to achieve information superiority by affecting adversary information, information based processes, and information systems, while defending one's own information, information based processes and information systems." A military definition can be found in the United States Department of Defense's definition, "actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and defending our information systems."

The military's goal of IW is to exploit the technological wonders of the twentieth century by using IW weapons as the first wave of attack. Before ground troops, long-range missiles, and even before stealth planes, the Army, Navy, Air Force, and Marines of the future will use IW to cripple their enemies. The tools they will use are computer viruses, worms, Trojan horses, logic bombs, chipping, nano-machines and microbes, electronic jamming, Van Eck monitoring, broadcast hijacking, High Energy Radio Frequency, and Electro-Magnetic Pulses.

Computer viruses and worms will be used to "hog" an enemy's information resources, significantly slowing, and sometimes stopping, the system's processing power. Trojan horses, logic bombs, and chipping will all be used to shut down an enemy's information system through pre-planted "kill switches." On a smaller scale, nano-machines and microbes (miniature robots and organisms designed to eat electronic equipment) will infest and devour enemy electronics. Concerning an enemy's electronic information transmissions, Van Eck monitoring will relay the messages, electronic jamming will stop them, and broadcast hijacking will replace them with inaccurate, damaging messages. High Energy Radio Frequency (HERF) guns and Electro-Magnetic Pulse (EMP) bombs will send high radio frequencies through an information target, rendering it unusable. The use of these IW tools will allow militaries to downsize, but even combined, they are not effective in all cases.

Because IW can only be used against an enemy which also has similar high-tech capabilities, underdeveloped militaries will have an advantage. Because any country can buy, hire, or develop hacker technology like IW tools, IW is referred to as The Great Equalizer. A hacker's hardware budget can be as low as a PC ($2,000), an ISDN modem ($300), and a monthly ISDN Internet service account ($60/month): a $2420 investment. Furthermore, all of the mentioned equipment is available world-wide, a lot of computer systems are poorly managed and poorly equipped to prevent against intruders, attacks over the Internet can originate from places that are physically located on the other side of the globe, and it is impossible to make a system absolutely secure. With IW so accessible, it is no wonder a country like the United States is concerned.

Because the United States is the most information reliant country in the world (our communications, air traffic, and banking all rely heavily on information technology), we are also

the most vulnerable to IW. According to "Onward Cyber Soldiers" by Douglas Walker, during the Gulf War, a group of Dutch hackers offered to disrupt the U.S. military's deployment to the Middle East for $1 million. Neil Munro's essay "The Pentagon's New Nightmare: An Electronic Pearl Harbor," says U.S. military officials acknowledge that they have no ability to protect themselves from cyberspace attacks and no legal or political authority to protect commercial phone lines, the electrical power grid and vast, vital databases against hackers, saboteurs and terrorists. Admiral William Studeman told a conference of intelligence officials that infowar targets “can include U.S. telecommunications, financial systems, ... the stock exchange, the Internal Revenue System of the United States, social security, banking, strategically important companies, research and development, air traffic control systems and high-tech databases, all of which are vulnerable today from outside." According to a 1994 report prepared by the National Communication System, no fewer than 30 countries are currently working on infowar techniques.

There are varying views of how important a role information warfare will play in future wars. William Tecumseh Sherman once said, "War is cruelty, and you cannot refine it," and an unnamed senior Army operations officer adds, "If you think this is going to replace four divisions or a carrier battle group, it can't..." However, others believe information warfare by information knowledgeable leaders and global conglomerates is the next logical step in warfare evolution after agrarian warfare by warrior class militia and tribes and industrial warfare by citizens and factories.