15

INFORMATION WARFARE

Hartmut Pohl Hartmut.Pohl@sang.net
University of Applied Sciences, Bonn-Rhein-Sieg and ISIS – InStitute for Information Security, Cologne, Germany.

Keywords: Attack types, Critical infrastructure protection, Information warfare.

1 INTRODUCTION

The changes in technology in the last 10 years and the future will definitely result into a convergence of communications and computing in the fields of communications (telephone mobile also, internet, satellite), electric power, gas, oil, water supply, banking, stock exchanges, insurances, (air) traffic control, emergency services and disease management, information processing facilities of governments, governmental activities etc. in all countries especially in the first world. These and others are the so called critical infrastructures [Clinton 1996]. They are highly vulnerable because of their dependability of computers (hardware and especially software). Attacking one of these fields or infrastructures may result in a total disaster of the whole state.

The critical infrastructures depend on each other – for example the traffic depends on the telephone/fax and internet. The internet depends on electric power, electric power distribution depends on the internet. There is no only one independent critical infrastructure.

It is possible to connect to the internet all over the world with cost about less than 50 $ US per month. Computers cost about 500 $ US. Therefore the attack costs are low – especially compared with the possible damage.

2 DEFINITIONS

2.1 Information Warfare

I will discuss information warfare as a warfare attacking information systems by using information systems to destroy information processing of a town, region or country with the aim to damage or destroy one or more critical infrastructures.

I will not use the word information warfare as the classical psychological warfare and the distribution of information by mail, files, papers, radio or TV. And I definitely will not use the word information warfare as information operations conducted during time of crisis or conflict to achieve information superiority or promote specific objectives over a specific adversary or adversaries. [DoD]

2.2 Strategy to Secure Cyberspace

National strategies to secure cyberspace are part of our overall effort to protect our nations. It is an implemented component of the national strategy for homeland security and is complemented by a national strategy for the physical protection of critical infrastructures and key assets. [Bush 2003].

2.3 Other Aspects of Information Warfare

Information Warfare can be divided into:

- Offensive information warfare.
- Defensive information warfare with all the security measures like access control, encryption, filtering (firewalls), monitoring, detection and prevention of intrusions, management of information security in companies, agencies and states.

In this paper especially the first aspect offensive information warfare is discussed.

3 CASES OF INFORMATION WARFARE

There are only few cases of information warfare seriously published – especially cases of business information warfare.

4 SEVEN THESES FOR THE FUTURE OF INFORMATION WARFARE.

4.1 Aims

The aim of an information warfare is to destabilize a state, a region or a government by shutting down one of the critical infrastructures – especially first of all the communication infrastructure, which serves the other infrastructures.

4.2 Attack Types

The attack types are very well known like viruses, worms, buffer overflows, Trojan horses, etc. Some are only a little bit hypothetical like the Warhol–worm or Flash–worm. The attacks of the future will be very quick in attacking most servers of the internet in minutes and will act for a long time covert.

4.3 Perpetrators and Motives

Perpetrators are of the level of computer criminals: High grade experts are specialised in the fields of operating systems, communications, database systems, and standard software like SAP, People soft etc. You can find those potential perpetrators, specialised experts all over the world. Most countries offer studies in computer science and studies in computer security and information security.

4.4 National Activities versus Coordinated Global Planning

The mentioned critical infrastructure do not end at the borders of national states but exceed continents like the communication infrastructure (internet), telephone system, electric power, gas, oil, water supply, banking, stock exchanges, insurances, and air traffic control. National activities are not useless but not equivalent to the global risks; one nation alone is not able to secure the links to the continental or global infrastructures.

4.5 Critical Infrastructure Protection

The way to secure critical infrastructures is to identify the most vulnerable infrastructures first and secure them. But because of the linkage between the infrastructures it is very necessary to secure them all.

4.6 Legal, Political and Technical Security Measures

It is necessary to adopt security legislation in all states and initiate security programs. Theses legal and political measures are also necessary on a supranational level.

The mentioned measures of the defensive information warfare have to be installed in total depending on the value of the processed data.

4.7 Arms Control

It is necessary to control the development of the mentioned attacks and new ones all over the world – for example by monitoring the internet.

5 CONCLUSIONS

Information warfare will be the war of the future between high tech states; and as asymmetric warfare between low and high tech states. The same attack types will be used by terrorist – small groups of men (one or more) attacking high tech companies and states and also bigger groups of men against (international) companies or states.

6 REFERENCES

Alberts, D.S.; Garstka, J.J.; Stein, F.P.(2000), Network Centric Warfare. Developing and Leveraging Information Superiority. 2nd Edition Washington.

Arquilla, J.J.(1993), Cyberwar is coming.
http://gopher.well.sf.ca.us:70/0/Military/cyberwar

Arquilla, J.J.; Ronfeldt, D.F.(1995), Cyberwar and Netwar: New Modes, Old Concepts, of Conflict.
http://www.rand.org/publications/RRR/RRR.fall95.cyber/cyberwar.html

Bush, G. (2003),The National Strategy to Secure Cyberspace. Washington.

Clinton, W.J.(1996), Critical Infrastructure Protection. Executive Order 13010. The White House http://www.pccip.gov/eo13010.html

Denning, D.(1999), Information Warfare and Security. Reading.

DoD (Ed.): DoD Dictionary of Military Terms. O.J.
http://www.dtic.mil/doctrine/jel/doddict/data/i/03097.html

Geiger, G.(1997), Verteidigung im "Cyberspace". Internationale Probleme, nationale Aufgaben. Ebenhausen.

Johnson, L. S., Toward a Functional Model of Information Warfare http://www.infowar.com/mil_c4i_101497a.html-ssi o.J.

Karresand, M.(2002), A Proposed Taxonomy of Software Weapons. Linköping.

Molander, R.C (1996), Riddile, A.; Wilson, P.A.: Strategic Information Warfare. Santa Monica.

PCCIP (1997), President's Commission on Critical Infrastructure Protection: Survey Form. Washington.

PCCIP, President's Commission on Critical Infrastructure Protection: Critical Foundations. Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection. Washington o. J. http://www.dis.anl.gov/survey

Pohl, H.(1996), Informationssicherheit der Global Information Infrastructure (GII) - Einige Bemerkungen zu Problemen und Entwicklungen. In: Tauss, J. et al. (Hrsg.): Deutschlands Weg in die
Informationsgesellschaft. Herausforderungen und Perspektiven für Wirtschaft, Wissenschaft, Recht und Politik. S. 358 - 390. Baden Baden.

Pohl, H. (1998), Information Warfare – Information Survivability. Datenschutz und Datensicherung, 2.

Pohl, H.(1998),Information Warfare: Der Krieg im Frieden. Zusammen mit Cerny, D. In: Bauknecht, K.; Büllesbach, A.; Pohl, H.; Teufel, S. (Hrsg.): Sicherheit in Informationssystemen SIS '98. Zürich .

Pohl, H.(2000), Business Information Warfare. In Geiger, G. (Hrsg.): Sicherheit der Informationsgesellschaft. Gefährdung und Schutz informationsabhängiger Infrastrukturen. Baden Baden.

Pohl, H.(2000),Information Warfare. In: Reinermann, H. (Hrsg.): Regieren und Verwalten im Informationszeitalter. Heidelberg.

Pohl, H., Civil War in Cyberspace. Ziviler Ungehorsam, innere Unruhen und Bürgerkrieg in der Informationsgesellschaft.

Schubert, S. et al. (Hrsg.)(2002), Informatik bewegt. Proceedings der 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI). Bonn.

Rathmell, A.; Overill, R.; Valeri, L.; Gearson, J.(1997) The IW Threat from Sub-State Groups: An Interdisplinary Approach. http://kcl.ac.uk/orgs/icsa/terrori.htm

Szafranski, R.(Preparing for 2020), A Theory of Information Warfare. o.J. http://www.cdsar.af.mil/apj/szfran.html

Szafranski, R,Parallel War and Hyperwar: Is every eant a Weakness? http://www.cdsar.af.mil/battle/chp5.html o.J.

Vatis, M.(2001), Cyber Attacks during the War on Terrorism: A Predictive Analysis. Dartmouth http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf.

Wenger, A.; Metzger,JDunn, M.(2002): The International CIIP Handbook. An Inventory of Protection Policies in Eight Countries. Zürich.