GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Cyber Warfare

Ernest Krutzsch
December 13, 2000

This paper will discuss the serious nature of Cyber Warfare and the security implications associated with the advancement of computers and computer technology as an implement of war.

When the Internet was first envisioned, there was probably no thought as to how the use of computers and computing could potentially become an instrument of war. However, with the increased reliance on the computer for maintaining and even operating the critical infrastructures that are key to the smooth operation of not only businesses, but also governments, and the conduct of war, this probability has become reality. The case is further proven when we consider that financial institutions, power grids, communications, and the conventional instruments of war rely more and more on computers for their operation.

In November 1999, in an article published by Reuters titled U.S. Military Grapples With Cyber Warfare Rules, there was talk in the Pentagon of "hacking into Serbian computer networks to disrupt military operations and basic civilian services". The Pentagon decided not to act due to continuing uncertainties and limitations surrounding the emerging field of "cyber warfare". They did in fact plan and test some of the concepts as to how to conduct this type of operation, but at the end, opted out.

The concept of cyber warfare is one that hits at the heart of warfare. The art of war requires that soldiers be able to shoot, move and communicate. With the increased reliance on computers and computer chips to operate vehicles, weapons systems and communications nodes, it is evident that attacking those computers from a distance becomes desirable.

However, lawyers have a different view of using computers to conduct warfare. The top legal offices of the Pentagon issued guidelines that indicated that the U.S. government could in fact be subject to possible war crime charges. Commanders were advised that they should apply the same standard of "law of war" principles to computer attacks as they would apply to bombs and missiles, which states that they can only be used against military targets, and must avoid indiscriminate attacks.

There is also the concern for the lack of international guidelines that would regulate the use of this type of attack. The Russians petitioned the United Nations to institute rules that would ban the use of "dangerous information weapons", even indicating that they would consider an attack on civilian or military infrastructures as an act of war.

To show the seriousness of this problem, in an article titled CYBER WARFARE: ARE HACKERS THE BIG NEW THREAT?, a scenario was initiated by RAND, a leading national think tank, that although may seem to be more of a movie plot, is becoming more of a concern for those responsible for the security of U.S. interests. The scenario was one which included Automatic teller machines malfunctioning, Telephone networks in strategic locations failing, Trains rerouted, and military communications systems failures. Who could possibly conduct this type of activity? That is what is of concern. In pre-Internet times, the conduct of acts of hostility

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

were difficult to plan, expensive to fund and although difficult, the responsible party was traceable. In this Information Age, anyone with knowledge, a computer and internet access could potentially wreak havoc, with little expense, little planning and the potential to never trace the true perpetrator of this act. The article continues to state that this demonstrates "America's growing reliance on computers and its vulnerability to terrorist hackers who could disrupt the nations electric power, banking, air traffic control, and oil and gas supplies'.

The article also states that 170 government, military, intelligence and businesses participated in the simulated crisis, and "nobody was able to tell reassuring stories about how this problem is going to get fixed.

To further indicate the problems that face decision makers is in how, when and if we engage in cyber warfare. An article titled Cyberwarfare: Ways, Warriors and Weapons of Mass Destruction, describes Cyberwarfare as the hottest topic in the U.S. military as well as the top executive offices. The reasons stated are "the United States is good at technology, and with the resources to procure whatever equipment and personnel it needs, information-warfare methods are potentially the most powerful weapons in the 21st Century arsenal".

The article focuses on three major issues that arise as the U.S. Military begins to involve itself in cyber warfare. Those issues are: 1) Are the techniques of cyber warfare actually weapons?, 2) What will be the identity and combatant status of those engaged in cyber warfare?, and 3) should these techniques be considered as weapons of Mass Destruction?

To set the stage, the article defines cyberwarfare as the "non-kinetic, offensive actions taken to achieve information superiority by affecting enemy information-based processes, information and computer –based networks." The methods used would include 'computer network attacks, transmitting computer viruses and other significant destructive hacking". It is interesting to note that as the art of warfare has advanced technologically, the rules of warfare have also changed to include the technological advances.

In military terms, "weapons are ordinary and lawful implements of war".
To engage in the first issue, as to whether the use of such techniques is indeed a weapon, the article states, "The employment of such weapons by militaries in armed conflicts would be what were traditionally called acts of war. Since the advent of the UN Charter, wherein signatories renounced the use of force in their relations with other nations, such acts may be termed hostile actions. Victims of these attacks would be authorized to resort to self-defense and to apply to the UN for military assistance".

"Not everyone agrees that all cyber attacks qualify as "armed" attacks under the UN Charter, however. One could argue that some electronic attacks would be more analogous to economic measures or other nonviolent coercive methods than to attacks with weapons. "

The second issue is whether the people who conduct these acts are actually combatants. Under International Law, the following components must be present to be considered a combatant:

- Be commanded by a person responsible for his subordinates.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Have a fixed, distinctive emblem recognizable at a distance.
- Carry arms openly.
- Conduct their operations in accordance with the laws and customs of war.

Obviously the use of civilians to conduct this type of activity would violate the international laws of war.

Finally, can this activity be considered as weapons of Mass destruction? As stated previously, the Russians stated that they would consider any Computer attack as using a weapon of mass destruction, and the normal response would be to respond in kind. The National Security Agency and the Air Force Office of Special Investigations came to the same conclusion. But where does international law stand on these premises. The problem is that there is no consensus as to the categorization of cyberwarfare as it applies to international law pertaining to the conduct of war.

As can probably be discerned, the answers to this question are complex and cannot be answered in this paper. The seriousness of this situation should be of concern not only to the United States, but to the entire world, as attacks on nations have become considerably easier. The following is an extract from the CIA Report to a US Congressional Committee, which exacts the serious nature of this topic.

"We are detecting, with increasing frequency, the appearance of doctrine and dedicated offensive cyber warfare programs in other countries. We have identified several, based on all-source intelligence information, that are pursuing government-sponsored offensive cyber programs. Foreign nations have begun to include information warfare in their military doctrine, as well as their war college curricula, with respect to both defensive and offensive applications. They are developing strategies and tools to conduct information attacks. Those nations developing cyber programs recognize the value of attacking adversary computer systems, both on the military and domestic front. Just as foreign governments and the military services have long emphasized the need to disrupt the flow of information in combat situations, they now stress the power of cyber warfare when targeted against civilian infrastructures, particularly those that could support military strategy."

As indicated in CYBER WARFARE: ARE HACKERS THE BIG NEW THREAT? There are some very basic steps that were recommended that could protect "Americans and their computers from most threats". David Banisar, a policy analyst at the Electronic Privacy Information Center, a Washington based research group that specializes in free speech issues on the internet, concludes that " there are lots of computers out there – and lots of military computers – where they have not done standard, simple security practices". The examples he gives are changing passwords and using encryption methods. The article also appropriately points out that this will not become a crisis to the U.S. Government until lives are lost or serious damage is done.

In conclusion, Cyber Warfare is a serious threat to not only the United States, but to the World. Active Security measures and techniques to protect the computer systems that run civilian

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

infrastructures as well as military hardware and communications facilities will be a paramount undertaking of unparalleled importance. We better do it right the first time.

References:

1. What Next in Net Technology, (not dated) http://www.skene-design.freeserve.co.uk/future.htm
2. Cyberwarfare: Ways, Warriors and Weapons of Mass Destruction, Commander Byard Q. Clemmons, US Navy, and Major Gary D. Brown, US Air Force, (October 1999) http://www-cgsc.army.mil/milrev/English/SepOct99/clemen.htm

3. CYBER WARFARE: ARE THE HACKERS THE BIG NEW THREAT? (March 1996) http://platon.ee.duth.gr/data/mailist-archives/cyberurbanity/1996/msg00050.html

4. U.S. Military Grapples With Cyber Warfare Rules, (November 8, 1999) http://www.infowar.com/mil_c4i/99/mil_c4i110899b_j.shtml

5. INFORMATION WARFARE, (not dated) http://www.mandia.com/kelly/cyber_warfare.html

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: May 29th, 2017

Upcoming Training

SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event