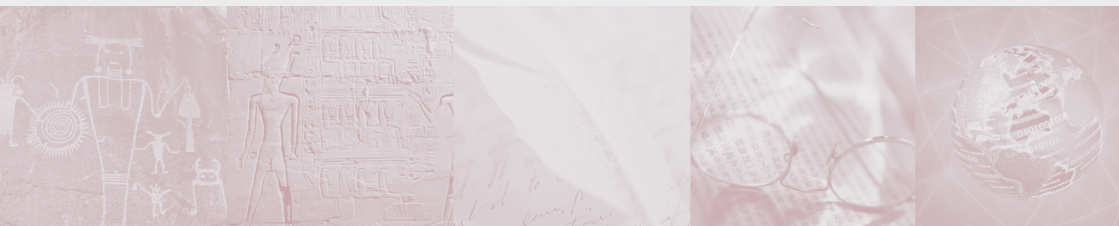


The Information Society Library
GETTING THE BEST OUT OF CYBERSPACE

HACKTIVISM, CYBER-TERRORISM AND CYBERWAR

THE ACTIVITIES OF THE UNCIVIL
SOCIETY IN CYBERSPACE

Stefano Baldi • Eduardo Gelbstein • Jovan Kurbalija



P R E F A C E

There is no shortage of books on all matters relating to information management and information technology. This booklet adds to this large collection and attempts to do a number of things:

- offer non-technical readers an insight into the few principles that are important and reasonably stable;
- present the material in a context relevant to the work of those involved in international relations;
- awaken the curiosity of readers enough that they will progress beyond this booklet and investigate and experiment and thus develop knowledge and take actions that will meet their particular needs.

The format of these booklets and their contents evolved from courses given by the authors over the last few years in various environments and the feedback of the attendees. Readers' feedback on these booklets would be greatly appreciated by the authors so that future editions can be improved. The coordinates of the authors are given at the end of this booklet.

ISBN 99932-53-01-4

Published by DiploFoundation

Malta: 4th Floor, Regional Building
Regional Rd.
Msida, MSD 13, Malta

Switzerland: c/o Graduate Institute of International Studies
rue de Lausanne 132
CH-1211 Genève 21, Switzerland

E-mail: diplo@diplomacy.edu
Website: <http://www.diplomacy.edu>

Edited by Hannah Slavik and Dejan Konstantinović
Cover Design by Nenad Došen
Layout & prepress by Rudi Tušek

© Copyright 2003, Stefano Baldi, Eduardo Gelbstein and Jovan Kurbalija

Any reference to a particular product in this booklet serves merely as an example and should not be considered an endorsement or recommendation of the product itself.

CONTENTS

Introduction	5
Cyberspace	8
The Yin-Yang of cyberspace	10
Hacktivists, cyber-terrorists and cyber-warriors	17
The world of hacktivism	21
Cyber-terrorism	31
Thinking about cyberwar	43
Training the military	49
Table of attacks and attackers in cyberspace	52
Known facts and unknowns	53
The things we know	55
Unknowns	59
The special challenges facing critical infrastructures ...	65
The law, open issues and some conclusions	67
Adoption of new information security instruments. ...	69
Applying existing international instruments to cyber-security	70
Legal challenges - international regulation of cyber-security issues	73
Conclusions	76
References	79
About the authors	80



SECTION



1

Introduction

Wisdom consists in being able to distinguish among dangers and make a choice of the least harmful.

Niccolo Machiavelli, *The Prince*

INTRODUCTION

It is generally agreed that human society, as we know it today, started after the end of the last Ice Age and that settlements founded through agriculture, producing food surpluses, began around ten thousand years ago or so.

Since then, successive waves of development have each contributed to what we call “civilisation”, including the discovery of such concepts as writing, legal codes, mathematics, science and astronomy, technology and many others.

Many technologies have caused social and political change and invariably, have been used as both tools and weapons. As the rate of technical innovation accelerates, it increasingly disrupts the societies it touches, while the governance mechanisms that are meant to contain such disruption continue to develop more slowly than technology.

Societies have also learned that no technology is perfect and that each technology leads to hard-to-predict side effects which need to be managed in the future. When antibiotics were first introduced they were thought of as “wonder medicines”: nobody anticipated the emergence of antibiotic resistant bacteria.

Today the use of global networks, enabling easy and cheap communication between businesses, governments, academia, individuals and any other interested parties is well established. However, global networks have also become crime scenes. It seems inevitable that in the future they will also become theatres of war.

Many “optimists” believe that the worst thing that could happen would be a shut-down of the Internet, which at present would be more of an inconvenience than a catastrophe. The optimists’ reasoning is that attacking critical infrastructures and networks that are not part of the Internet (such as those used by emergency services or global funds transfer networks) is technically “too difficult” at present. They may well be wrong. It may be technically difficult but it is not impossible. This booklet will discuss the vulnerabilities that increase the risk of cyber-

war and cyber-terrorism in particular, and the actions that need to be taken to reduce those vulnerabilities.

It will also explore the side effects and disruptions associated with cyberspace and complement the booklets on *Good Hygiene for Data and Personal Computers* and *Information Insecurity* by discussing the more organised and professional areas of hactivism and cyber-terrorism, including the concept of cyberwar.

CYBERSPACE

The word “cyberspace” is a relatively recent addition to our dictionaries. It was first used in the science fiction novel *Neuromancer*, by William Gibson, published in 1984. It is worth remembering that good science fiction writers are often the first to explore the potential side effects of new technologies. If only their works were read sooner...

The current usage of the word “cyberspace” describes a world of data and software, both intangible entities existing in the electromagnetic spectrum as waves, impulses, electric charges and magnetic states. These electromagnetic entities manifest themselves physically through a multiplicity of devices such as computers, storage devices, network cables, routers, telephones, satellites and printouts of the software code describing how that software operates.

Cyberspace consists of many components, including the Internet and its sub-component the World Wide Web, intranets (private internets) and extranets (internets with restricted memberships), and all other networks using different protocols (detailed operational specifications) from the Internet.

Such networks include the telephone networks (fixed and mobile), the satellite networks for communications and the Global Positioning System, as well as the proprietary networks developed by a multitude of vendors over the last fifty years for the use of major companies, the military, intelligence and police communities, emergency services and others.

The Internet has become ubiquitous. In the last few years many bridges have been built to link non-Internet protocol networks to the Internet

in order to support easy and low cost global access to data and information, electronic commerce and other transactions as well as the interchange of electronic mail between proprietary private systems and the global Internet e-mail system.

The emergence of the Internet should be regarded as an event without precedent. It was first developed as a private network (called the DARPA-net) designed to withstand a nuclear attack, and access to it was limited to individuals working on defence projects.



In the 1970s and early 1980s, the exchange of data between computer systems was hard to achieve. To make an airline reservation, travel agents had to either phone an airline or install a terminal connected to the airline's computer system. If they acted on behalf of six airlines, they needed six different terminals, each with its own peculiarities, technologies and processes.

In the early 1970s, one of the services available on this network, electronic mail, became very popular with the large academic community that was by then connected to the network and it continued to grow quietly but generally out of sight of the general public.

Alongside these developments came proposals for new standards – such as the Open System Interconnection (also known as the OSI) model that enabled dissimilar computer systems and networks of the world to work together regardless of which industry standards they used. Many of these useful standards were rapidly adopted, for example, X.25, used for packet switching in data transmission.

However, the full OSI model was never implemented and it was displaced by the Internet. At the same time, the work of the UN Conference on Trade and Development (UNCTAD) in establishing the EDI-FACT standards for electronic data interchanges remains widely used.

In 1998, Tim Berners-Lee, then at the European Centre for Nuclear Research (CERN), in Geneva, developed a workable scheme to link documents together using the Hypertext Transmission Protocol, and this quickly became the foundation of the World Wide Web.

In 1992, at the NCSA (National Center for Supercomputing Applications) of the University of Illinois, Marc Andreessen developed a web browser with a graphical user interface which made access to the Inter-

net virtually intuitive. This was a major turning point in the Internet's short history.

By early 2003, it was estimated that over 620 million individuals around the world had access to the Internet and its services.


THE YIN-YANG OF CYBERSPACE

At this point, it would be appropriate to consider the concept of “Yin-Yang”, believed to be over three thousand years old, representing the ancient Chinese understanding of how things work.

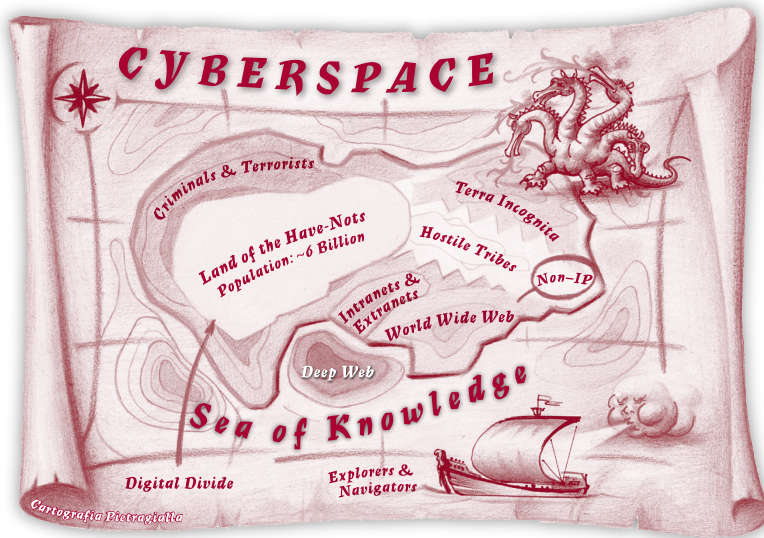
The outer circle of the yin-yang symbol represents “everything”, while the black and white shapes inside the circle represent the interaction of two separate energies, called *yin* (represented in black) and *yang* (represented in white), which cause everything to happen and which cannot exist without each other.

While *yin* is dark, downward, and cold, *yang* is bright, active, hot and expanding. The shapes of the yin and yang sections of the symbol give a sense of the continual movement of these two energies within the circle that encloses them, which causes everything to happen: for example, objects to expand and contract, and temperature to change from hot to cold or vice versa.

CYBERSPACE

- 
- Easy to connect to
 - Easy to learn
 - Facilitates publishing
 - Supported (in part) by fast optical networks
 - Facilitates the use of encryption
 - Facilitates anonymity
 - Transcends time zones and distance
 - Easy to hack
 - Easy to misuse
 - Easy to disrupt
 - Impedes data interception
 - Easy to hide in

The “map” of cyberspace as a frontier land (see below) has been used in other booklets in this series. It is included again in this discussion for two reasons: it illustrates both sides of the yin-yang concept by showing Hostile Tribes and Criminals and Terrorists, as well as the Sea of Knowledge. The Sea of Knowledge will also be relevant when we examine the legislative aspects of cyber-terrorism and cyberwar later on in this booklet, as the Law of the Seas appears to provide a number of useful analogies for the situation we find in cyberspace.



THE YANG SIDE

We know that it is *easy to connect to* cyberspace. In the world today there are over one billion fixed-line telephones and hundreds of thousands of private networks, which may or may not be connected to the Internet, in offices, factories, military installations, police force facilities, universities, hospitals and many other institutions.

The Internet, as already mentioned, has over 620 million account holders. While its presence and affordability vary between countries, this number continues to grow rapidly. Information content on the World Wide Web is becoming more multilingual and multicultural despite the digital divide between those who have all that is required to exploit this and those who do not.



An example of a Simputer, which uses so-called Open Source software.

New devices such as simple computers (or simputers), designed to be low-cost and requiring only a minimum level of literacy are appearing and will almost certainly further support this growth. Some of the prototypes of these simple computers contain a totally graphical user interface, without a keyboard. They support output that uses text-to-speech conversion, which has been technically mastered years ago and can be used to make the computer “speak” in any language, thus helping to overcome the illiteracy barrier.

It is also clear that it is *easy to learn* how to exploit the services and features of the Internet as illustrated by the success of initiatives to put computers in schools.



Exceptions

Some countries have set up barriers that make participating in chat rooms or even searching for information on the Web more difficult.

Such barriers can include, for example, the price of the service, even through an Internet café, or filters that block access to specific URLs (sometimes on the basis of national laws and regulations).

There are workarounds for most of these measures – except for price.

We also know that creating a website is within the reach of most computer users.

Cyberspace *facilitates publishing*. Unlike traditional publishing houses or professional journals, which have complex and formal editorial, review and approval processes, there are no such restrictions on the Internet or the World Wide Web.

For example, anyone who has access to cyberspace can participate in a chat room, post messages on a discussion board or create his or her own website. The first two activities require little effort and are free apart from the cost of Internet access itself.

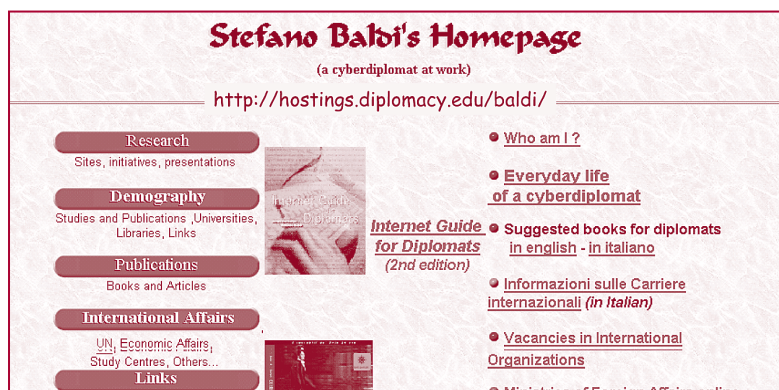
Creating a website may appear to be a more complicated task but a simple site can be constructed using a current version of any word processing package or any of a number of software packages that can be acquired for a modest amount of money.

Designing a high quality, high functionality website is a different story (see DiploFoundation's publication *Building.org* for more information on this subject), however, and requires specialised skills. For the purposes of hacking and hacktivism, simple, easy to build sites have proven to be quite adequate.

Registering a website (obtaining a domain name) is also easy (see the booklet *Internet Basics* in this series).

The ease of becoming a publisher on the Web is confirmed by the fact that as of August 2003, there were more than 42 million websites in existence (source: <http://www.netcraft.net>).

One of the authors of this booklet first created his own personal website way back in 1995 – its title at that time was “A Day in the Life of a Cyber-diplomat”.



Other essential features of the Internet particularly relevant to the topics under discussion in this booklet are optical networks, encryption and anonymity.

Cyberspace is supported (in part) by fast optical networks that circle the globe – mainly from west to east, with much less capacity being provided in the southern hemisphere. These networks provide very high capacity, thought to be sufficient for many years to come.

Optical communications technology, barely 30 years old, is inherently resistant to electromagnetic interference and is therefore difficult to intercept without physically cutting the line.

Cyberspace *facilitates the use of encryption*. Encryption, used to render communications unintelligible to all but the intended recipient, has become commonplace. Some of the software used for this purpose, such as Pretty Good Privacy (PGP), is available free of charge for personal use. In addition, many commercial products and services, such as public key encryption, steganography and more are readily available. This topic is discussed in more detail in the booklet *Information Security and Organisations* in this series.

Good computer programmers with the necessary knowledge of mathematics can also produce sophisticated encryption tools, and this is known to be the case as most of the information needed to do so is in the public domain.

Cyberspace *facilitates anonymity*, which refers to the ability to become untraceable in cyberspace, and particularly on the Internet. This can be easily achieved in many different ways, such as pre-paid cards for Internet access and Internet cafés, products for anonymous surfing (see for example <http://www.anonymizer.com>), anonymous remailers that forward e-mail messages and remove the identity and origin of the sender, stolen or cloned personal digital assistants, and e-mail accounts with fictitious names opened with one of the many free e-mail service providers (e.g. <http://www.hotmail.com>; <http://www.yahoo.com> and others).

Cyberspace *transcends time zones and distance*. Both factors have lost much of their meaning in cyberspace. Websites are available virtually 24 hours a day, 7 days a week. Postings and e-mail flow around the world instantaneously and many individuals have accepted this as the current lifestyle of the Information Age.

THE YIN SIDE

Counterparts to most of the elements described above do exist.

The mix of simplicity and complexity of the technologies used in cyberspace creates vulnerabilities that can be, and are, exploited by hackers and other members of the “uncivil society”. The simplicity is inherent in the basic protocols that describe how the Internet works. These protocols are designed to be well understood and documented. The complexity is present in the many different software implementations of the

underlying infrastructure (including operating systems, server management software, and browsers).

Cyberspace is *easy to hack*. The history of hacking (gaining unauthorised access to a computer or a network and then making computer systems perform specific functions against the wishes of the computer's owner) is almost as long as the history of computing itself.

The truth is that hacking is not that difficult to do. Besides, many hackers are frequently helped by system and network administrators who fail to take appropriate security measures.



Hackers are remarkably well organised. They form hacker clubs and arrange conferences, such as the annual DefCon conference, held in Las Vegas every August. The 2003 conference was the 11th in the series and it attracted some 10,000 participants. The attendees include not only serious hackers but also academics, vendors and law enforcement officials.

Hacking tools are readily available to anyone who is interested through the simple use of a search engine on the Web. "Serious" hackers design and use such tools extensively. Quite a few of these tools are available free of charge.

The screenshot shows a Google search results page. At the top is the Google logo and navigation links: Advanced Search, Preferences, Language Tools, and Search Tips. The search bar contains 'hacking +tools' and the 'Google Search' button. Below the search bar, it says 'Search: ☒ the web ☐ pages from the UK'. The navigation bar includes Web, Images, Groups, Directory, and News. The search results are for 'hacking +tools' with 727,000 results. The first result is 'Ben's phaster online web utilities (hacking tools)' with a description of exploits, bugs, and guides to ethical hacking. The second result is 'Tools' with a description of defensive and offensive tools. The third result is 'New Order - the computer & networking security portal' with a description of hacking, cracking, and security exploits. The fourth result is 'Best hacking tools - choose ...' with a description of finding all about hacking programs, tools, and hacks.

Google™ Advanced Search Preferences Language Tools Search Tips

hacking +tools Google Search

Search: ☒ the web ☐ pages from the UK

Web Images Groups Directory News

Searched the web for **hacking +tools** Results 1 - 10 of about 727,000

Ben's phaster online web utilities (hacking tools)
... includes: exploits/bugs, internet security **tools**, guides to ethical **hacking**, encryption, network security documentation, hacks, cracks, phreaking stuff, etc. ...
www.phaster.com/find_info_net_traffic.html - 26k - 25 Aug 2003 - [Cached](#) - [Similar pages](#)

Tools
Each of the **tools** below are discussed in "**Hacking Exposed: Network Security Secrets and Solutions**". Both defensive and **hacking tools** and web sites are presented ...
www.hackingexposed.com/tools/tools.html - 93k - [Cached](#) - [Similar pages](#)

New Order - the computer & networking security portal
Description: **Hacking**, cracking and security exploits.
Category: [Computers > Hacking > Cracking](#)
neworder.box.sk/ - 65k - [Cached](#) - [Similar pages](#)

Best hacking tools - choose ...
Searching for **hacking tools** ? You just found us ! All about **hacking** programs, **tools**, hacks and more. ... are you searching for. **hacking tools** ? Enter Now. ...
2biz.de/hacking-tools/ - 8k - [Cached](#) - [Similar pages](#)

Resourceful security practitioners also obtain such tools and apply them against their own systems and networks in order to identify vulnerabilities in their arrangements. For example, a system administrator could implement password-breaking software (no recommendations will be given here) on his or her network as a means of proving to those who do not wish to be bothered to design good passwords how easy it is to access their computers.

Anything that is easy to use is, reciprocally, *easy to misuse*. Every recipient of spam – unsolicited e-mail, which is often commercial in nature and sometimes downright absurd – has learned that this is true as such messages make up an increasing percentage of daily mail.

This booklet, however, concentrates on misuse at a higher level. It will deal with the convergence of activism, political or otherwise, and hacking (referred to as “hacktivism”) and beyond, the convergence of terrorism and hacking (“cyber-terrorism”) as well as the military use of cyberspace and its technologies (“cyberwar”).

Although both cyberspace and the Internet are very dependable and resilient to damage, they can still be disrupted, for example, through an attack on Domain Name Servers (see the booklet *Internet Basics* in this series). Spam e-mail is another technique that can be used for disrupting individuals’ surfing and overloading the global e-mail system. This involves the sending of spam mail in volumes in excess of a million per hour from a single source.

Other disruption techniques include Distributed Denial of Service (DDoS) attacks, used by hacktivists to literally “bombard” a targeted website or e-mail system until the point where it can no longer handle the volume of traffic and collapses. This technique will be explained in more detail in the section dealing with hacktivism.

The features of optical fibre communications and encryption also make the work of law enforcement agencies more difficult, as tapping such lines is physically difficult. Also, while there is some legal provision for obtaining encryption keys from public key infrastructure operators and from the provider of PGP and other vendors of such software, breaking a custom made encryption code requires enormous computing power and substantial time – up to a year or more if the code is well designed.

The “Bad Guys”, however they are defined, have access to all of these facilities as well as to anonymity and, as with other technologies, criminals are always among the first to adopt them, in order to gain advantage over those who try to stop them.

HACKTIVISTS, CYBER-TERRORISTS AND CYBER-WARRIORS

Among the 620 million people with access to the Internet, the vast majority are well behaved and make good use of the valuable information sources and services available, such as e-mail, online learning, and professional communities of interest dealing with such subjects as health and the environment to name but two.

However, even if only one individual in a million had somewhat less than benevolent intentions, this would still amount to six hundred such people. This is a much larger number than the ones mentioned in the box below. Such individuals acting in concert could dramatically disrupt any society that was heavily reliant on computer systems and networks. This happens to be the case for all the major economies in the world as well as for many developing countries.



At the end of 1999, Jim Settle, the former Director of the FBI Computer Crime Squad, stated the following: “You bring me a select group of ten hackers and within 90 days, I’ll bring this country to its knees.”

Security must have improved since then because on April 8, 2003, Mike McConnell, Vice-president of Consultancy at Booz, Allen and Hamilton and formerly with the US National Security Agency (NSA), was reported as saying that, “30 hackers and ten million dollars could bring the United States to its knees.”

We already know that DefCon (a major hacker convention held annually in Las Vegas) attracts over ten thousand attendees.

For the purpose of this discussion, we need to distinguish between four categories of players: cyber-criminals, hacktivists, cyber-terrorists and cyber-warriors.

We will not discuss cyber-criminals in this booklet. They are individuals, working either independently or in groups, who take advantage of the many freedoms that exist in cyberspace to perform criminal acts.

They are mentioned here simply because they use the same tools and techniques as the other players with one major difference: their aim is to remain undetected.

LEVEL OF DISRUPTION CAUSED		
HACKTIVISTS	<div>Propaganda Recruitment Fundraising Tools and Techniques</div>	CYBER-TERRORISTS
Instruments: Visibility Advocacy Publicity	Commonalities	Undermine - public confidence - institutional security Interfere with - critical infrastructures - emergency services
Goal: Embarrass targets		Objective: Remain undetected
Objective: Be seen and heard		

In practice, the other three categories also use the same tools and techniques to achieve their ends. The main difference between their activities is in the type and level of disruption that they intend to unleash against their targets.

For the purpose of this discussion, we will consider the main differences between cyber-terrorists and cyber-warriors to be those of sources of sponsorship and impact on the civilian population.

Cyber-warriors possess the characteristic of being sponsored by states and being subject to the oversight of their governments. It is hoped that states, if and when they engage in any form of cyberwar, will respect the appropriate sections of the United Nations charter. This is a topic that will be discussed again later in this booklet.

COMMON OBJECTIVES

The boundary between hacktivists and cyber-terrorists is blurred, as they both share the intention of bringing about disruption by using more or less the same tools and techniques. Both these groups use the Internet to advocate their causes (propaganda), and to find supporters, both to aid them financially (fundraising) and to participate in their activities (recruitment).

The level of collaboration and information sharing is rather high between hacktivists. The same is probably not true for cyber-terrorists.

Hacktivist targets are usually well defined – for example certain international organisations (World Trade Organisation, World Bank, International Monetary Fund and G8) have been targets of the anti-globalisation movement. Other groups of hacktivists protest against damage to the environment, genetically modified food, the mistreatment of animals and other causes.

It is also well-known that hackers and cyber-warriors on opposite sides of an issue or cause will “fight” each other by disrupting or defacing each other’s websites.



SECTION



2

The world of hacktivism

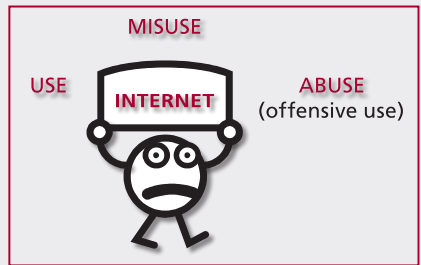
Hacktivism is the marriage of hacking and activism.

Prof. Dorothy Denning

THE WORLD OF HACKTIVISM

Many activists use the Internet in a non-disruptive and non-destructive manner, to further their causes with their supporters and the general public, to recruit new supporters, and to raise funds.

Most hacktivists appear to be passionately involved with their chosen causes. They are technically literate and make creative use of technology. Hacktivists themselves are happy to avoid any definition of what “hacktivism” actually consists of, as many of their websites and publications demonstrate. The common theme in their publications is the idea that hacktivism is merely another form of civil disobedience, albeit an electronic form.



Hacktivists can be divided into three groups, depending on how they approach their activities in cyberspace: whether they merely use cyberspace, misuse, or even abuse (or offensively use) it – the last form of activity possibly strays into the realm of cyber-terrorism.

Activist websites, for example, *use* cyberspace to offer documents, arguments and detailed information about the major issues related to their programmes, calendars of planned events, information on how to join their causes and/or support them financially, links to related websites as well as services such as e-mail newsletters. The freedom to publish on the Web is a major boon for activists.

Activism is most visible when it takes to the streets and becomes violent, as the picture on the right shows, taken during demonstrations against the World Bank and the IMF in Seattle, USA, in 1999.



Hacktivists are somewhat more subtle in their approach to political protest as they act without physical presence and without causing injury or lasting damage.

Typical forms of attack by hackers include electronic sit-ins and virtual blockades, automated e-mail bombing, viruses and worms, defacement and spoofing of websites as well as occasional computer system break-ins.

The birth of hacktivism is usually traced back to a group called the Electronic Disturbance Theater (EDT). In September 1999 this group organised a series of virtual sit-ins against targets which included President Zedillo of Mexico, the White House, the Pentagon and others.

During an electronic sit-in, the websites of targeted organisations become the victims of a Denial of Service (DoS) attack or a Distributed Denial of Service (DDoS), depending on how the attack is organised. During these attacks websites are accessed every few seconds by thousands of computers from all around the world, overloading the networks and servers and ultimately causing the websites to collapse.

Such attacks are not harmless. They can cause considerable economic damage to their targets as was the case with a series of coordinated

“This is relatively easy to do and not easy to defend against.”

— Peter Naumann,
SRI International
security analyst

attacks in February 2000 against electronic commerce websites. At this time, e-commerce operators including eBay, Amazon.com and Buy.com, along with Yahoo!, news site CNN.com, online trading sites E*Trade and Datek, and technology information provider ZDNet all reported similar DoS attacks. Janet Reno, US Attorney General at the time, stated that federal law enforcement officials would combine their resources to combat online vandalism.

Although they appear to be legal at present, Distributed Denial of Service attacks (DDoS) constitute a *misuse* of cyberspace as they disrupt the activities of others who have the right to a legitimate presence on the Web.

The Zapatista Tactical FloodNet

A collaborative, activist and conceptual art work of the net
by Brett Stalbaum

How were such attacks carried out? The answer is: “Relatively easily.” Websites were created to provide the necessary

software for the supporters of this movement. This software was designed to automatically request a specific page from a target website.

These attackers appear to consider that they are acting within the law, as they do not operate anonymously. Brett Stalbaum, the person named on the FloodNet site from where this software could be obtained, is now involved with another organisation called JTDDS (Joint Tactical Disinformation Distribution System). The URL for this organisation's website will not be provided in this booklet and readers are advised that a warning notice on the home page states:



“A visit to this site implicates the user in unauthorized attempts to upload information to U.S. government web servers. This is strictly prohibited and may be punishable under the Public Law 99-474 (The Computer Fraud and Abuse Act of 1986).”

In March 2000, another group, the Electrohippies, attempted to shut down the websites of the World Bank and the International Monetary Fund by launching another Distributed Denial of Service attack against these sites. They also targeted the World Trade Organisation and managed to reduce the performance of their website for periods lasting four or five hours at a time. The hacktivists claimed that over 450,000 people collaborated in swamping these websites.

The Electrohippies, established by five UK activists, insist that they are acting within the law and that they seek “a world where e-commerce is balanced by e-protest”, or at the very least, a system where cyberspace is not immune from public pressure.

There is disagreement within the hacktivist community concerning the Electrohippies' world view. The counterargument put forward by another hacker group, “The Cult of the Dead Cow”, is that Denial of Service attacks violate the First Amendment (of the US Constitution) privileges of their opponents, which guarantee freedom of speech.

Although their identities were never a secret, the Electrohippies were not arrested by law enforcement authorities and there was, at the time,

no consensus on the legality of their actions. Since then, however, new legislation in many countries states that interfering with a computer system is a criminal offence.

Hacktivism continues in various forms. Following the example of FloodNet, a group calling themselves RTMark is engaged in projects which it claims are designed to lead to positive social change.

Projects with roughly the same intent, risk, or likelihood of success are grouped into units known as “fund families”. One example is “The Frontier Fund”, which is dedicated to investigating the implications of allowing corporations and other multinational interests to operate outside of any social context.

FAKE (SPOOFED) WEBSITES

One of the most visible and original hacktivist activities connected to the WTO protests was the establishment of a look-alike site for the World Trade Organisation (<http://www.wto.org>), using the name of its predecessor organisation (<http://www.gatt.org>). It appears that when the World Trade Organisation was re-named, no one thought of retaining the organisation’s previous official domain name of <http://www.gatt.org>, which thus became available to the creators of the alternative site. They do not seem to be breaking any laws by impersonating the World Trade Organisation and it is unclear whether this constitutes misuse or can still be considered legitimate use.

The official website of the World Trade Organisation and its hacktivist alternative (both screens were captured on the same date in late July 2003) are shown below:

The image shows two side-by-side screenshots of websites. The left screenshot is the official World Trade Organization (WTO) website, featuring the WTO logo and navigation links such as 'THE WTO', 'WTO NEWS', 'TRADE TOPICS', 'RESOURCES', 'DOCUMENTS', and 'COMMUNITY/FORUMS'. The right screenshot is a spoofed version of the WTO website, mimicking the layout and content of the official site but with altered details, such as the 'WTO' logo being replaced with a stylized 'W' and 'O'.

WORLD TRADE ORGANIZATION

search on this site register contact us

THE WTO | WTO NEWS | TRADE TOPICS | RESOURCES | DOCUMENTS | COMMUNITY/FORUMS

español français

[A-Z list](#) [Site map](#)

FREQUENTLY VISITED

IN THE WTO

[What is the WTO?](#)

[The director-general](#)

[Vacancies](#)

WTO NEWS

General Council extends timeframe to review WTO dispute settlement rules to 31 May 2004

At its meeting on 24 July 2003, the General Council agreed to extend negotiations in the Dispute Settlement Body Special Session which is reviewing WTO rules for dispute settlement. The timeframe was extended from 31 May 2003 to 31 May 2004. [News page](#)

Also:

- > Working party completes Cambodia's membership negotiation. [News page](#)
- > Australia, Brazil and Thailand request a panel to examine the EU sugar subsidy regime. [News page](#)

IN TRADE TOPICS

Watch this space ...

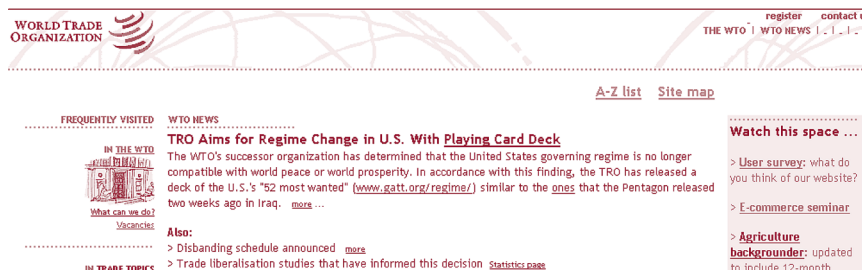
Cancun Ministerial Conference

10-14 September 2003

[Main Page](#)

> [Media accreditation](#)

The fake site looks very similar and contains numerous links to the official WTO site, but the content is not that intended by the WTO.



WEBSITE DEFAACEMENT

A war of words escalates into a war of action when the contents of a target website are modified without the consent of the owner. This is a frequent phenomenon, the electronic equivalent of painting graffiti on a wall. It could be argued that such action constitutes *offensive use* (or abuse) of cyberspace.

Many such defacements are simply too offensive to include in this booklet. A sample collection of images of sites that were defaced in the past can be found at:

<http://www.appsecinc.com/resources/security/defacedwebsites.html>

Ongoing defacements can be viewed at:

<http://www.zone-h.org/defacements/onhold>

How do hackers deface websites? By gaining access to the servers where the web pages are located. In order to do this they need a thorough understanding of how effective the defences put in place to prevent access actually are. The number of sites continually defaced confirms that accessing some servers is not very difficult. As discussed in other booklets in this series, sometimes the most basic security features are omitted by system administrators, allowing hackers easy access to their systems. Regrettably, this is not an uncommon occurrence and the authors have seen many examples of such security gaps (which were immediately reported to the owners of the websites, of course).

Website defacement battles between rival hackers have occurred in most conflict situations of the last few years. It is not known whether these hackers were government-sponsored. Given that no material damage is involved, it is inappropriate to refer to such actions as “cyberwar” as some media have done, because they have more to do with vandalism than with warfare.

POTENTIALLY VIOLENT AND CRIMINAL HACKTIVISM

Many hacktivist groups exist, each with its own objectives and “culture”. Not all of them abide by the concept of non-disruptive and non-destructive activities to promote their ideals. For example, some websites provide information about doctors and clinics which offer abortion services and advocate violence against them, even murder in the case of the doctors. Many websites around the world advocate hate. Some countries have introduced legislation that bans such sites, for example Germany. In such cases governments rely on the cooperation of Internet service providers to remove the illegal content.



In January 2001, a hacktivist group calling itself the *Virtual Monkey Wrench* hacked into the computer systems of the World Economic Forum, meeting in Davos, and obtained the confidential information, including credit card numbers, of 27000 forum attendees.

This information was written onto a CD-ROM and given to a journalist working for a Swiss newspaper. While an arrest was made in this case, no charges were ever raised as it became clear that the World Economic Forum’s database was not adequately protected (see the discussion above): the system administrator’s password was simply “sa” – a rather obvious guess for a hacker.

A number of hacker groups, such as the “Cult of the Dead Cow”, “2600” and the “Electrohippy Collective”, advocate the unconventional use of technology to promote and assist certain political causes. They make software tools available to aid hacktivism and to bypass government restrictions (such as filters that block certain URLs) although this may be a subversive or illegal act in many countries.

LEGAL MEASURES DEALING WITH HACKTIVISM

Several governments have begun to see politicised hacktivism as a potential threat. For example, the UK's Terrorism Act of 2000 defines terrorism as: *"the use or threat of action ... designed seriously to interfere with or seriously to disrupt an electronic system."*

To date, UK legislators have not had to deal with a hack deemed to be an act of terrorism.

The US Patriot Act signed into law in October 2001 raises the maximum sentence for breaking into a computer network from five years to ten. The Cyber Security Enhancement Act passed in July 2002 calls for up to life imprisonment for hackers who recklessly cause or attempt to cause someone's death.

Hacktivism and human rights organisations have both been vocal in their disagreement with this approach, which, they say, places politically motivated hacking in the same category as life-threatening acts.

On the other hand, apart from ethical hacking, intended to discover system vulnerabilities and report them to the system vendors, designers and administrators, is there really such a thing as "innocent hacking"?

WHAT IS THE FUTURE OF HACKTIVISM?

It is difficult to make predictions about the future of hacktivism, because hacktivist movements are so highly dispersed and adhere to so many different philosophies and motivations. However, given that many of the tools and techniques developed by hackers are widely distributed on the Web, it would be safe to assume that the number of individuals who obtain these tools and experiment with them is not going to diminish. At the same time, hacking tools are improving, and consequently have greater impact on the targeted systems.

If hacktivist movements remain as disorganised as they are now, at the most, the status quo may be maintained. However, we know that the Internet makes it easy for groups with common interests to unite for certain events or actions, and this phenomenon is likely to become more and more effective.

With the expansion of the Internet, societies are becoming increasingly dependent on its information infrastructures and services in the areas of government, business and other activities. As we describe later in this booklet, security is not yet a prime consideration in the design and implementation of networks and, as a result, the risk and impact of potential attacks will continue to increase.



The media's portrayal of hacktivism benefits the vendors of security tools and products intended to stop them, but does little to clarify whether hacktivists are the latest version of activists, radicals, potential terrorists, or simply disenfranchised individuals.

It is hard to conclusively demonstrate that a particular group of hacktivists is aligned with, or supported by, a particular hostile government.



SECTION



3

Cyber-terrorism

*Tomorrow's terrorist may be able to do more damage
with a keyboard than with a bomb.*

*US National Research Council
"Computers at risk", 1991*

As the previous section shows, hacktivists can be divided by their philosophies and not all advocate the offensive use of cyberspace. However, the number of overtly hostile activities in cyberspace is increasing. This is a factual observation supported by many independent and authoritative sources.

Although much is written about cyber-terrorism, all of it is speculative, because there is no public record of an attack on a computer system or network that was attributed to (or claimed by) a group defined as a “terrorist organisation”.

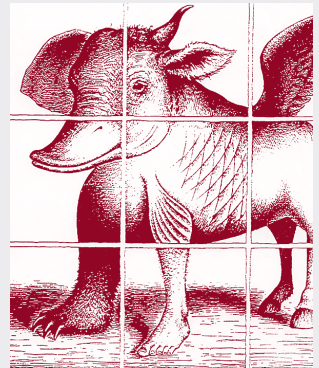
A possible definition of terrorism as it applies to cyberspace has been put forward in an FBI paper on cyber-terrorism:

Cyber-terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by sub national groups or clandestine agents.

The problem of definitions will be discussed again in Section 6, where a lack of adequate definitions relating to terrorism or war scenarios in the virtual world of cyberspace will be covered.

It is well known that hackers from around the world continue to target the facilities of their own, as well as of foreign governments, militaries, nuclear power plants and others. Every attack helps hackers learn more about the defences that are out there. These encounters have become a battle of wits between the hackers and the defenders.

How would cyber-terrorism differ from the current activities of hackers, hacktivism or criminals in cyberspace?



To date, most terrorist acts have involved the use of explosives as well as instances of the use of chemical and bacteriological weapons (such as Sarin gas in Japan and anthrax in the US). These attacks attracted extensive media coverage.

There is no single hacker culture. Like the picture on the previous page, the image of a “hacker” has many different components that do not fit well together.



The basic “hacker” is a male (hacker literature and hacker conventions indicate that, unlike in the movies, there are very few female hackers) who uses his technical skills to exploit unintended features and facilities in computer systems and networks. Ethical hackers report these loopholes in security, unethical ones abuse them.

Hacktivism uses technical skills to deface websites, redirect traffic, and launch e-mail bombs related to a particular target.

Cyber-criminals operate for financial gain, for example, the theft and subsequent misuse of credit cards.

Cyber-terrorists are not thought to be primarily interested in criminal activities such as the theft of credit cards but in activities that would:

- achieve global and highly visible media attention;
- impact economic systems;
- destabilise civilian life and create panic;
- wage asymmetric warfare against law enforcement and other government agencies;
- diminish trust in a government’s ability to protect its population;
- exploit any successes from the above to gain new support for their causes.

Who can become a cyber-terrorist?

The bad news is that in principle, almost anyone with adequate computer skills can become a cyber-terrorist. At a recent informal workshop on information security, a senior information technology manager working in a military organisation said that the best information security policy is simply to “Trust No One”.

Analyses about potential cyber-terrorists tend to assume that they are foreign nationals. However, many such foreign nationals have completed university studies, training programmes, have work experience in technologically advanced countries and may reside in yet another country.

Other foreign nationals may have been born in the country where the analysis is conducted and lead ordinary lives, but culturally, may still be strongly attached to another country’s culture, and possibly, politics.

The trusted insider is discussed in more detail in later sections and is thought to present the most danger of all.

DEFENDER

- Policies
- Technologies
- Operating processes
- Staff and ERT
- Contingency plans
- Crisis management
- Much to lose

ATTACKER

- Has easy access to know-how
- Operates with minimal infrastructure
- Gains new knowledge about defences with every attack
- Has nothing to lose

**Cost, Effort,
Traceability, Risk,
Impact, Motivation**

The *cost* of mounting a cyber-attack (a few personal computers, some software tools, know-how) is almost trivial when compared to the cost of building, implementing and operating the required defences.

The *motivation* of the attacker seems to always be greater than the motivation of the defender.

Attackers face little or no *risk* when operating from a distance. Even when an insider is involved in an attack he or she may remain undetected for long enough to be able to disappear. Moreover, legislation is not always in place to deal with such actions.

When their time comes, as it almost certainly will, cyber-terrorism and cyberwar will take place in the electromagnetic spectrum and will have an impact on the physical world: data, databases, networks, computers, satellites, data centres, telecommunications exchanges and the systems they support are all potential targets. Such systems are essential in the operation of critical infrastructures, emergency services, military activities, hospitals, etc.

A cyber-terrorist attack could take one or more of the following three distinct forms:

- A **physical** attack aimed at destroying a networking, telecommunications or computing infrastructure or at disrupting signals and messages. For example, it is possible to jam the signals from Global Positioning Satellite (GPS) systems.
- A **syntactic** attack that causes computer systems to perform undesired functions. This occurs when malicious code (such as a virus, worm, logic bomb or Trojan Horse) is inserted into a computer system to perform specific functions.
- A **semantic** attack in which disinformation is used to instigate a harmful reaction.

Physical attacks will not be discussed here as these have little to do with cyber-terrorism but the possibility of a terrorist organisation using more conventional approaches to attack critical infrastructures cannot be excluded. Besides, the likelihood and effectiveness of cyber-attacks being launched in support of conventional ones should be seriously considered.

SYNTACTIC ATTACKS

Syntactic attacks occur all the time, and malicious code is becoming quite sophisticated. Moreover, it is extremely hard to trace the originators of such code.

The creators of such worms as Code Red, Nimda and Slammer remain undetected and unknown to this day. On January 29, 2003, *Information Week*, a highly respected journal covering the ICT industry, stated the following:

Leading experts on Internet security are sceptical that the FBI and other investigators will be able to track down whoever was responsible for last weekend's attack on the Internet. These experts, including many who provide technical advice to the FBI and other US agencies, said exhaustive reviews of the blueprints for the attacking software are yielding few clues to its origin or the author's identity.

"We don't have the smoking gun," said Ken Dunham, an analyst at iDefense Inc., an online security firm... "being able to track down the specific source of this is very unlikely".

But the situation is even more complicated than it first appears. Many experts believe Slammer was based on software published on the Web months earlier by David Litchfield, a British computer researcher. It was later modified by a virus author known within the Chinese hacker community as "Lion".

Litchfield has stated that he now appreciates the dangers of publicly disclosing such computer code. He said he originally published those blueprints in order to help computer administrators understand how hackers might use such a program to attack their systems.

This raises an important ethical issue. Scientific and technical progress requires the exchange of information. But researchers like Litchfield face a dilemma. Their publications could help unscrupulous individuals to create cyber-weapons – assuming you agree that malicious code can be used as a weapon.

The optimists also fail to consider the possibility that Slammer (and similar malicious code), which spread around the world in just one hour, causing damage estimated at US\$1 billion, may have been just a *proof of concept*. In this case Slammer did not have a destructive payload. However, the existence and use of military strength viruses and worms (frequently mentioned in works of science-fiction) cannot be excluded.

SEMANTIC ATTACKS

A familiar example of a semantic attack is the issuance of a fake, but apparently legitimate, press release announcing that a certain company's results will be considerably worse than anticipated. This would immediately create a wave of selling of its shares which could drop dramatically in value.

In this particular example, the crisis would normally be of short duration because official denials as well as independent sources would establish the falsity of the press release, and the shares would regain their value in a fairly short period of time.



We also need to consider what Clifford Stoll said about the worst thing that could happen to him as an astrophysicist: for someone to alter the fifth decimal value of the constant π (pi) in his computer, as this would render all of his work useless.

Clifford Stoll is the author of the book *Cuckoo's Nest*, the personal story of how he, an astrophysicist, became a system administrator who became a one-man security force tracking down a computer cracker when he discovered a 75 cent accounting error.

Many other kinds of semantic attacks have been envisaged which would have an even greater impact. Here are a few speculative examples found in various publications:

- alter the quantities of the various ingredients that go into making a medication;
- modify the formulae used to calculate the amount of fuel needed by an aircraft;
- create phantom airplanes in an air traffic control system;
- alter the calculations of social security benefits or income tax.

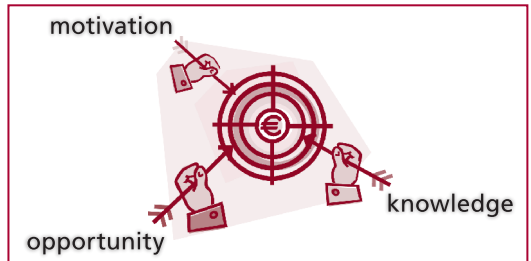
The optimists say that such schemes are “too difficult” and that they are too unlikely to be taken seriously.

The authors cannot side with the optimists due to one additional potential component of cyber-terrorism: the trusted insider.

THE TRUSTED INSIDER

These individuals represent a major risk simply because of the fact that a well placed insider enjoys privileged access to systems and facilities.

An insider will not only have privileged access but also the necessary knowledge of how the system works. Many years of studies of computer crime show that few insiders act with malice, but that those who are unaware of security issues, trusting and full of good will can be taken advantage of by individuals with malicious intent. One of the most important factors in maintaining adequate information security is the awareness of how “social engineering” works.



For example, a visitor to a facility or office politely asks to be given access to a computer for a few minutes to send an urgent e-mail, or pretends to be a maintenance engineer and requests access to the computer room to perform some tests.

Except in organisations with strong security cultures, it is not uncommon for requests such as these to be granted, and if the visitor in question happens to be an agent of, or a cyber-terrorist himself with good computer skills, this simple action would bypass all the barriers set up to prevent external interference.

Disgruntled staff can also act with malice on their own initiative or through pressure from a third party.

Two recent examples illustrate the risk that trusted insiders represent:



Queensland, Australia, April 2000: A disgruntled employee hacked into a computerised sewage control system and instructed it to release one million litres of untreated sewage into the grounds of a luxury hotel. Detected and arrested, he was tried and found guilty of 46 charges of computer hacking. His sentence: two years in jail.

Italy, August 2002: Fourteen Italian hackers known as the “Reservoir Dogs”, almost all of them information security professionals, were arrested by the Italian Financial Police and charged with hacking into the networks of NASA, the US Army, the US Navy and several universities. The European Electronic Crime Task Force (EECTF) was able to seize and subject the computers of the arrested individuals to a forensic examination that recovered enough evidence to keep the defendants in jail until a more complete investigation was completed in the US.

This is not the end of the story. The definition of “insider” has changed fundamentally as a result of the use of outsourcing for software development, maintenance and operations support.

Outsourcing has become a global industry with a turnover of some US\$100 billion a year. A substantial part of the work has moved to countries where the earnings of ICT personnel are much lower (as much as 90 percent lower) than in the US and Europe. Countries with a substantial presence in software development include India, China, Russia, the Philippines and Pakistan.

The usual measures of conducting background checks, closely supervising the activities of such personnel and carrying out security vetting are, in most cases, not available or not under the control of the client. When new software is destined for a critical infrastructure or a major global commercial enterprise, outsourcing can create a potential security issue.

Several vendors offer monitoring systems that have the capability to track and analyse the activities of individuals in an office, such as access to restricted areas, attempts to log on to systems to which they have no access rights, as well as their electronic mail and Web usage, etc. These systems are invariably expensive and complex to implement.

While appropriate in locations where high security is essential, their use may be controversial elsewhere as it raises questions of civil liberties, privacy at work and many other human rights issues.

The economic impact of cyber-terrorist activities, if and when they occur, must not be underestimated: reports for 2001 estimated that the



cost of malicious code (virus and worm infections) to the US economy had a price tag of US\$17 billion. These expenditures were required to clean malicious code from all affected equipment, restore lost and corrupted data, help end users while this work was in progress and also deal with external clients whose systems were affected or who could not access the services they required. In addition, it was necessary to test and restore systems to normal operations. The

above figure includes an estimate for the productivity lost during the time computer systems were down.

These costs are constantly increasing because malicious software is becoming more sophisticated and spreads around the world faster than ever before. While the Melissa virus of 1999 took four days to go around the world, the “I Love You” virus (2000) did so in just one day, Code Red (2001) in a few hours and the Slammer worm (2003) in just one hour. Malicious code alerts are also becoming more frequent.



SECTION



4

Thinking about cyberwar

War is the continuation of politics by other means.

Karl von Clausewitz

THINKING ABOUT CYBERWAR

The attacks described in the previous two sections could equally well be carried out by cyber-warriors engaged in a state-sponsored action. This invites two questions: Will there ever be a cyberwar? Will cyber-terrorists disrupt civil society?



Many individuals have no doubts. In May 1998, addressing the US Naval Academy, US President Bill Clinton said the following:

Our security is challenged increasingly by non-traditional threats from adversaries, both old and new, not only hostile regimes, but also international criminals and terrorists who cannot defeat us in traditional theatres of battle, but search instead for new ways of attack by exploring new technologies and the world's increasing openness.

He then added: "... intentional attacks against our critical systems are already under way".

This statement, not the only one of its kind in the last few years, seems to suggest that cyberwar has already started; however, it has not yet had enough impact to become instant global news.

This statement also reiterates the view that information security, in all of its aspects, is not merely a technical problem. Primarily, it is a problem of human action and the only way to manage it is to apply one of physics' fundamental principles: a reaction of equal force in the opposite direction, which also consists of human action.

The technologies of electronics, computing and communications all found their place in the fields of intelligence, defence and law enforcement many years ago. Intelligence, defence and law enforcement activities today rely on high quality information flows in order to be effective. Therefore, in situations where violence is highly likely, for example in the field of battle, one of the key goals will be to disrupt or confuse the enemy's communications and information handling capabilities.



One aspect covered by the media in the early part of 2003 was the threat of interference with the signals from the network used for Global Positioning by Satellite (GPS). It was reported that the equipment needed to disrupt these (very low intensity) signals is already available in many countries.



It is interesting to note that the US Airline Owners and Pilots Association (<http://www.aopa.org>) has conducted tests on GPS interference and jamming, and that the US Department of Transportation Volpe Center (<http://www.volpe.dot.gov/ssd/ssd-gps.html>) is also planning to do so.

However, a cyberwar scenario involves much more than just field communications and intelligence gathering. After all, these have been part of the battlefield for most of history. The following sections deal with the main components of cyberwar:

Remote reconnaissance and sensing: This involves data collection through satellites, monitoring systems and listening posts; covert message interception by official agencies (through the use of such systems as Carnivore and Echelon) and others, including hostile parties; and subsequent analysis of the data gathered.

State monitoring and tracking: Within the framework of national and regional legislation (such as the European Union's Data Protection Directive), a country has the right to intercept, track and monitor any individual's communications and activities in cyberspace. Many concerned parties have expressed the view that such laws may be abused and that they could fundamentally change the concepts of privacy and personal freedom.

State intelligence gathering and analysis: These activities are organised and executed by countries, acting against other countries, individuals or groups suspected of illegal activities (such as activists, terrorists, organised crime and companies illegally supplying their products to specific countries).

State sponsored cyberwar: This can take several forms and include many activities such as:

Non-destructive (Information operations)

- information dissemination in support of a cause;

- disinformation dissemination to create confusion;
- communications interference to delay messages or render them unusable;
- communications interception and modification.

Disruptive (Information operations and information warfare)

- disruption of critical services and infrastructures through electronic means including, but not limited to, hacking.

Destructive

- use of smart(er) weapons;
- use of high energy weapons (radio frequency and plasma streams/electromagnetic pulse) to damage electronic circuitry.

It would be sensible to assume that most information on this topic is classified, as little else can be found from government sources. Many think tanks and academic centres do research and publish material on this topic but it should be considered mostly speculative.

This booklet presents four major assumptions about cyberwar:

Assumption 1: Technology can be used outside of our perceived ethical limits.

Assumption 2: Every technologically capable country – not just the OECD members – is working on information warfare programmes.

Assumption 3: Such programmes include both defensive and offensive activities.

Assumption 4: The military employs hackers to help them with these programmes.

MIGHT THE MILITARY CONSIDER EMPLOYING HACKERS?

Hacktivism is convinced that government-employed hackers are working against them. It has been reported that since the September 11, 2001 attacks on the United States, some hackers have been quietly offering their skills to the US government.

There is a lot to be said in favour of gaining inside knowledge. If you are fighting against individuals with hacking skills, it may be a good

idea to learn from other members of these hacking communities. This could be done by joining hacker clubs or using “honeypots”, which are combinations of hardware and software that have been set up to trick unwary hackers into thinking they are successfully penetrating interesting networks and systems while in fact all they are doing is disclosing the techniques they use to gain access (see the booklet *Information Security and Organisations* in this series). However, such techniques are not likely to be as successful as actually recruiting a competent hacker with the right motivation. At first sight, this might appear to be unworkable.



The image of the military is one of strict discipline, including dress code, total commitment to the principle of the chain of command and much emphasis on physical activity.

On the other hand, the popular image of hackers is at odds with all of the above and most of their websites advocate civil disobedience as part of a new world order. Frequently thought of as being male (the vast majority indeed are), they describe themselves as non-conformists who live by their own rules. The popular press presents them as unshaven, badly dressed, tattooed, and undisciplined. This is an image that many hackers are happy to support as photographs and TV reports from hacker conventions demonstrate.



These differences might lead one to believe that these two cultures are mutually exclusive and non-reconcilable. However, many hackers have respectable full time jobs – sometimes they are responsible for information security, as was the case with the group calling itself “Reservoir Dogs”, described in the previous section. It is no secret that hacker conventions such as DefCon are also attended by government and military representatives, many of them openly, some of them possibly secretly.

We’ll never know the full story as it is unlikely that a government department dealing with security would make public statements about its strategies. However, it is not unreasonable to assume that if hacking and code design skills cannot be found among the usual government and military employees, these would have to be recruited from outside, specifically, the hacker community.

TRAINING THE MILITARY



Military colleges and academies include information technology topics in their curricula, and courses of this kind have titles such as “Digital Battlespace and Information Warfare”, “Electronic Warfare”, “Information Technology and National Security”, exploring both the defensive and offensive aspects of this field.

Many major conferences have dealt with information security issues as well as with information warfare. One example was the Infowar-Con, held in Washington DC in late September 2003 with the slogan “*Learn the tactics and technologies of digital warfare*”. The speakers included representatives of the US Secret Service, the National Infrastructure Protection Center (NIPC/FBI), InfraGard, the US Air Force Information Warfare Center and the White House’s Office of Homeland Defense. (InfraGard (<http://www.infragard.net>) is an organisation that brings together US industry and government to encourage the exchange of information between them.)

A search for “information warfare”, “information operations” and “guerre électronique” courses reveals that these topics are found in the curricula of many military colleges, including for example:

- Naval Postgraduate Courses of the US Navy
- Information Resources Management College of the US National Defense University
- Defence Academy of the United Kingdom at Cranfield University
- Ecole Nationale Supérieure de l’Aéronautique et de l’Espace in France

Such topics are also dealt with in organisations in Canada and other countries where such information is published on the World Wide Web.



The course curricula of military academies published on the World Wide Web, for example that of the Information Security Network, hosted by the Zürich Electrotechnical University (ETHZ) at:

http://www.isn.ethz.ch/wgcdn2/wgcdn_catalogue.cfm

confirm that both the defensive and offensive aspects of the use of information systems in a military setting are covered in these courses.

In addition, the Federation of American Scientists (<http://www.fas.org>) has translated and published articles excerpted from China’s *Military Science*, for example “The Challenge of Information Warfare” by Major General Wang Pufeng, from Spring 1995.

While we can only speculate about how an Information Warfare scenario would evolve, a few possible stages can be identified:



Level 0: Gathering public information from websites, newspapers, official publications and even overheard conversations could not possibly be considered either a breach of the peace or an activity incompatible with diplomatic status.

Level 1: Intercepting an unencrypted e-mail message may breach national legislation but again, it is unlikely that it would be considered a breach of the peace.

Level 2: It is conceivable for one party engaged in some kind of information warfare operation to create the equivalent of an electronic minefield. For example, a specially designed Trojan Horse is embedded in a document likely to be of interest to outside parties. This document is kept in a well protected system that is appealing to prospective hackers, with the intention that one of them will find and download it.

The perpetrator of this intrusion and data theft will now have imported a professionally designed piece of malicious code, which conventional anti-virus software cannot detect. So far, the Trojan Horse has not been activated and therefore, the only offence committed is the theft of a document. An interesting legal question arises when the party who obtained this document activates the embedded Trojan Horse – such code might be designed to copy itself into and infect an entire target system, acting like a minefield. Did the party who originally planted this code in their system commit an offence?

Level 3: This is the same as Level 2 but from the reverse perspective. Does the penetration of a protected system to access one or more documents constitute an offence? The answer is yes, in all those countries that have legislation on computer crime. Will it constitute a breach of the peace if two countries' military forces are involved?

Level 4: This level involves a scenario such as the following: One party penetrates another party's systems to plant malicious code or a back-door that would provide it with access in the future. This constitutes an escalation from Level 3 because of the intent to interfere with the prop-

er functioning of a private computer system through the planting of malicious code or a backdoor.



The Kosovo War is considered by some analysts to be the first war with a strong “cyber” element. The Internet was used mainly by the Yugoslav side for propaganda purposes and attacks on information systems. The question of why NATO did not cut Internet access to Yugoslavia, which was not only technically feasible but also legally justifiable under the sanctions regime, remains open. Some analysts have argued that the Internet was a very valuable source of information for NATO about the precision of bombing, the mood of the population, etc. Thus, a mutual interest to leave the Internet operational was established, as was a new war interdependence.

Level 5: This level could be called one of anticipatory self-defence. Here is a quick example to illustrate. A government department in some country has evidence (or strong suspicion) that a cyber-attack is about to be launched against them by a hacktivist group (the Electrohippies, for example, had made it clear that they intended to conduct an electronic sit-in against the World Trade Organisation). What would be the legality of pre-emptive action taken against the likely offenders, assuming such action complied with the principle of proportionality, or of a pre-emptive cyber-attack against the potential hackers?

The authors could not find authoritative answers to these questions despite consulting numerous sources.

To conclude this section, the following quote from Gregory J. Walters (Gordon F. Henderson Chair in Human Rights and Associate Professor of Ethics at Saint Paul University, Ottawa) that appeared in the “Argument & Observation” section of *The Ottawa Citizen* on Saturday, March 14, 1998, is highly appropriate:

Information warfare blurs the traditional ethical distinction between civilians and combatants because a high percentage of military communications travel along civilian owned and operated systems. An information warfare attack aimed at a nation's power grid, transportation, communications and financial infrastructures could never be morally acceptable. School children, hospital patients, the elderly, the ill, the average worker producing goods not directly related to military purposes, farmers, and other 'non-combatants,' all would suffer from such an attack.

TABLE OF ATTACKS AND ATTACKERS IN CYBERSPACE

Group	Motivation	Type of attack	Reported cases (selection)
Script kiddies	Inexperienced hackers. - curiosity; - teenage bravado.	Use readily available software and code downloaded from the Internet. Potential damage: low to medium.	Frequent cases of attacks on private users or on companies.
Hackers	Experienced hackers. - challenge of breaking through new defences; - financial gain (sometimes).	More sophisticated automated tools. Can organise coordinated attacks. Potential damage: medium to high.	Same as script kiddies. - defacements; - Denial of Service (DoS); - cases of organised attacks on big companies and institutions (Distributed Denial of Service - DDoS); - DDoS attacks on Yahoo!, eBay and CNN (February 2000).
Malicious insiders	- revenge; - extortion and blackmail.	Wrongful activity through full access to information systems. Potential damage: medium to high.	Companies and institutions suffer from this kind of attack. Case of Australian sewage plant (2000).
Hacktivists	- propaganda; - political; - social and economic; - religious.	Same as script kiddies and hackers but with different motivations. Potential damage: medium to high. The ultimate cost of attack is generally greater for commercial targets than for government ones.	From Seattle (1999) on, protesters have often coupled traditional protests with online actions. - Palestinian-Israeli Hacker Conflict (1999 – 2002); - US-China cyber-skirmish (May 2001).
Cyber-terrorists	- propaganda; - political; - economic; - threat to national security; - espionage.	Potential attacks on Central National Infrastructures (CNIs): - electrical power systems; - oil and gas pipelines; - water supply infrastructures; - national air traffic systems; - banking systems. Potential damage: high.	No officially reported cases.
Cyber-warriors	- gather political or economic intelligence; - steal trade secrets; - disrupt critical infrastructures.	Same as cyber-terrorists.	No officially reported cases.

This classification of the threat groups is partly adapted from the publication *Threats to Canada's Critical Infrastructure* by the Government of Canada – Office of Critical Infrastructure Protection and Emergency Preparedness (http://www.ociepc.gc.ca/opsprods/other/ta03-001_e.asp).



SECTION



5

Known facts and unknowns

(see also the booklet *Information Security and Organisations* in this series)

*Apart from the known and the unknown,
what else is there?*

Harold Pinter, playwright

THE THINGS WE KNOW

About legislation

A few hundred years ago, justice was swifter and punishment more severe. Recent court cases dealing with hacking, intellectual property theft and other cyber-offences have resulted in relatively minor fines or prison sentences for the perpetrators.

In addition, current legislation, both national and international, does not appear to prohibit the production, distribution or possession of software such as viruses, worms, Trojan Horses or others with comparable purposes, at least *when it is not used to commit a crime*. It is perfectly legal to obtain hacking software to test the security of one's own computers and networks. A substantial part of current legislation addresses physical weapons.



Section VII of the UN Charter covering “action with respect to threats of the peace, breaches of the peace, and acts of aggression” in articles 39 to 51 does not deal with actions such as those described in this booklet, except for Article 41.

Information and communications technology (ICT) and society

ICT systems are ubiquitous in all OECD countries and are spreading to the rest of the world. The orderly operation of a society is heavily dependent on ICT and further relies on the integrity of such systems and networks. The following list summarises these dependencies:

- Entire industries and services are totally dependent on ICT: funds transfers, online trading, just-in-time deliveries, logistics, inter-connected power generation networks, air traffic control, telecommunications, water supply.
- The links that exist between enterprises as well as between government departments, emergency services, etc., resemble a line of dominoes.

- Outsourcing of software development, network development and operations, data centre operations, call centres and help desks is a major industry (US\$100 billion/year). Much software development is outsourced to India, China, Russia, Pakistan and other countries where it is not possible to exercise control over the staff or conduct security clearances.
- The latest statistics for the number of Internet accounts indicate a number of over 600 billion.
- Tens of thousands of non-IP networks are used by business, transportation, the military and emergency services.
- Over 1 billion fixed telephones and 300 million cell phones are in use today.
- Giant networks are getting larger: for example, in 1996, the US Department of Defense had 2.1 million computers connected to 10,000 local area networks, which in turn were linked to 100 wide area networks. Numbers and complexity have increased since; as a result manageability has become an important issue.
- The interconnection of fixed computer networks to wireless systems (such as computers, personal digital assistants and smart phones) through wireless LANs, GPRS and 3rd Generation (3G) systems pose new headaches for security managers.
- Extensive published research on high energy and directed energy weapons that can damage electronic circuitry is available.
- Techniques that are capable of interfering with (jamming) Global Positioning by Satellite (GPS) systems have been developed.
- The subjects of “cyberwar” or “information warfare” are now on the curricula of several war colleges.

All of the above are well known facts, readily available to potential cyber-terrorists around the world. Moreover, information about the vulnerability of such systems is relatively easy to obtain.

All networks are at risk of attack, particularly by those individuals with access to inside knowledge (employees, former employees, vendors' employees, trainers, consultants and many others who are essential components of today's complex computerised work environments).

In addition, our increasingly networked societies and business environments add further to the complexity, as more organisations establish partnerships with each other, requiring them to interconnect their

systems and networks in order to either jointly participate in electronic commerce or be part of each other's supply chains.

Obviously the most visible effects of cyber-attacks are seen on the Internet but the most damaging and expensive are, and will continue to be, felt in businesses, services and military systems, many of which are not even connected to the Internet or, if they are, it is behind several layers of protection.

About ICT vulnerabilities and security failures:

Information security, according to the ISO 17799 "Code of Practice for the Management of Information Society", consists of three sections: Availability, Integrity and Confidentiality.

The *Code of Practice* and other publications on security all make it clear that 100 percent security can never be achieved and that as a result there will always be a *residual risk*. The cost, complexity and effort needed to achieve a very low residual risk are all very high.

The best cyber-attack survivability rates are achieved by making sure critical systems are not connected to shared infrastructures. This is as true for connections to the Internet as much as it is for connections to the networks of other organisations.

In practice, the economic benefits of using the public telecommunications infrastructure and the Internet have led to the displacement of many private networks. As a result, today many critical infrastructures, including those of the military, emergency services and others, rely heavily on the public infrastructure and the Internet for their communications needs. This increases their vulnerability to attack.

Other vulnerabilities to data, systems and networks also exist. Specifically, these include software, configuration management and operating practices.

SOFTWARE

All software has vulnerabilities, which are unknown until somebody discovers them. There are many reasons for the existence of vulnerabilities:

- Software development remains more of a craft than an engineering discipline.
- Software is designed to perform clearly defined functions. It is rarely (if ever) designed to ensure that functions not part of the original definition *cannot* be performed.
- Software is hard to read, document and test. The effort put into testing is usually limited, so that timescales and budgetary targets can be met.

Attackers will exploit software vulnerabilities to make the software perform functions that were never intended by the designers.

Commercially available software, such as operating systems (Windows, UNIX and Linux) and applications from all vendors, contains programming errors and vulnerabilities. The terms and conditions of software licences absolve vendors from any liabilities for such errors and vulnerabilities.

Hackers systematically look for such vulnerabilities in the most popular software, in particular when it is Windows-based.

Specialised software and custom built software receive less attention from the general hacker population. This is not the good news it at first appears to be, as such systems offer much greater paybacks for cyber-crime and cyber-terrorism and may receive the unwelcome attention of more “professional” hackers. It is one thing to circulate a virus or worm via e-mail and quite another to mount a successful attack on a global funds transfer system.

A missing practice in most organisations that have a strong dependency on information systems is that of requiring Chief Information Officers to certify that the systems they buy, design, implement and operate are secure. If applied, this practice becomes the equivalent of requiring the Chief Finance Officer to sign a set of accounts and have them independently audited. Security audits, unlike financial audits, are rarely mandated.

CONFIGURATION MANAGEMENT AND OPERATING PRACTICES

The best software in the world will only be as secure as its installation and configuration. A software firewall that is installed but left with all of its features “turned off” is not going to be of much use. Experience shows that most security failures occur as a result of simple omissions and/or a few individuals failing to perform their duties.

Good practice

Server login: Mfw33

Server password: 7aqTV26

Bad practice

Server login: Ed

Server password: Gelbstein

Ugly practice

Server login: Sys_Admin

Server password: Sys_Admin

UNKNOWNNS

QUESTIONS FOR WHICH WE DON'T CURRENTLY HAVE GOOD ANSWERS

Academics, philosophers, lawyers and others are all considering possible scenarios related to cyber-terrorism and cyberwar. Given that there has been no public crisis related to these topics, progress in this area has been much slower than the development of technology.

The first set of questions that arises is that of definitions and actions, such as:

- What constitutes an act of aggression in cyberspace?
- What constitutes the use of force in cyberspace?
- What constitutes a breach of the peace in cyberspace? (Article 39 of the UN Charter)
- Is there such a thing as a virtual battlefield?
- How do you tell who the attacker is (a country, a hacktivist, or a script kiddie)?
- How do we measure the range and power of cyber-weapons?
- How do we count cyber-weapons, given that unlike conventional, biological, nuclear and chemical weapons they can be developed, produced and stored “invisibly”?
- How do you tell the nature (tool or weapon) of a piece of software before it has been tested or used?
- What constitutes acceptable defensive action? – Is pre-emptive action a suitable choice?

- How do you retaliate if a cyber-attack is launched from a less developed country (LDC)?
- What constitutes victory?
- What will be the impact of cyberwar on military doctrine?
- How do we increase awareness and remove obstacles to good security, particularly concerning critical infrastructures?
- How do we deal effectively with “external” components: purchased software, vendors, outsourcers, partner organisations, end-user computing?

While these are relatively simple questions it would appear that there are no simple answers.

WHAT CAN BE DONE ABOUT THESE THREATS?

Humanity has a long history of dealing with crime and war and defence requires actions in four categories: Deterrence, Prevention, Detection and Reaction. In the particular case of cyberspace, these can be interpreted as follows:

Deterrence: One form of deterrence leads to escalation. This deterrent is based on the following idea: “Our technology is superior to yours and we will retaliate if you start any funny business”. However, it would seem that governments are currently undecided about whether or not to pursue this path.

The other form of deterrence is that of international legislation (discussed in Section 8). At present such legislation is limited to the Council of Europe’s Convention on Cybercrime, signed by 32 countries in November 2001 and awaiting ratification by the requisite number of countries for it to enter into force.

Politicians and parliaments have not given much attention to the option of sanctioning retaliatory attacks against hackers. However, such a step would not be as easy as it sounds, because hackers find it easy to hide in cyberspace and to carry out their attacks by making use of the computers and networks of innocent parties without their knowledge or consent.

Is the concept of Mutually Assured Disruption applicable, where cyber-attacks between combatants continuously escalate to the breaking point? What happens if the principle of proportionality does not apply

because one of the combatants is a society with a low degree of computer and network use?

Prevention: Prevention makes use of the collected knowledge, experience and best practices dealing with computer systems and networks in order to establish the best level of security. Computer security measures are the equivalent of secure locks and alarms for protecting a house.

Such measures should include improved software and hardware design (the responsibility of vendors), the adoption of security standards and practices as well as the use of digital signatures, encryption and other tools capable of creating obstacles for potential attackers.

It should never be forgotten that all of these tools are also available to the hacker community and that it specialises in looking for vulnerabilities in them.

Public/private sector cooperation as well as international cooperation are seen as being essential for further development in these areas. One such initiative in the US is called InfraGard (<http://www.infragard.net>).

Detection: Response to a security incident usually starts after the detection of an attempted intrusion, security breach or some kind of malicious code. While a pre-emptive self-defence attack on a potential attacker cannot be excluded, hackers rarely signal which targets they are intending to strike and when, or their forthcoming release of a new virus...

The detection of external events relies on systems designed to operate as Intrusion Detection facilities and also on alerts from vendors and specialised facilities such as the Computer Emergency Response Teams that now exist in many countries.

The detection of a potentially improper action by an insider requires a different approach: several products on the marketplace can monitor information systems and network activity within a company and analyse its patterns to identify potential breaches in security. These are complex (and expensive) to install and manage and their effective implementation may require a study of the specific ethical issues within an organisation, as well as its personnel rules and policies towards disciplinary action.

Reaction: The first duty of the individuals responsible for the security of information systems and networks is to contain and then resolve any security problem and to take steps to strengthen the defences to prevent the repetition of such an attack.

The second issue concerning reaction is that of what constitutes an appropriate response. This is a matter for each organisation to consider.

PRACTICAL MEASURES

Two other booklets in this series explore information security issues: *Good Hygiene for Data and Personal Computers* and *Information Security and Organisations*. Some material from these booklets is included here for the readers' convenience. The key points advocated by the authors in these booklets are:

Preparing for information insecurity and cyberwar before it ever happens

We all know the adage "Better safe than sorry." We apply this concept in our homes as a matter of course, because in most societies it is not practical to live in a house without the means to protect our personal security and property.

Every situation is different and depends on the value of the items we wish to protect as well as the level of threat against which we seek such protection. In the end, we all ensure that at a minimum our property has good enough locks and, depending on who and where we are, burglar alarms, secure fences, guard dogs and other additional levels of protection.

Even then, we know from experience that 100 percent security can never be achieved – a good professional thief will be able to defeat the best "secure" locks or safes. In addition, every measure of security we implement will afterwards constitute an obstacle for us to deal with: extra locks on the door, a burglar alarm that needs to be reset within 30 seconds, a leaping excited guard dog to calm down, and so on, and so on.

The principles of protecting information systems and networks are no different. They involve the correct installation and maintenance of appropriate technologies and the setting up of processes and policies that

will ensure these technologies are used correctly, and at the same time are not so cumbersome that they become obstacles to the employees' work.



A very good practical guide to information security can be found in the International Standard ISO 17799 (Code of Practice for the Management of Information Security). Although it does have its critics and indeed may not be perfect, it is still a good guide to minimum requirements. These are discussed in the booklet *Information Security and Organisations* in this series.

Other standards do exist, for example the SAS 70 (<http://www.sas70.com>), the Statement on Auditing Standards Number 70, developed by the American Institute of Certified Public Accountants (AICPA), and the NIST's 800-37, put forward by the Computer Security Resource Centre of the US National Institute for Standards and Technology (<http://csrc.nist.gov>).

All these standards emphasise that information security is not only a technical problem but also a managerial one. The features which are common include the need for clear definitions of security needs and the formulation and promulgation of security policies.

A number of essential components are involved; each one is relatively simple and essentially non-technical:

Access controls: These can be either logical or physical and apply to both computer systems and networks. Such access controls should be conceived from the inside out: the highest level of protection should always be built into the most critical systems and networks.

Technology products, for example firewalls, are in widespread use and considered essential. However, unless properly installed and configured, they may simply offer a false sense of security. Ample evidence suggests that improper firewall configurations are not all that uncommon. Firewalls are protective measures for external threats whereas many attacks originate from within the firewall perimeter.

Access controls must be put in place without exception. However, in practice, exceptions are frequently made. Expert social engineers, who seem credible, are well-mannered and good negotiators, are then able to take advantage of such exceptions to carry out successful attacks.

Contingency plans: Well developed, documented and tested plans for use by Emergency Response Teams, disaster recovery, business conti-

nuity and crisis management are essential elements for surviving a cyber-attack. In the case of truly critical environments, a backup of the contingency plan may be necessary to further improve the chances for success should the initial plan fail for any reason.



Emergency contingency plans do occasionally fail. A certain bank (that must remain anonymous) needed to move its activities to its recovery site because of a gas leak outside their building. Upon arriving at this site, the employees discovered that the computer systems were undergoing maintenance (something that should only happen at the quietest possible time, for example on a Saturday at 2 am). The bank's trading room was unable to operate for a whole day. Soon afterwards, the manager responsible for this gaffe was told to pursue his career elsewhere.

Tests, audits and security certification: It is always a good practice to have an independent assessment of your security arrangements. This could take the form of unannounced but tightly controlled penetration tests where ethical hackers are employed to try to gain access to certain predetermined files on an organisation's networks or to conduct a password breaking exercise.

Tests, formal security audits by specialists and certification of security arrangements by independent certifying authorities are all good practices, but require considerable effort and expense to carry out.

Awareness: There is no substitute for all employees with access to networked systems having a good understanding of information security issues, in particular if they are mobile workers and access networks and systems from outside an organisation's security perimeter. Formal briefings, published policies and compliance practices are minimum security requirements. More elaborate measures are required for any critical computer application or installation. These measures include:

- providing appropriate resources for information security (staff, budgets and technologies);
- staffing for success – finding, training and retaining talented, intelligent, hard working and trustworthy individuals. It is easier to recommend this than to actually do it;
- encrypting critical systems – this is a self-evident measure that requires the careful management of encryption keys and distri-

bution of decryption rights. This in turn is best supported by appropriate vetting and clearance procedures for all employees who have been granted access rights and subsequent monitoring of the use (and misuse) of such rights;

- making available tools for monitoring and managing large networks (yes, they are expensive);
- resolving such legal issues as the right to monitor the activities of employees who have access to critical systems, networks and data.

THE SPECIAL CHALLENGES FACING CRITICAL INFRASTRUCTURES

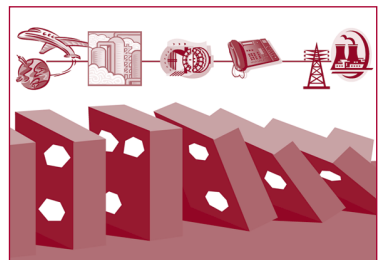
Critical infrastructures are potential prime targets for cyber-terrorists and cyber-warriors. Such infrastructures fall into three categories at the national level:

- public administration (government departments, nationalised industries);
- intelligence, defence, police and emergency services;
- private sector companies.

While in the past many of these institutions relied entirely on private networks, economic pressures have forced them to migrate many of these networks to the public infrastructure and the Internet in particular.

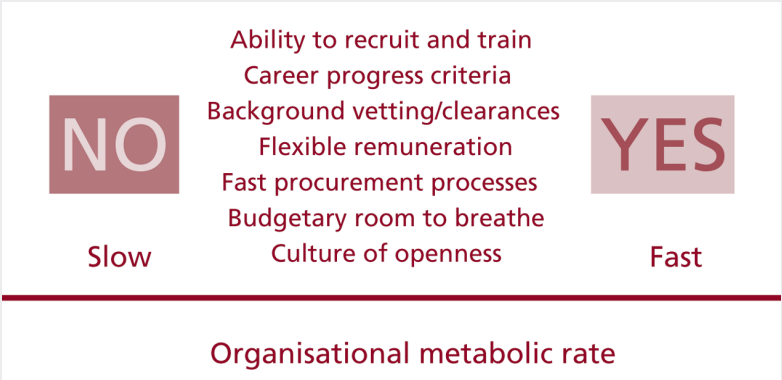
A potential consequence of this process is that a successful attack on one of these critical infrastructures could propagate to others, thus creating major disruption to any society where a high degree of computerisation and networking has been achieved.

A fourth category of critical infrastructures should also be noted, covering international organisations, which perform critical activities that could, if seriously interfered with, have serious consequences in the short term – examples include NATO, Interpol and Europol and other organisations such as the World Food Programme that need to operate in unstable and dangerous situations.



Many countries are fully aware of the potential consequences of such events. The recent blackouts in a large area of the North-eastern US and Canada on August 14, 2003 (which were not the result of hacking, but could have been), have reinforced the urgent need to address these problems.

Many critical infrastructures in public administration share a number of characteristics, regardless of where in the world they are located:



Organisations with slow metabolic rates already have built-in obstacles to good security. In such organisations, the best technical minds and their plans for protecting the organisation, are persistently undermined or paralysed.



SECTION



6

The law, open issues and some conclusions

Law is order, and good law is good order.

Aristotle

ADOPTION OF NEW INFORMATION SECURITY INSTRUMENTS

Organised crime, terrorists, and others will continue to use information systems and cyber-weapons just like they did previous weapons and technologies. This particular Pandora's Box has been opened and whatever is done, the problem will not go away. The very nature of the Internet circumvents traditional geography based on international borders. Organised crime and terrorists misuse and abuse the Internet's global nature. This is why the Internet requires global security arrangements. What has been the response of the international community to this point?

Generally speaking the question of international information security has been discussed in international organisations such as the OECD and the United Nations since the early 1980s. These discussions continue. For example, the United Nations General Assembly has passed several resolutions on a yearly basis on "Developments in the field of information and telecommunications in the context of international security", specifically resolutions 53/70 in 1998, 54/49 in 1999, 55/28 in 2000, 56/19 in 2001 and 57/239 in 2002. So far, regulatory dynamism has been sadly lacking.

The United Nations General Assembly has outlined elements for creating a global culture of cyber-security, inviting its member states and all relevant international organisations to take them into account in their preparations for the summit (A/RES/57/239).

Information security will be on the agenda of the World Summit on the Information Society in December 2003 and its planned follow-up in 2005.

Most of the above-mentioned initiatives are mainly political in nature without any real practical and legal implications. In this context the only exception and main breakthrough was the "Council of Europe Convention on Cybercrime", which has not yet been ratified by the requisite number of countries for it to enter into force. Once the conven-

tion enters into force it could have a universal impact. The convention is open for general accession by all countries.

Apart from this convention, no major legal instruments focusing on the international aspects of ICT security are in the works. In the absence of existing rules this legal vacuum will be filled by applying existing legal norms from appropriate sections of international law through the use of legal analogy.

APPLYING EXISTING INTERNATIONAL INSTRUMENTS TO CYBER-SECURITY

The closest analogies for the regulation of cyberwar can be found in the following international legal regimes:

- the *jus ad bellum* (the law of justification for the use of force);
- the *jus in bello* (the law of armed conflict);
- disarmament and arms limitation.

Jus ad bellum

The *jus ad bellum* is the law covering questions of self-defence, use of force, protection of international peace, etc. The main source of these rules is the UN Charter.

The following table presents a survey of a few key articles from the UN Charter and how they might be applied to the field of cyber-security.

UN CHARTER	CYBER-SECURITY ISSUES
<p>Article 4:</p> <p>.....</p> <p>All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations.</p> <p>.....</p>	<p>What exactly constitutes force or the use of force? Does the article refer only to "armed" force, or might the use of force via the Internet be considered under this article?</p>
<p>Article 39: The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.</p>	<p>Can a cyber-attack on a critical infrastructure or computer system be considered a threat to the peace, breach of the peace or act of aggression? What are the criteria for determining these categories? The answers to these and other questions will be decided by diplomatic interpretation.</p>
<p>Article 41: The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.</p>	<p>This article could be applied to Internet communication as it stands. In two recent conflicts (Kosovo and Iraq) this provision was not used to cut Internet communication.</p>
<p>Article 51: Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.</p>	<p>What constitutes an armed attack? A cyber-attack does not involve physical force, but can nonetheless lead to potentially serious damage, which could surpass the consequences of a military attack. For example, a cyber-attack on critical infrastructures (such as power plants, health centres, air control installations, etc.) could result in loss of life, chaos and panic, and with a domino effect, could lead to a very serious threat to national security. Some authors have argued that classification of the term "armed attack" should focus more on the severity of the consequences of the attack than on how it was performed. This is a very controversial issue since a vague interpretation of the term "armed attack" could permit the use of Article 51 far beyond its intended scope.</p>

Neutrality is another area of international law which could be of relevance where cyberwar and cyber-attacks are involved. Would the use of the territory or facilities of a neutral country for a cyber-attack constitute a breach of that country's neutrality status? The closest analogy in this case is the obligation of neutral countries to control radio broadcasting within their territorial waters in case of conflict. This obligation was enforced during the two world wars. Could this example of radio communication be used as an analogy for the Internet?

Jus in bello

The *jus in bello* consists of two legal branches. The first is the "Law of Geneva", which regulates protection of the victims of war including wounded, prisoners of war and civilians. It consists of four conventions (1949) and two protocols (1977). The second is the "Law of the Hague", which regulates the conduct of armed conflicts including a list of which methods and weapons are allowed to be used in armed conflicts. The "Law of the Hague" consists of a set of international legal instruments adopted in 1899 and 1907.

Article 36 of the Geneva Protocol I regulates the use of new weapons:

In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.

This is a general rule that could potentially regulate the use of cyber-weapons through the consequences they can create.

Article 54 (paragraph 2) of the Geneva Protocol I can be potentially applied with respect to cyberwar through the safeguarding of critical infrastructure:

It is prohibited to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population, such as foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works, for the specific purpose of denying them for their sustenance value to the civilian pop-

ulation or to the adverse Party, whatever the motive, whether in order to starve out civilians, to cause them to move away, or for any other motive.

Disarmament and arms limitation

The third area of international law with potential relevance for cyber-warfare deals with disarmament and arms limitation. Disarmament and arms limitation are very developed issues with a number of institutions (e.g. Conference on Disarmament) and legal instruments dealing with nuclear weapons, biological and chemical weapons, etc. Once a clearer situation of the various cyber-weapons emerges it is very likely that some arms limitation procedures will be applied.

LEGAL CHALLENGES – INTERNATIONAL REGULATION OF CYBER-SECURITY ISSUES

Even this short survey of the potential applicability of existing laws to the question of cyber-warfare shows the level of complexity of this subject. Here is a list of the major challenges which future regulators will have to face:

Internet regulatory paradox. Regulation of the Internet as a concept encompasses a fundamental paradox. Laurence Greenber outlined it as follows: “The very openness that contributes to the ubiquity, utility and power of networked systems may make those systems vulnerable to intrusions or other attacks that seek to ruin, manipulate, or steal the data that travels through them, or cause damage to other systems that depend on them or that they control.”

Slow speed of adopting international legal documents. The Council of Europe Cybercrime convention was in preparation for almost 20 years. It is simply not possible for those creating regulations to follow technological developments over time spans such as these. Experience from international law shows that in cases of dynamic regulatory fields, regulation should be kept on the level of general principles without going into details that may become obsolete before the new regulation enters into force. The complex and slow decision-making process of the international community means that it reacts in a more reactive (crisis-driven) way than a proactive one (anticipating potential problems).

Internet security regulation must be universal in order to be functional. The principle of universality, one of the cornerstones of the UN system, has been gradually supplanted by increasing regionalism. For example, in the fields of human rights and environmental protection the trend is strongly towards using regional mechanisms (e.g. the Council of Europe Human Rights Regime). Universality is crucial for an Internet regime because conventions in this field can fulfil their purpose only if they reach acceptance by all states. An international cyber-security regime could also make use of the principle of universal jurisdiction, which specifies that any state has jurisdiction over foreigners in the case of serious crimes (*delicta juris gentium*) such as piracy, trafficking of women and children and slavery.



Possible Analogy – Principle of Universality

Law of the Sea Convention - Article 105.

On the high seas, or in any other place outside the jurisdiction of any State, every State may seize a pirate ship or aircraft, or a ship or aircraft taken by piracy and under the control of pirates, and arrest the persons and seize the property on board. The courts of the State which carried out the seizure may decide upon the penalties to be imposed, and may also determine the action to be taken with regard to the ships, aircraft or property, subject to the rights of third parties acting in good faith.

High importance of “dual-use” facilities. Most potential targets of cyber-attacks could be of dual use, both military and civilian. How does one distinguish between these two potential uses?

Use of analogies for regulating cyber-security. The main laws which provide analogies for cyberspace regulation are the Law of the Sea and the Law of Outer Space.

State responsibility for activities under its jurisdiction. The Montevideo declaration from 1938 specifies territory, population and government as the three main attributes of the state. It also implies that states are responsible for activities in their territories. Traditional international law restricted responsibility to acts of states or their organs. After the Second World War the net of responsibility has been gradually extended.

The International Court of Justice in the *Corfu Channel* case specified that it was the obligation of every state “not to knowingly allow its terri-

tory to be used for acts contrary to the rights of other states.” The widest use of this principle has occurred in cases involving transboundary environmental damage. A few international environmental damage cases have assigned responsibility to a particular state for the damage it caused across its borders.

Can states be held accountable for cybercrime cases on their territories? The first problem is how to “anchor” cyberspace to traditional geography. Once a clear geographic link is made between cyberspace activities and geographic location, legal regulation will be much simpler.

An increasing number of tools are capable of geographically identifying Internet activities. In the Yahoo! case, Yahoo! argued that with modern tools it could clearly identify the geographic origin of 90 percent of the users accessing its website. The other element for establishing state responsibility is the keyword “knowingly”. What is the likelihood of a state knowing what is happening in its area of cyberspace? Very slight!

CONCLUSIONS

Despite the risks of a future digital battlefield, the benefits of cyberspace are too many to risk losing them. Therefore, we should continue to look at cyberspace as a structure that facilitates the free flow of information and capitalise on the benefits it brings to society including the promotion of development.

Cyberspace encourages freedom of speech, advances in civil society and facilitates doing business. Freedom of information needs to be protected and promoted and we should avoid the trap of restrictions and censorship - the denial of a free choice of information to citizens - in the name of security. The main task of containing this threat is the need to build confidence and trust in cyberspace.

This implies that there are a number of dilemmas to address.

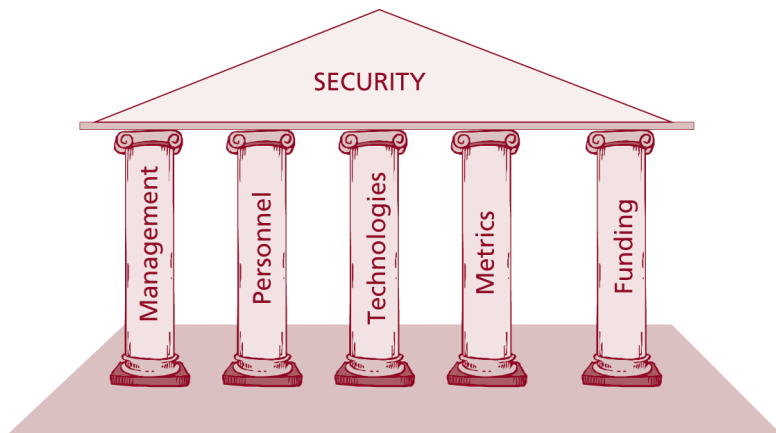
The first one is economic. A hacker can cause considerable disruption and economic loss at little cost and risk. The defender faces an unknown, invisible opponent who has more freedom for action.

The seriousness of the consequences of a professionally orchestrated cyber-attack requires that executives and governments commit to adopting the concept of a “Better safe than sorry” policy.

However, this does not imply that the security of computers and networks should be abdicated to technical individuals. Such individuals have a major responsibility in ensuring that security measures are properly implemented, but they cannot do it without adequate executive support on priorities and policies.

Achieving effective security is a way of life that requires five management pillars to support it:

- Management must create and support an environment where good security policies are created, disseminated and monitored for compliance.
- Management should make sure that such security activities are properly resourced: the right individuals in the right place, provided with the right conditions and the appropriate funding.
- Ensuring a better level of security is hard to justify in the conventional terms of return on investment. This is just as true for water sprinklers, fire extinguishers and other measures that protect individuals and buildings. In the last decades such measures have become legal requirements in many countries, but so far this has not been the case for the components of information security.



- Metrics are particularly important – the only way to know how secure information assets are is to monitor for both internal and external patterns of misuse or abuse. It is also particularly important to have security arrangements regularly tested by trustworthy people acting as hackers to avoid living with a false sense of security.
- Despite the need for confidentiality about security incidents, a strong case can be made for greater cooperation and exchange of intelligence and experiences with others facing the same problem. This is undoubtedly better than a do-it-yourself approach.

REFERENCES

- Adams, James. *The Next World War: Computers Are the Weapons and the Front Line Is Everywhere*, Simon & Schuster, March 2001.
- Center for Strategic and International Studies (CSIS). *Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo*, November 1998.
- Denning, Dorothy E. *Information Warfare and Security*, Addison Wesley, 1999.
- Denning, Dorothy E. *Obstacles and Options for Cyber Arms Controls*, Georgetown University, June 2001.
- Forno, Richard, Ronald Baklarz. *The Art of Information Warfare: Insight into the Knowledge Warrior*, 1999, electronic book, <http://upublish.com>.
- Gelbstein, E. and A. Kamal. *Information Insecurity*, published by the UN ICT Task Force and the UN Institute for Training and Research, September 2002.
- Government of Canada – Office of Critical Infrastructure Protection and Emergency Preparedness. *Threats to Canada's Critical Infrastructure*, http://www.ocipe.gc.ca/opsprods/other/ta03-001_e.asp.
- Greenber, Laurence. "Danger.com: National Security in a Wired World," in *Economic Strategy and National Security: A Next Generation Approach*, ed. Patrick J. De Souza. New York: Council on Foreign Relations, 2000.
- Report of the Defense Science Board Task Force on Information Warfare*, November 1996.
- Schneider, Fred B. (editor). *Trust in Cyberspace*, Committee on Information Systems Trustworthiness, National Research Council (USA), 1999. Available online at <http://books.nap.edu/books/0309065585/html/index.html>
- Sharp, Walter Gary. *Cyberspace and the Use of Force*, Aegis Research Corp., 1999.
- United Nations: Law, Policies and Practice*. Dodrecht: Martin Nijhoff Publishers, 1995.
- US Department of Defense, Office of General Counsel. *An Assessment of International Legal Issues in Information Operations*, May 1999.
- Waters, Gregory J. *Human Rights in an Information Age: A Philosophical Analysis*, University of Toronto Press, 2001.
- Weisenburger, Kirsten. "Hacktivists of the world, divide", April 23, 2001, <http://www.SecurityWatch.com>.
- Wingfield, Thomas C. *The Law of Information Conflict: National Security Law in Cyberspace*, Aegis Research Corp., August 2000.

ON THE WEB

- <http://www.iwar.org.uk/hackers/resources/the-hackivist/issue-1/vol1.html>
- <http://www.terrorism.com> (Website of the Terrorism Research Centre)
- <http://212.111.49.124> (The Information Warfare Site)
- <http://www.fas.org/irp/wwwinfo.htm>

Many other websites dealing with these topics are available.

Glossary of Information Warfare Terminology: <http://www.psycom.net/iwar.2.html>

ABOUT THE AUTHORS

Stefano Baldi

Stefano Baldi is a career diplomat in the Italian Ministry of Foreign Affairs, Counsellor at the Permanent Mission of Italy to the UN – New York. He has also served at the Permanent Mission of Italy to the International Organisations in Geneva, where he has developed several initiatives for the use of information technologies (IT) in the diplomatic community.

Baldi has an academic background in demography and international social issues. He also lectures on the use of internet for ministries of foreign affairs and missions at DiploFoundation's Postgraduate Diploma Course on Information Technology and Diplomacy. Baldi's most recent research focuses on the impact and future developments of information technology in international affairs.

<http://baldi.diplomacy.edu>

baldi@diplomacy.edu

Ed Gelbstein

Eduardo Gelbstein is a Senior Special Fellow of the United Nations Institute for Training and Research (UNITAR) and a contributor to the United Nations Information and Telecommunications (ICT) Task Force and to the preparatory work for the World Summit on the Information Society. He is the former Director of the United Nations International Computing Centre.

In addition to his collaboration with the United Nations, he is a conference speaker and university lecturer reflecting his 40 years experience in the management of information technologies.

He has worked in Argentina, the Netherlands, the UK, Australia and after joining the United Nations in 1993, in Geneva (Switzerland) and New York (USA). He graduated as an electronics engineer from the University of Buenos Aires, Argentina in 1963 and holds a Master's degree from the Netherlands and a PhD from the UK.

gelbstein@diplomacy.edu

Jovan Kurbalija

Jovan Kurbalija is the founding director of DiploFoundation. He is a former diplomat with a professional and academic background in international law, diplomacy and information technology. Since the late 1980s he has been involved in research on ICT and law. In 1992 he was in charge of establishing the first Unit for IT and Diplomacy at the Mediterranean Academy of Diplomatic Studies in Malta. After more than ten years of successful work in the field of training, research and publishing, in 2003 the Unit evolved into DiploFoundation.

Jovan Kurbalija directs online learning courses on ICT and diplomacy and lectures in academic and training institutions in Switzerland, the United States, Austria, the United Kingdom, the Netherlands, and Malta.

The main areas of his research are: diplomacy and development of the international regime on the Internet, the use of hypertext in diplomacy, online negotiations, and diplomatic law.

jovank@diplomacy.edu