Educational Exercises in Information Warfare — Information Plunder and Pillage

By Helen Armstrong and John Davey

Helen Armstrong
School of Computer and Information Science
Edith Cowan University
Bradford Street
Mount Lawley, Western Australia
Phone: +61-8-9370 6856
Fax: +61-8-9370 6100
Email: h.armstrong@ecu.edu.au

John Davey
Defence Security Branch
Department of Defence
Campbell Park Offices
Canberra ACT 2600
Australia
Phone: +61-2-6266 3025
Fax: +61-2-62662732
Email: jack.davey@cbr.defence.gov.au

Submitted to
NCISSE 2001, May 22-24, 2001
5th National Colloquium for Information Systems Security Education
George Mason University
Fairfax, Virginia

Educational Exercises in Cyberwarfare — Information Plunder and Pillage

Abstract:
This paper looks at the concept of cyberwarfare and discusses its application in both defense and business environments. An approach to teaching offensive and defensive skills in this area is presented. The warfare tactics of the ancient Mongols are described and used as a trigger for formulating tactics for more modern warfare in cyberspace. Action learning is an important facet of such a learning environment as students need to experience application of the theory in order to produce proficiency in using the required tools.

Keywords:
Cyberwarfare, Cyberweapons, Information Warfare, Information Operations, Cyberterrorism, Action Learning

Introduction
Information warfare and cyberwarfare are growing activities in our globally connected and competitive world. The need for skills in offensive and defensive cyberwarfare operations is evident from the constant reports of attacks on government and business communications and computer networks.

Information warfare is a broad term that encompasses many types of offensive and defensive activities involving intelligence, tactics and strategies, and manipulation of information and communications systems. Information warfare is taking action to degrade or manipulate an opponent s information resources and defending one s own information resources. The suggestion that information warfare consists of offensive and defensive operations against information resources of a win or lose nature (Denning, 1999) presents only a narrow view. Rather than operations to win or lose, information warfare can also include surreptitious operations designed to slow down or temporarily immobilise an opponent or ally, or it may be action targeted to disable a given function.

Information Warfare in Defense and Business Environments
In the context of defense, information warfare is commonly considered to be electronic warfare, cyberwarfare or netwar. However, information is not only to be found on computer systems and networks. Information warfare in a defense environment encompasses intelligence warfare, psychological operations, cyberwarfare, cyberterrorism, electronic warfare, intelligence warfare, security operations, psychic operations and so forth. During the 1996 US Senate s hearings on Security in Cyberspace the NSA reported more than 100 nations are preparing for information warfare in the twenty-first century (Power, 2000).

In a business environment information warfare encompasses competitive intelligence, industrial and economic espionage, sabotage, theft and other types of cybercrime. Cybercrime is a high level term relating to any criminal activity carried out via electronic or computer means. FBI Director, Louis Freeh claims cybercrime is one of the fastest evolving areas of criminal activity (Brixley, 2000). FBI Deputy Director, Thomas Pickard

stated Never before have unknown faceless people been able to commit so many different types of criminal acts on a global scale and from remote locations, exploiting vulnerabilities unheard of a few short years ago (Brixley 2000, p. 8). Organisations engaged in the creation of information technology are targets for corporate espionage (Morris, Ettkin & Helms 2000). This is because the activities of these firms concentrate on leading edge technologies and their information on products and management strategies is unique and valuable to competitors and political groups. Netspionage agents, techno-spies and other criminals are attempting to do what they have always done: to steal, defraud, and subvert others for personal, corporate, national and/or political gain (Boni & Kovacich, 2000, p 23), and organisations leave themselves open to attack and crime by ignoring vulnerabilities.

Cyberterrorism

The Japanese doomsday cult responsible for the sarin nerve gas attack in the Tokyo subway in 1995 (Aum Shinri Kyo) were not only proficient in chemical and biological weapons, but also had established an intelligence group to steal high-tech secrets from a variety of corporations and research organizations. The Japanese Defense Agency became concerned when they discovered that 90 Japanese government agencies and private organization had ordered software produced by the cult (Power, 2000). They delayed the installation of a new computer system developed by the cult in order to check the system. Cyberterrorism covers unlawful attacks or threats of attack against computers, networks, and the information stored within those systems (Denning, 2000).

Cyberwarfare

Cyberwarfare is a subset of information warfare and involves offensive and defensive operations carried out in cyberspace. Cyberwarfare can be carried out by a number of different parties, using a variety of tools. Cyberwarfare attacks could emerge from political opponents, commercial opponents, hackers, disgruntled employees and other internal staff, dissident groups and terrorists. According to Denning (1999) information warfare is also used by corporations to gain competitive advantage and government bodies to investigate crimes, intelligence and defense concerns. For example, the FBI uses a software tool called Carnivore to secretly intercept and monitor Internet traffic. In Australia the ASIO Amendment Act 1999 gives ASIO the power to use any computer, electronic or communications equipment to obtain data relevant to a security matter, and if necessary to add, delete or alter data in the target computer (Maher, 2001).

Five types of cyberwarfare are discussed by the Centre for the Study of Technology and Society (nd) and these are web vandalism, disinformation campaigns, gathering secret data, disruption in the field and attacking critical infrastructure. These five types would appear to be applicable to both defense and business situations. Cyberwarfare can be applied not only in defense and law enforcement, but also business and economic environments.

In a business environment the impact of cyberwarfare could include denial of service attacks, sabotage, negative intelligence gathering, loss of customers and market share, theft of proprietary and confidential information, loss of data or insertion of

misinformation. Unless a firewall picks up an attack in a defense environment the organization may not know they are being attacked. Even if the attack is observed, without the required skill set (ie proficiency in the tools and methods) the organisation will not be in a position to defend or match the skills of their opponent.

The impact of attacks in cyberspace will depend on the tactics employed. Hundley and Anderson (1997) categorise the consequences of cyberspace attacks into levels of impact - minor annoyance or inconvenience, limited misfortune, major or widespread loss, or major disaster. Tools used in cyberwar attacks could include social engineering, hacking, denial of service attacks, eavesdropping, dumpster diving, identity theft, sabotage, insertion of rogue code, industrial espionage, stealing intellectual property and confidential information, physical theft, insertion of misinformation and perception management. Defensive actions include hiding information resources, increased authentication and access controls, monitoring, intrusion detection and backups.

An organization may not even be aware of a cyberattack if the tools, skills and procedures do not exist or are not used. The typical response by the target organization is to bring the computer systems down in an effort to reduce damage, thus denying the organization of its own functions.

The Need for Education and Training

The US Department of Defense (DoD) is currently working on a means of raising awareness of cyberattacks across the entire organization. This is being undertaken because DoD recognises that they currently have insufficient intrusion detection systems, insufficient analysis capability, insufficient notification systems and insufficient training (Power, 2000). The importance of education and training together with deployment of security tools is highlighted by Armstrong (2000) in the fight to minimise security vulnerability.

Cyberwarfare is an area of education where practical application of the theory is essential. Within business and defence environments the aim is to, at best win the game, or at worst, not lose the game. Experience solidifies learning and the only way to master the skills involved in cyberwarfare is to have hands-on experience. If an organisation wishes to stay equal to, or one step ahead of an adversary, proficiency in the art of defensive and offensive cyberwarfare is required. Becoming immersed in either offensive or defensive cyberwarfare without the practical learning experience will result in having an inferior position of knowledge to the adversary, and an inability to protect one s own information resource. In this case the organization is liable to be compromised by an attacker that has more refined techniques. Offensive and defensive cyberwarfare activities without practical experience could result in early defeat or an inability to refine the methods of attack or defense being used.

In addition to gaining experience in the tools and methods, the training function also teaches authority, command and control together with team dynamics. Cyberwarfare games teach procedures, compliance to rules, management of situations and events. In

addition games promote teamwork and encourage proficiency in tools and techniques resulting in faster reaction times in the event of attack.

Information Warfare attacks create emergency situations and defense against such attacks could be viewed as disaster recovery mechanisms. Just as all disaster recovery potential team members should be tried and tested in a mock crises situation to gauge how they would react in an emergency, so members of the defense team need test scenarios involving attack and defense strategies and tactics. Nicklin (2001) suggests that contingency planning training should be presented on a team basis, as the interaction between team members is a vital component of crises management. This is also the case in cyberwarfare training.

Ethical Aspects of Information Warfare

The Pentagon considered hacking into Serbian computer networks to disrupt military operations and basic civilian services, however, the attack was not undertaken due to legal and ethical issues. The Department of Defense s legal office issued a warning that misuse of computer network attacks could subject US authorities to war crime charges (Power, 2000). Power goes on to suggest that although the US government held back due to considerations of ethics and international law, he doubts that the Aum Shinri Kyo and similar cults would feel the same pangs of conscience.

Ethics is an important aspect of any type of warfare, but is particularly pertinent in cyberspace where battles are fought in the ether and foes do not meet face to face. Offensive and defensive actions need to be planned and mindfully actioned. One of life s basic rules is that what one gives out, one will certainly get back.

Defensive action is seen to be more acceptable and ethical than offensive action. Most parties involved in information warfare will admit to exploring defensive actions. However on occasions it may be necessary to initiate offensive action in order to protect one s information resources and possible one s nation.

Cyberwarfare Training in Stages

There are five stages in the teaching of cyberwarfare (see Figure 1). The first stage is the gaining of skills in network architecture, network security and security products. Each team member will need a detailed knowledge of the tools and environment. The network will require 3-4 workstations, software tools, mapping software and security tools. Each student will learn about the network, the O/S and the software, and will use these until they are proficient in managing all the components.

Stage 2 is one-on-one play between team members. Team members apply the knowledge gained in operating systems, networks and security tools from stage 1. Network traffic generated by the two is investigated, and tools for intrusion detection, monitoring, etc. are investigated to increase familiarity with the software and hardware. This activity is conducted initially on one network and then expanded to two networks.

Stage 3 is further one-on-one play between two team members on two networks, however, routers and firewalls are added to each of the networks. Students use the same tools as in stages 1 and 2, but play with the implementation of routers and firewalls on both networks. Debriefing sessions between the students are held to review actions and counteractions. Supervisors attend some of the debriefings to solve any problems and give guidance.

Stage 4 can be accomplished with a minimum of two team members, but it is preferable that a team is gradually built up on each network to allow the development of basic team skills. Additional pseudo network traffic is added during this stage in order to simulate a normal network traffic environment. Further debriefing sessions are included between students, and with students and supervisors.

Stage 5 is the final stage where scenarios are acted out in full games. Application of tactics and strategy previously learned will be necessary during this stage. Full teams of 4-5 members act out predefined scenarios on each network, and debriefing sessions are held regularly. Each team has at least one supervisor and one scribe to log all the activities as they happen. Team members rotate in the supervisory role. Managers at a higher level give guidance for strategy, but most of the decisions are made by the group under the leadership of the team supervisor. Rules of play and the criteria for success are determined before the game commences. Debriefing sessions provide the venue for planning and reflecting upon actions.

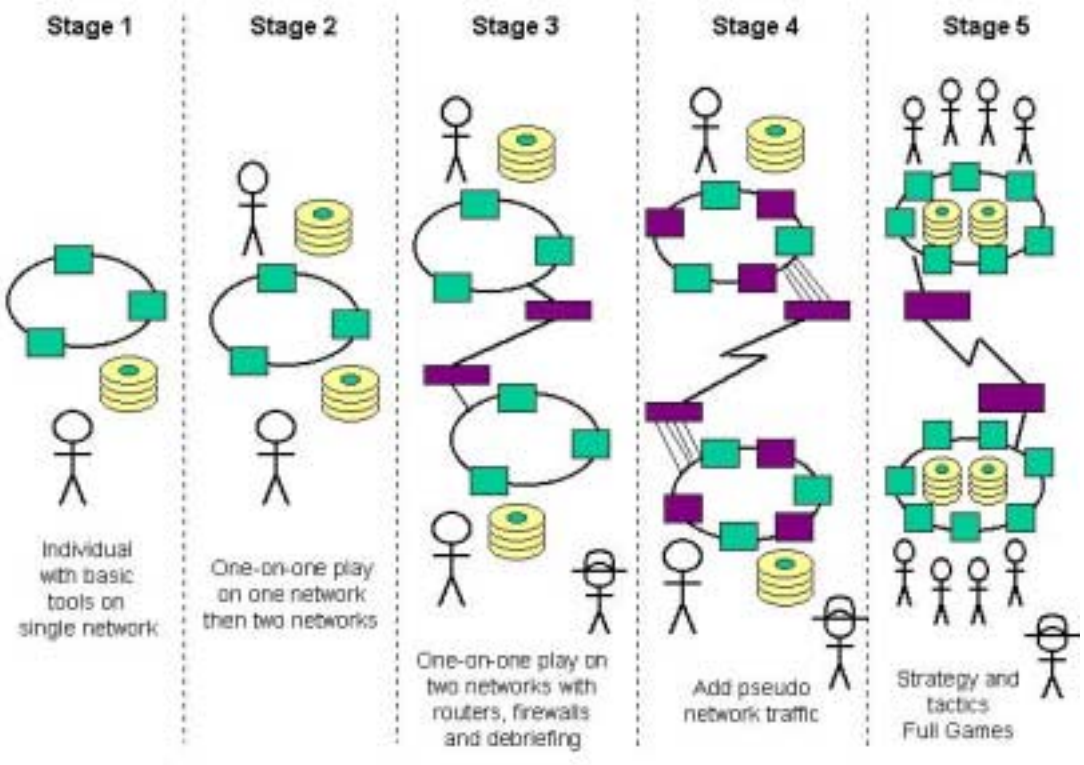

Figure 1: The Stages in Teaching Cyberwarfare

At the end of the game, a meeting of the entire cast is held to reflect upon the exercise. Each student writes a report on the exercise, reflecting upon the hardware, software, communications, tactics employed, team interaction, supervision, and debriefing sessions.

Information Pillage and Plunder Tactics

There are numerous sources of information on warfare tactics including the Internet, films, television news footage, books, journal papers and technical reports. Many of the strategies presented in these sources can be modified to be acted-out in cyberwar games. For example, during the 12th and 13th century the Mongols used information warfare tactics and strategies to defeat a number of enemies. Although their numbers were small, the Mongols were able to use information warfare tactics to gain an edge over their opponents and eventually win most of their battles. Some of the tactics used by the Mongols included—

- Hid information regarding their whereabouts until they attacked unannounced
- Intercepted the enemy s messengers as they moved between the headquarters and action
- Used communications and coordinated operations to fragment the tactics and control of their opponents
- Provided misinformation about their position to confuse the enemy
- Sent out small detachments as lures and lead opponents into the full Mongol forces
- Ensured they had extensive and current information about their opponents in order to build a big picture of the battlefield
- Mongol scouts and messengers made a practice of taking several tethered horses so they could change mounts when a horse tired
- Used a semaphore system for communications allowing a change of tactics at short notice
- Developed a decentralized command structure in the field for fast decision making
- Used non-linear campaigns, striking when circumstances were favourable
- Gathered intelligence on their foes, particularly the defense coalition s order of battle
- Identified the advancement patterns of their foes and avoided them
- Used netwar tactics early in their campaigns by broadcasting that any city resisting would be razed and its inhabitants slaughtered encouraging peaceful takeovers.

(Arquilla & Ronfeldt 1997, Chambers 1985, Curtin 1908)

Due to their advanced information operations and intelligence, the Mongols were able to repeatedly use a river crossing during the battle of Khwarizm in the intervals between the river was being used by the enemy — the Poles and Prussians (Arquilla &Ronfeldt, 1997).

Many of the tactics used by the Mongols can be applied in cyberwarfare today and these are evident in the following list of possible tactics. This list is not meant to be an exhaustive list, just provide some examples -

- Eavesdropping on the opponent s computer networks and communications
- Interrupting transmission of messages across adversary s communications lines
- Intercepting and altering messages being transmitted between management and operations
- Mapping the opponent s networks
- Scanning the opponent s networks for vulnerabilities
- Providing misinformation to confuse the opponent
- Planting fast acting rogue code on the opponent s system (ie viruses, worms, etc)
- Using known vulnerabilities in the software to gain access to the opponent s system
- Planting bad data or code to surreptitiously undermine the opponent s systems or data
- Launching denial-of-service attacks on the opponent s
- Ensure accurate reporting of happenings, ie report only the facts
- Monitoring own systems for intrusions, eavesdropping, mapping and scanning
- Analyse the opponent s patterns of attack for pre-empting future actions and attacks
- Attacking from bogus, anonymous or innocent sources
- Penetrating computer networks
- Reconfiguring the opponent s firewall
- Planting spies in opponent s operations
- Monitoring own transactions for spies
- Having imaged backups of computing software and environment to allow fast recovery
- Ensuring backup hardware and power supply are on hand
- Develop efficient command and control systems
- Ensure all members know their area of responsibility and boundaries for decision-making
- Ensure all members know the procedures and rules
- Ensure all members have an in-depth knowledge of their tools and tactics
- Debrief regularly

Hundley and Anderson (1997) discuss five different types of cyber attacks, ie those that are operations-based, user authentication-based, software-based, network-based and hardware-based. Many past cyberspace attacks have consisted more than one of these mechanisms.

One of the crucial aspects of training in cyberwarfare is learning to plan before action, and reflect after action. This is possibly the most important skill to walk away with, win or lose.

Conclusion

The increasing amount of coverage being afforded information warfare in the press, other printed publications and the Internet is a signal that awareness of information warfare is rising. The face of warfare in defense is gradually changing and many authors claim future wars will increasingly be fought in cyberspace before troops and fighter aircraft are deployed. The battlefield in business indicates that hackers, competitors and disgruntled employees will increasingly use computerised tools to attack networks and computer systems crucial to business survival.

Most nations are well-versed in the traditional methods of warfare. Business organisations are gradually becoming aware of their vulnerabilities and applying means of protecting their information resources. Information warfare will be around for many years yet, and organisations need to be prepared in order to defend their resources from opponents, competitors, employees, criminals and dissidents. Part of this preparation is training their operators in offensive and defensive information operations and ensuring that experience is the foundation of learning.

References

Armstrong, I., (2000) Security Fights for Internet Foothold, *SC Magazine*, November, pp 12-17

Arquilla, J. & Ronfeldt, D., (1997) *In Athena s Camp: Preparing for Conflict in the Information Age*, RAND, Santa Monica, CA, USA

Boni, W. & Kovacich, G.L., (2000) *Netspionage: The Global Threat to Information*, Butterworth-Heinemann, Boston, USA

Brixley, J., (2000) Fighting Cybercrime, *Inside Fraud*, October, pp 8-9

Centre for the Study of Technology and Society, (no date) *National Security — Cyberwarfare*, WWW document URL http://www.tecsoc.org/natsec/focuscyberwar.htm

Chambers, J., (1985) *The Devil s Horsemen*, New York, Atheneum Publishers

Curtin, J. (1908) *The Mongols*, Little Brown Publishers, Boston

Denning, D., (1999) Information Warfare and Security, Addison-Wesley

Denning, D., (2000) Cyberterrorism: Real or Not?, *Computer Security Alert*, No. 208, July, pp 2-3

Hundley, R. & Anderson, R., (1997) Emerging Challenge: Security and Safety in Cyberspace, in Arquilla & Ronfeldt *In Athena s Camp* , Rand

Maher, W., (2001) Spies Like Us, *Australian Personal Computer*, April, pp 62-68

Morris, D.J., Ettkin, L.P. & Helms, M.M., (2000) Issues in the illegal transference of US information technologies, *Information Management & Computer Security*, Volume 88, No. 4, pp 164-172

Nicklin, R.E., (2001) An Ounce of Prevention and a Pound of Planning, *Security Management,* February, pp 62-66

Power, R., (2000) *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace*, Que Publishing, Indianna, USA