JOINT SERVICES COMMAND AND STAFF COLLEGE

DEFENCE RESEARCH PAPER

By

Maj B DE SAN NICOLAS FAF

ADVANCED COMMAND AND STAFF COURSE

NUMBER 12
SEPT 08 - JUL 09

Page Intentionally Blank

DEFENCE RESEARCH PAPER (DRP)
SUBMISSION COVER SHEET

Student Name:	**Maj DE SAN NICOLAS**
DRP Title:	**Cyberspace as an environment for Military operations - What are the opportunities to exploit it and how states organise to exploit it?**
Syndicate:	**A7**
Syndicate DS:	**Wg Cdr Toft**
DSD Supervisor:	**Dr Marc Hilborne**
FE submitted towards psc(j) and the KCL MA in Defence Studies (delete if not applicable)	**PSC(J)** **KCL MA**
MOD Sponsored Topic?	**No**
Word Count (If applicable)	**14999**

Signature: Date:

DS/DSD Comments

Seen by:	Date:	Comment/Action:

Page Intentionally Blank

Abstract

The main objective of this paper is to give to the reader some clues in order to understand Cyberspace. Cyberspace is shaped by several components. The analysis of these components and the recent history show that Cyberspace is an environment for operations. By studying the different components of Cyberspace, this paper demonstrates that there are opportunities to exploit it. An organisation is needed in order to use Cyberspace as an environment for operations and this paper proposes some ideas in order to manage cyberspace. During this paper, it is suggested that Cyberspace is an environment as land, maritime, air and space where the principles of warfare can be applied and a general understanding of this environment is needed.

Page Intentionally Blank

Cyberspace as an environment for Military operations - What are the opportunities to exploit it and how states organise to exploit it?

INTRODUCTION

Cyberspace is the "place" where a telephone conversation appears to occur. Not inside your actual phone, the plastic device on your desk. Not inside the other person's phone, in some other city. The place between the phones. ...in the past twenty years, this electrical "space," which was once thin and dark and one-dimensional—little more than a narrow speaking-tube, stretching from phone to phone—has flung itself open like a gigantic jack-in the- box. Light has flooded upon it, the eerie light of the glowing computer screen. This dark electric netherworld has become a vast flowering electronic landscape. Since the 1960s, the world of the telephone has cross-bred itself with computers and television, and though there is still no substance to cyberspace, nothing you can handle, it has a strange kind of physicality now. It makes good sense today to talk of cyberspace as a place all its own.

– Bruce Sterling, Introduction to The Hacker Crackdown[1]

In 0.26 seconds there are at least 12,500,000 websites which contain the word “Cyberspace” on the Internet. Today, Cyberspace is a Geek word and 1,596,270,108 people use the Internet and potentially Cyberspace. Year on year, Cyberspace has become a place where 1,596,270,108 people “live”. They can speak to each other, they can buy goods, they can learn, they can teach, as all free citizens of Cyberspace. Users, hackers, criminals and Nations use Cyberspace. As in the real world, the diversity of behaviour creates the difference. And as with all societies, there could be conflicts between people. One type of conflict could be war. Although, with little surprise, people can read: “U.S. Air Force Prepares for War in Cyberspace”[2]. Firstly, this sentence means that the US Air Force considers Cyberspace as an environment for military operations. Secondly, it supposes there are some opportunities to exploit it because for waging a war in an environment, opportunities are needed. Thirdly, considering that the US Air Force is a military component of the United States of America, it means that this nation is organised in order to exploit Cyberspace. Firstly, by analysing different materials and using personal thoughts, this paper will demonstrate that Cyberspace is effectively an environment for military operations. Secondly, the definition of Cyberspace as an environment for military operations allows the establishment of opportunities in

[1] Bruce Sterling, “The Hacker Crackdown,” Massachusetts Institute of Technology, http://www.mit.edu/hacker/hacker.html (accessed May 29, 2009).
[2] “U.S. Air Force Prepares for War in Cyberspace,” ABCnews, http://blogs.abcnews.com/theblotter/2007/07/us-air-force-pr.html (accessed May 29, 2009).

order to exploit it. Thirdly, this paper will demonstrate as to how states should organise themselves in order to exploit this fifth environment.

CYBERSPACE AS AN ENVIRONMENT FOR MILITARY OPERATIONS

The first part of this paper will demonstrate that Cyberspace is an environment for military operations. Firstly it will determine what is an environment for operations. Secondly, it will define what is Cyberspace. Thirdly, it will show how Cyberspace is used today. Fourthly, some cases will be studied in order to conclude that Cyberspace is an environment for operations and that it is used for this purpose.

What is an environment for operations?

Firstly, an environment for operations should be defined. According to Joint Doctrine Publication 0-01.1 an environment is: "The surroundings in which an organization operates, including air, water, land, natural resources, flora, fauna, humans, and their interrelation."[3]
An operation is: "A military action or the carrying out of a strategic, tactical, service, training, or administrative military mission; the process of carrying on combat, including movement, supply, attack, defence and manoeuvres needed to gain the objectives of any battle or campaign."[4]
Then, an environment for operations is the mixture of both definitions. It is an area:

- Where an organisation can perform a military action or carry out of a strategic, tactical, service, training or administrative military mission;
- Where an organisation can carry on combat including movement supply, attack, defence and manoeuvres needed to gain the objectives of any battle or campaign.

This definition will help to determine if Cyberspace could be considered as an environment for operations. Before making this connection, Cyberspace should be defined.

What is Cyberspace?

From the ether to reality

Indeed, Cyberspace is often used in literature, but not always well defined. This section will define Cyberspace. It is a travel from virtuality to reality.

[3] United Kingdom. Development, concepts and doctrine. *United Kingdom glossary of Joint and Multinational Terms and definitions*. Joint Doctrine Publications 0-01.1. 7th ed. (Shrivenham: DCDC, 2006), E-6.
[4] United Kingdom. Development, concepts and doctrine. *United Kingdom glossary of Joint and Multinational Terms and definitions*. Joint Doctrine Publications 0-01.1. 7th ed. (Shrivenham: DCDC, 2006), O-3.

Cyberspace was used for the first time in 1984 in a novel – Neuromancer - written by William Gibson. The story is about a computer hacker who tries to struggle in Cyberspace: "The matrix has its roots in primitive arcade games, said the voice-cover, 'in early graphics programs and military experimentation with cranial jacks.' On the Sony, a two-dimensional space war faded behind a forest of mathematically generated ferns, demonstrating the spatial possibilities of logarithmic spirals; cold blue military footage burned through, lab animals wired into test systems, helmets feeding into fire control circuits of tanks and war planes. 'Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts… A graphic representation of data abstracted from banks of every computer in the human system. An Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data.'"[5]

Twenty four years later, United States Air Force Cyber command defined Cyberspace thus: "Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."[6]

In fact Cyberspace is built with computers, communication systems, networks, satellites, infrastructure of communication, transport systems which use information, sound data, voice, text, pictures, systems which can be remote controlled and which control energy, digital clock, video camera, robots but also weapons, missiles, GPS, all technologies of communication – WIFI, laser, modem, satellites, local networks, cell phones, optical fibres, etc. This world of interconnection, of inter dependence, where information flies from one medium to another is treated, duplicated and stored. It constitutes the information sphere, the information environment, the cyberspace.[7] Then, it is obvious that people are surrounded by Cyberspace. Practically nothing can be done without Cyberspace. It means that the idea of Cyberspace moved from virtuality to reality.

Another definition from Oxford Dictionary is:

> "The notional environment within which electronic communications occurs, especially when represented as the inside of a computer system; space perceived as such by an observer but generated by a computer system and having no real existence; the space of virtual reality."[8]

And according to the US official joint definition Cyberspace is:

> "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet,

[5] William Gibson, *Neuromancer* (London: HarperCollins publishers, 1995), 67.
[6] United States. Air Force Cyberspace command, *Air Force Cyber command Strategic vision*. 2008.
[7] Daniel Ventre,*La guerre de l'information* (Paris: Lavoisier, 2007), 42.
[8] Oxford English Dictionary (Oxford, 2007),592.

telecommunications networks, computer systems, and embedded processors and controllers."[9]

According to Dr Dan Kuehl (Information Resources Management College/National Defence University):

"Cyberspace is an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interconnected information-communication technology (ICT) based systems and their associated infrastructures"[10]

The main problem of these definitions is that they define Cyberspace as a container with Information being the content. However, today Cyberspace is more than a simple container and the most interesting definition of Cyberspace is this one:

> *"Some call Cyberspace the fifth* domain*. But, unlike earth, sea, air and space, this term derives from Latin for* lord *or* master *and thus is inapt in describing a global, ungoverned, uncontrollable and fiercely contested commons. Cyberspace is better understood by examining its three components:*
>
> • *The physical component describes* means*. It encompasses the hardware, software and connecting media (ether) employed to acquire, store, manipulate, exploit and exchange data, swiftly, reliably and securely. The metrics for evaluating performance in this component are described as* information assurance*.*
>
> • *The information component concerns* purpose*. Evaluation of performance in this component requires an appreciation of languages, history and cultures of both the originator and recipient of* messages*. The metric is a subjective determination of the extent to which the* purpose *of a message has been achieved.*
>
> • *The cognitive component deals with* results*. Since the message targets the human brain and its decision-making process (wetware) the metric is the* effect *the message has on behaviour, or the value of an exchange.*
>
> *Why should you care about cyberspace? Cyberspace connects you to anyone you desire, but also connects everyone to you, desired or not. Your personal, financial and national security depends on the ability of the cyberspace components to satisfy demanding expectations, especially when under natural or purposeful stresses. The physical component of cyberspace converts reality into digits by means and processes that permit data to be distorted in ways that can be unpredictable, unexpected, anonymous and undetectable. There are no agreed*

[9] United states of America, Department of defence, *Joint publication 1-02*, 17 October 2008, 141
[10] Dr Dan Kuehl, "From Cyberspace to Cyberpower: Defining the problem," US Army war college, http://www.carlisle.army.mil/DIME/documents/Cyber%20Chapter%20Kuehl%20Final.doc (accessed May 28,2009).

rules of conduct or meaningful sanctions for miscreants. Consequently, you can't always trust what you see, or read or even hear. [11]

It is very important to note that Cyberspace is constituted in three parts: a soft part e.g. information, knowledge, software; a hard part e.g. technical systems, energy, routers, etc. ; and the last one which is the way to "fly", or to "move" inside Cyberspace.
In order to define and to understand Cyberspace, however, the different components have to be defined.

The physical component of Cyberspace

The first part of Cyberspace is a physical part which should be analysed. In fact, it is mainly the Internet and the large amount of systems which are connected together through the Internet. It is difficult for somebody to identify exactly what the hard part of Cyberspace is. Initially, however, it should be explained briefly how Cyberspace was born.
In fact the beginning of Cyberspace was in the 1960s. It is a pure product of the Cold War. In order to retaliate from a massive nuclear attack from the Soviet Union, the US Department of Defence created the Advanced Research Project Agency (ARPA). This agency developed an experimental network in 1969 in the University of California called ARPANET. In 1971, Louis Pouzin, a French scientist, developed a network of 25 computers between France, United Kingdom and Italy.[12] He created the first world network by inventing the technology of packet switching. The ARPA team drew their inspiration from this technology in order to create a new protocol of communication: TCP/IP (Transmission Control Protocol/ Internet Protocol) still used today as the standard protocol. This network connected about twenty military centres, industries and universities. The strength of this network was the grid created by the connection between all the nodes - routers and after switches. The aim was to bring information flow from one location to another even though a node was destroyed. Year by year, ARPANET was used by more and more users and the web increased. Increasingly local networks were connected to each other all over the world. The word 'Internet' was born on the 1st of January 1983. In 1972, electronic mail was invented. At the beginning of the 1990s, the "web" – world wide web - was born. In fact it was the creation of a protocol – HTTP, Hyper Text Protocol – which allowed the publication of text on the Internet. All this protocol allows all computers to connect:

> "The explosive growth of the Internet initially conceived to be part of an American defence plan to improve communication during nuclear attack has transformed computer usage."[13]

This short history of the Internet shows that in order to implement the Internet, hardware is needed:

[11] Col. Alan Campen, USAF (Ret.), "What is cyberspace and why should you care?" CyberInfoware.com, http://www.cyberinfowar.com/ (accessed May 4, 2009).
[12] Nicolas Arpagian, La Cyberguerre, la guerre numerique a commence (Paris: Vuibert, 2009)
[13] William C. Martel, *The technological arsenal* (London: Smithsonian institution press,2001), 243.

- Computers, servers (computers with data storage, software dedicated to the network), backbone computers;
- Software (protocol, data storage, routing, etc.);
- Routers, switches;
- Links (satellites, radio, cables);
- Power;
- Air conditioning;
- Buildings.

All these components constitute the core technical infrastructure of the Internet.[14] This technical infrastructure allows connecting everything, machines and people: "Now, computers networks support everything from local, regional, and national banking systems to telephone and transportation structure. Information technology also includes fax machines, cellular phones, and satellite television. Although these technologies are important, the Information Age could be governed by the growing significance and presence of the networked computer."[15]

This technical approach of the Internet is strengthened by a study of nodes and links. It is possible also to have a geographical and economic approach. In fact, there are relationships between Internet networks and territorial developments. A study made by two researchers, Mr Puel and Mss Ullmann demonstrated clearly that this connection exists. They "highlight how technologies, actors' strategies and territorial realities are relevant components in the geography of Cyberspace"[16]

Their approach is:

- Where are the tubes?
- Where are the nodes?
- Where is the content (websites)?
- What are the dynamics of the network?
- Who are the masters of the network?

Although, Cyberspace is linked to a physical environment, it is made up of material and is settled in a physical world.

This world wide network allows people to be connected. Today, there are 1.6 billions users of the Internet.[17] According to some specialists Cyberspace could be the 6th continent. Today, in the age of Information, the Internet is the main support for sending, seeking and storing information. It is the main support for knowledge and information and in fact information is the second component of Cyberspace.

---

[14] Lech J Janczewski, Andrew Colarik, *Cyber warfare and Cyber terrorism* (London: Information Science Reference, 2007), 38.
[15] William C. Martel, *The technological arsenal* (London: Smithsonian institution press,200), 243.
[16] Gilles Puel, and Charlotte Ullmann,."Les noeuds et les liens du reseau internet : approche geographique, econonomique et technique." *L'Espace geographique*, no 2 (2006): 97-114.
[17] Internet world stats, http://www.internetworldstats.com/stats.htm (accessed May 07, 2009).

The information component of Cyberspace (the content)

The previous part demonstrates that Cyberspace has a physical component. So what? One may ask. What can be found inside the Cyberspace? How is Cyberspace used today all over the world? Let's come back to the real beginning of the Internet. Remember, the aim was to send vital information even in the case of a nuclear attack. After this step, the World, thanks to globalisation, developed the Internet in order to share more and more Information. All information systems were connected together in order to exchange information and thus Cyberspace was born.
A definition of the connection between Cyberspace and Information could be this one:

> "The nature of cyberspace as an information environment is complex and contradictory; anarchic self-expression is juxtaposed with commercial interests, information sharing communities with commercial content providers. It is a networked, virtual environment, which continues to confound attempts to regulate the international flow of information and cultural values that it facilitates. The complexity of this environment might be viewed as an exaggerated representation of the post-modern condition; fragmented, with multiple narratives and individual constructions of meaning. This fusion of cultural zeitgeist, technology and communication condenses into occasional human form. It can be seen, for example, in the bizarrely meaningless (or rather, meaningful) displays of "flash mobbing", where groups of strangers join together to give human substance to momentary online communications (Schmueli, 2003)."[18]

This definition is interesting, because it underlines the social aspect of Cyberspace. This aspect is less obvious than information or knowledge sharing. The technical component of Cyberspace allows interconnecting people, societies and states. It increases enormously the connection between people and their relationship with each other. Social networks and information societies were born thanks to Cyberspace. These social networks and information societies can live into the Cyberspace thanks to the following:

- Blogs - A blog (a contraction of the term weblog) is a type of website, usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video[19];
- Twitter[20]-like websites - Twitter is a free social networking and micro-blogging service that enables its users to send and read other users' updates known as tweets. Tweets are text-

[18] Jake Wallis. "Cyberspace, information literacy and the information society." Centre for Digital Library Research. http://cdlr.strath.ac.uk/pubs/wallisj/jw200501.htm (accessed May 21, 2009).
[19] "Blog," Wikipedia, http://en.wikipedia.org/wiki/Blog (accessed May 21, 2009).
[20] "Twitter," Twitter, http://twitter.com/ (accessed May 21, 2009).

based posts of up to 140 characters in length which are displayed on the user's profile page and delivered to other users who have subscribed to them (known as followers)[21]

- Facebook[22]-like websites - Facebook is a free-access social networking website that is operated and privately owned by Facebook, Inc.[1] Users can join networks organized by city, workplace, school, and region to connect and interact with other people. People can also add friends and send them messages, and update their personal profiles to notify friends about themselves. The website's name refers to the paper facebooks depicting members of a campus community that some US colleges and preparatory schools give to incoming students, faculty, and staff as a way to get to know other people on campus.[23]

These examples of technologies used inside Cyberspace demonstrate the birth of social networking that is the creation of Cyber societies. Thanks to connectivity people can stay at home and be connected to more people than they could ever meet in real life. One can readily imagine that these societies live as real societies and can be under the same threat by spread of false information, rumours, lobbying, etc.

The cognitive component of Cyberspace (The means or how to “fly”)

This third component will deal with the means that can affect both previous components. As was written before in this paper, Cyberspace is composed of three components. There are several ways to deal with the physical and the information components.
Firstly, it is possible to deal with the physical components by having a direct effect upon them. These effects can be applied on each layer of the physical components of Cyberspace (cables, routers, etc.). These actions can be done directly, or through software which can disable or destroy the different layers. The different ways and means of this type of effect is:

- Cyberwar: it is the war assisted by computers
- Net war: it is the same as Cyberwar, but via networks
- Hacking

Secondly, it is possible to deal with the information component of Cyberspace by manipulation, destruction and thefts. The different means for this type of effect are nearly the same as Information warfare, but are adapted to Cyberspace:

- Spin doctoring: act of propaganda.
- Intelligence:
    - HUMINT for human intelligence;
    - SIGINT for signal intelligence (interception of electronic waves)

[21] “Twitter,” Wikipedia, http://en.wikipedia.org/wiki/Twitter (accessed May 21,2009).
[22] “Facebook,” Facebook, http://www.facebook.com/ (accessed May 21, 2009).
[23] “Facebook,” Wikipedia, http://en.wikipedia.org/wiki/Facebook (accessed May 21, 2009).

- COMINT for Communications intelligence
- ELINT for Electronic intelligence
- IMINT for Image intelligence
- OSINT for Open source Intelligence
- TECHNINT for Technical intelligence

- Social engineering
  - Social engineering is the act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.[24]
  - About social engineering, reformed computer criminal and later, security consultant Kevin Mitnick popularized the term 'social engineering', pointing out that it is much easier to trick someone into giving a password for a system than to spend the effort to hack into the system. He claims it was the single most effective method in his arsenal.[25] [26]

Cyberwar - Cyberwarfare

When Cyberspace is evoked within a military environment the word Cyberwar appears. Cyberwar is directly linked to Cyberspace. What could be Cyberwar?
According to the shorter Oxford English Dictionary, “Cyberwar is the use of computers to disrupt the activities of an enemy country, especially the deliberate attacking of communication systems.”[27]
We could be simpler and write that Cyberwar is war in Cyberspace.
“Conflict itself is likely to take place in new environments: cyberspace, the high seas, near space, and increasingly, in expanding cities.”[28]
The study of the previous definitions states that cyberspace is shaped by three components. Firstly, there is a physical component which is constituted by software and hardware (from the simple cable up to the satellite via networks). Secondly, there is an Information component constituted by knowledge, information and communities which are born inside Cyberspace thanks to the physical component. Thirdly, there is a cognitive component which is the interaction between the both previous components. All these components define an environment in which wars could

[24] “Social engineering,” Wikipedia, http://en.wikipedia.org/wiki/Social_engineering_(security) (accessed May 27,2009).
[25] “Kevin Mitnick,” Wikipedia, http://en.wikipedia.org/wiki/Social_engineering_(security)#Kevin_Mitnick (accessed May 27, 2009).
[26] Mitnick, K: "CSEPS Course Workbook" (2004), 4, Mitnick Security Publishing
[27] Oxford English Dictionary (Oxford, 2007),592
[28] United Kingdom. Development, concepts and doctrine. *The DCDC Global Strategic Trends Programme 2007-2036.* (Shrivenham: DCDC, 2007), 70.

be waged. Some case studies will follow and demonstrate that it is possible to wage operations in Cyberspace.

Cases studies

Georgia

In the summer of 2008, tension increased between Russia and Georgia. The website of the President of the Republic of Georgia was attacked by hundreds of Zombies who were computer remote controlled. This type of attack stopped the website and nobody could access it. Some weeks after, on the 12th August 2008, several websites were attacked – main Medias, foreign affairs, parliament, Minister of Defence, National Bank of Georgia, TV Channel Rustavi2. Hackers replaced the photos of Georgian personalities with false photos for example the same person but in a Nazi uniform. These electronic assaults happened at the same time as the entry of Russian Tanks in Ossetia. Russia targeted the Georgian Air Command and control networks by Electronic warfare in order to immobilize the Georgian Air Force. The only solution for the Georgian government was to create websites outside Georgia in order to be able to communicate.[29]
Other websites which were linked to Georgia and Ossetia were attacked in Russia.
There is no evidence that it was planned by Russians. However it can be supposed that Russia used Cyberwarfare at the same time as they entered in Georgia. It can be assumed that Russian planned to attack Georgia after a Cyber attack. Therefore if a planning process was to be considered, the Cyber superiority – i.e. Air superiority – was to prove a decisive point in the plan of the Russians.

Estonia

Estonia is another story which shocked the world of Cyberspace specialists. In fact, this case is very interesting, because Estonia could be the future for all modern countries. Estonia is one of the most connected countries in the world[30]. Estonia is a country where the government decided to be fully integrated in Cyberspace. All the institutions of the country work into the Cyberspace, and maybe Estonians are the first cyber citizens. This extract from a newspaper summarizes what happened in Estonia in 2007:

> The Baltic state has suffered serious electronic disruption since it decided to relocate a controversial Soviet war memorial, a move that prompted Russia to threaten sanctions. The

[29] Nicolas Arpagian, *La Cyberguerre, la guerre numerique a commence (*Paris: Vuibert, 2009), 36.
[30] Adrian Blomfield, “Russia accused over Estonian 'cyber-terrorism',” The Telegraph, http://www.telegraph.co.uk/news/worldnews/1551850/Russia-accused-over-Estonian-cyber-terrorism.html (accessed May 14, 2009).

> presidential administration's website was inaccessible for six days late last month while those of most cabinet ministries suffered reduced connection speeds after they too were targeted. Jaak Aaviksoo, the Estonian defense minister, said about one million computers worldwide were used to cripple government and corporate sites, adding that his government had "identified in the initial attacks IP numbers [computer addresses] from the Russian governmental offices. "We clearly feel it as a threat to national security," he said. However, he cautioned that there was "not sufficient evidence" of a Russian governmental role, "but it indicates a possibility".[31]

In January 2008, an Estonian was arrested for having organized this attack. According to Security experts, and even government officials, there's little evidence much less proof to back up these charges. It seems more likely that a loose-knit group of individuals and different groups united by outrage inflamed by posts on Russian-language blogs and forums were behind the assault.[32]

How to manipulate the world press?[33] [34]

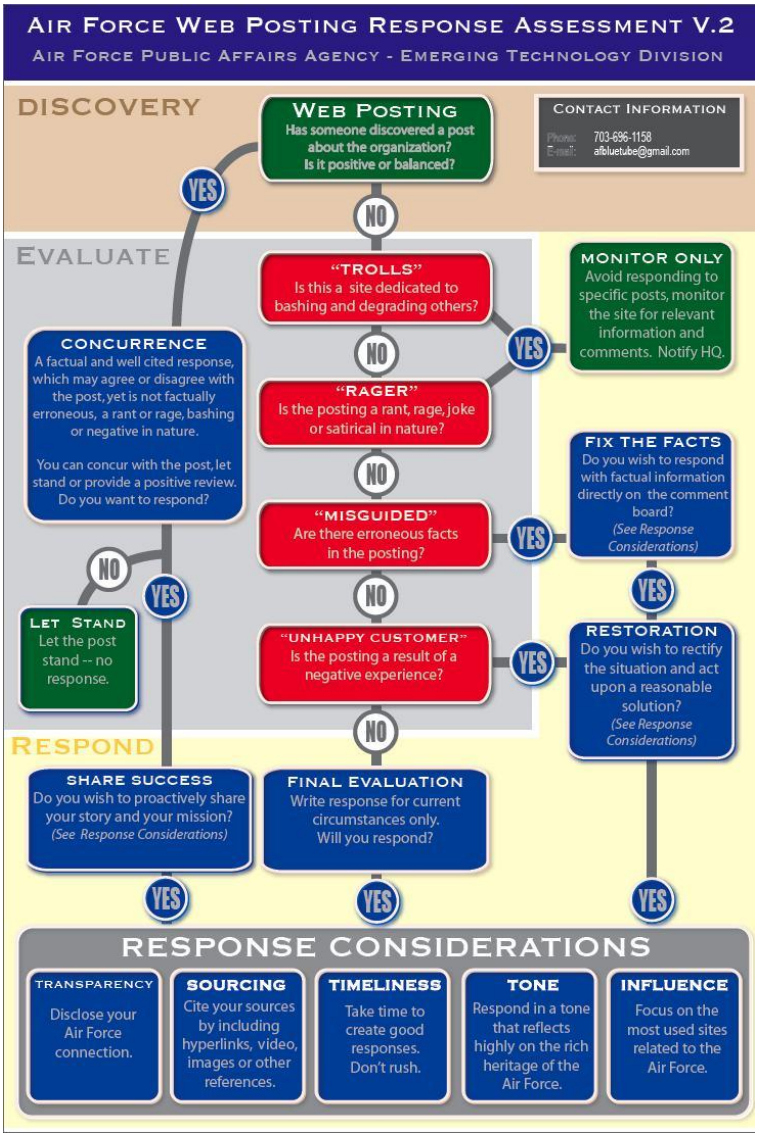
In April-May 2009, an Irish student posted on Wikipedia a false quotation – “One could say my life itself has been one long soundtrack. Music was my life, music brought me to life, and music is how I will be remembered long after I leave this life. When I die there will be a final waltz playing in my head and that only I can hear. When I was 15, I did not know nothing about what concerned the world of music”[35] - of Maurice Jarre, a famous conductor. Even the moderator of Wikipedia deleted it because there were no references, the student continued to write it on the website. This false quotation was written in more than ten newspapers which did not verify their sources. Today, this quotation can be found on the Internet[36].

[31] Adrian Blomfield, “Russia accused over Estonian 'cyber-terrorism',” The Telegraph, http://www.telegraph.co.uk/news/worldnews/1551850/Russia-accused-over-Estonian-cyber-terrorism.html (accessed May 14, 2009).
[32] John Leyden, “Estonia fines man for DDoS attacks,” The register, http://www.theregister.co.uk/2008/01/24/estonian_ddos_fine/ (accessed May 14, 2009).
[33] Genevieve Carbery, “Student's Wikipedia hoax quote used worldwide in newspaper obituaries,” IrishTime.com, http://www.irishtimes.com/newspaper/ireland/2009/0506/1224245992919.html (accessed May 21,2009).
[34] Guerric Poncet, “INTERNET - Un étudiant trompe la presse mondiale grâce à Wikipédia,” Lepoint.fr, http://www.lepoint.fr/actualites-technologie-internet/2009-05-07/un-etudiant-trompe-la-presse-mondiale-grace-a-wikipedia/1387/0/341294 (accessed May 21,2009).
[35] “Maurice Jarre,” Wikipedia, http://en.wikipedia.org/w/index.php?title=Maurice_Jarre&oldid=280558491 (accessed May 21, 2009).
[36] “Maurice Jarre, Doctor Jivago video,” Daily radar, http://movieblips.dailyradar.com/video/maurice_jarre_doctor_zhivago/ (accessed may 21, 2009).

How to manipulate blogs and then Cyber communities?

Cyber communities can be manipulated. Even people can express freely their opinion; they can represent a threat in the public domain. It is the reason why the US Air Force created a counter blogger directive:

"It's all part of an Air Force push to counter the people out there in the blogosphere who have negative opinions about the U.S. government and the Air Force,"[37] [38]



[37] Noah Shachtman, "Air Force Releases 'Counter-Blog' Marching Orders," The wired, http://www.wired.com/dangerroom/2009/01/usaf-blog-respo/ (accessed May 21, 2009).
[38] Steve Watson, "Air Force Creates "Counter Blog" Response Plan To Quell Online Dissent," Infowars.net. http://www.infowars.net/articles/january2009/090109bloggers.htm (Accessed may 21, 2009)

Critical attack and its planning process

The general way to attack in Cyberspace is described on *Security Gurus* website:
“Strike scenario
The cyber-attack requires detailed structure and a plan in order to achieve the expected objective. Such plan should have this structure:

1. General Target analysis
2. Choosing specific objectives
3. Selection of team members with sufficient qualification
4. Detailed target analysis
5. Attack planning
6. Training the attack
7. Execution of the attack
8. Observing the target to ensure the objectives were met

At first point analysts collect as much information about the target as possible by standard means (eg. Newspapers, web-sites; newsgroups;..). This information should help identify:

- Target's mission (what is the goal of system's existence)
- Content and structure of the target's systems (network structure; geographical location; external systems connected; customers ;..)
- Technologies used (systems used; software and hardware implemented; defensive measures)
- History of system implementation (system integration times; upgrade dates; vendors)
- Human resources (how many people are employed; how well trained are they; what kind of information they collect; what are their interests ;..)

All the information above should help to pick up the best (or the weakest) target and possible source of attack as well as time plan of action.
Second point should identify all the weakest spots or interesting spots that should be looked into more deeply. These targets do not have to be specific systems they also can be information sources or people.
In third point the team should be assembled containing specialists for every type of system used at the target. As it is not always possible to collect all the information necessary to choose the team all the starting members in the team should be able to call in any specialists they need for target analysis or strike.
Point four should gather all the necessary information about the target to create a specific plan of action to achieve the objectives specified in point two. This point identifies specific target structure

and validates the information collected at point one. This is done by scanning the target systems and identifying operation systems, network elements as well as services and daemons running on them.
At point five the above information is processed and specific weaknesses identified for possible break-in. It is not always possible to identify them up to the detail necessary, but with correlation of other information collected it may be possible to make the attack plan more specific. The plan can contain further testing and scanning as there may be other systems that are not identifiable from outside.
Training the attack at point six is a preparation for the attack that optimizes and tests the cyber-weapons as well as the plan for the attack on a group of similar systems.
This also helps to develop a certain level of automation that speeds up the attack and minimizes the probability of human intervention.
Attack plan is usually very simple:

- use a system vulnerability detected
- gain the authorization level required
- achieve the objectives
- remove all the clues (if the objective was other than destroy the target)

Verification of achieving the objectives is dependant on their contents, but can be proved by analyzing the information collected or checking the target's services that should have been disrupted or analyzing the local information sources (eg. Newspapers)."[39]

Finally, Cyberspace is an environment for operations.

By analysing definitions, the different components of Cyberspace and some activities inside it, the first part of this paper demonstrates that cyberspace is an environment for operations. To conclude this first part, below are given some evidences.
Firstly, the British Defence Doctrine defines the operating environment:

> "The operating environment, the surroundings or conditions within which military activity takes place, has a variety of dimensions: maritime, land, air, space, information (including cyberspace), electro-magnetic and time."[40]

Secondly the US Department of Defence considers Cyberspace as an environment for operations. Indeed, it defines Cyberspace Operations as follow: "The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such

[39] "Cyber Warfare," Security Gurus, http://www.security-gurus.de/papers/cyberwarfare.pdf (accessed May 25, 2009).
[40] United Kingdom, Ministry of Defence, British defence doctrine, JDP 0-01, 2-10.

operations include computer network operations and activities to operate and defend the Global Information Grid."[41]

As Cyberspace is defined as an environment for operations, these can be waged within. However there are some similarities with the other environments and the evocation of the notion of power and warfare:

> As Colin Gray wrote, "What Air Power meant for warfare in the last century, cyber power and space power will mean for the future. The purposes here are to ensure thet the new geographies of warfare, Cyberspace and outer space, are approached and understood correctly"[42]
>
> "Cyber power and space power will be layered on to, integrated with, land power, sea power, and air power. They may well transform the character of some warfare, but they will not revolutionize war itself into a zone where one could begin to talk about a possible alteration in war's nature."[43]

So, it can be researched to prove that there are opportunities to exploit Cyberspace.

WHAT ARE THE OPPORTUNITIES TO EXPLOIT CYBERSPACE?

Indeed there are opportunities to exploit Cyberspace. These could be determined by studying the threats which exist inside Cyberspace. Then, when the threats are determined, it will be possible to exploit cyberspace by using strategies we use in the other environments.

What are the threats?

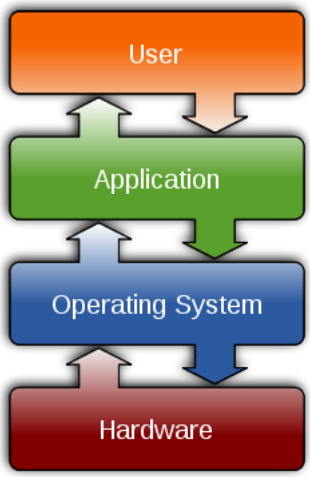
Studying all the threats in Cyberspace cannot be done in this paper. In order to understand the concept of the threats in Cyberspace it should be done by following the definition of Cyberspace given in the first part of this paper: the physical component, the information component and the cognitive component.

The physical approach (the place)

To understand the threats on Cyberspace the structure of a network should be understood. A network is composed of computers, cables, routers.

[41] United States of America, Department of Defence, Joint Publication 1-02, Department of defence dictionary of Military and associated terms, 17 october 2008, 141.
[42] Collin S. Gray, *Another bloody century (*London: Phoenix, 2006),156.
[43] Collin S Gray,*Another bloody century* (London: Phoenix, 2006), 157.

A computer is a machine that manipulates data according to a set of instructions.[44]
A router is a networking device whose software and hardware are usually tailored to the tasks of routing and forwarding information. For example, on the Internet, information is directed to various paths by routers.[45]
Inside the computer, and in order to use it, there is an Operating system. An "Operating system (commonly abbreviated to either OS or O/S) is an interface between hardware and user; it is responsible for the management and coordination of activities and the sharing of the limited resources of the computer. The operating system acts as a host for applications that are run on the machine. As a host, one of the purposes of an operating system is to handle the details of the operation of the hardware. This relieves application programs from having to manage these details and makes it easier to write applications. Almost all computers, including handheld computers, desktop computers, supercomputers, and even video game consoles, use an operating system of some type. Some of the oldest models may however use an embedded operating system that may be contained on a compact disk or other data storage device."[46]



"A Server is any combination of hardware or software designed to provide services to clients. When used alone, the term typically refers to a computer which may be running a server operating system, but is commonly used to refer to any software or dedicated hardware capable of providing services."[47]
Cables link computers and servers to routers and routers to routers. By using all these devices a network can be implemented. There are several types of networks:

[44] "Computer," Wikipedia, http://en.wikipedia.org/wiki/Computer (accessed May 15,2009).
[45] "Router," Wikipedia, http://en.wikipedia.org/wiki/Router (accessed May 15, 2009).
[46] "Operating system," Wikipedia, http://en.wikipedia.org/wiki/Operating_system (accessed May 15,2009).
[47] "Server," Wikipedia, http://en.wikipedia.org/wiki/Server_(computing) (accessed May 15, 2009).

- A personal area network (PAN) is a computer network used for communication among computer devices (including telephones and personal digital assistants) close to one's person.[48]
- A local area network (LAN) is a computer network covering a small physical area (Within 1 KM), like a home, office, or small group of buildings, such as a school, or an airport.[49]
- A campus area network (CAN) is a computer network that interconnects local area networks throughout a limited geographical area, such as a university campus, a corporate campus, or a military base.[50]
- A Metropolitan area networks (MAN) is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities. MANs can also depend on communications channels of moderate-to-high data rates.[51]
- Wide Area Network (WAN) is a computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries).[52]

All computers, servers, routers can "talk" together thanks to software and protocols. "In computing, a protocol is a convention or standard that controls or enables the connection, communication, and data transfer between computing endpoints. In its simplest form, a protocol can be defined as the rules governing the syntax, semantics, and synchronization of communication. Protocols may be implemented by hardware, software, or a combination of the two. At the lowest level, a protocol defines the behaviour of a hardware connection."[53]

The most common protocols are:

- IP (Internet Protocol)
- UDP (User Datagram Protocol)
- TCP (Transmission Control Protocol)
- DHCP (Dynamic Host Configuration Protocol)
- HTTP (Hypertext Transfer Protocol)
- FTP (File Transfer Protocol)
- Telnet (Telnet Remote Protocol)
- SSH (Secure Shell Remote Protocol)
- POP3 (Post Office Protocol 3)
- SMTP (Simple Mail Transfer Protocol)

[48] "Personal area network," Wikipedia, http://en.wikipedia.org/wiki/Personal_area_network (accessed May 15, 2009).
[49] "Local area network," Wikipedia, http://en.wikipedia.org/wiki/Local_area_network (accessed May 15, 2009).
[50] "Campus area network," Wikipedia, http://en.wikipedia.org/wiki/Campus_area_network (accessed May 15, 2009).
[51] "Metropolitan area network," Wikipedia, http://en.wikipedia.org/wiki/Metropolitan_area_network (accessed May 15, 2009).
[52] "Wide area network," Wikipedia, http://en.wikipedia.org/wiki/Wide-area_network (accessed May 15, 2009).
[53] "Protocal (computing)," Wikipedia, http://en.wikipedia.org/wiki/Protocol_(computing) (accessed May 15, 2009).

- IMAP (Internet Message Access Protocol)
- SOAP (Simple Object Access Protocol)
- PPP (Point-to-Point Protocol).

This list of protocol shows that navigating in the Internet is more difficult than using a simple browser – Internet explorer, Mozilla Firefox, Safari, etc. Each user of the Internet uses these protocols without knowing that they use them.

The most famous protocol, as it was written in the first part of this paper, is TCP/IP. Although these protocols are very well documented, when the software is created, the programmer can make errors. These errors provoke vulnerabilities.

"In computer security, the term vulnerability is applied to a weakness in a system which allows an attacker to violate the integrity of that system. Vulnerabilities may result from weak passwords, software bugs, a computer virus or other malware.

A security risk is classified as vulnerability if it is recognized as a possible means of attack. A security risk with one or more known instances of working and fully-implemented attacks is classified as an exploit. The window of vulnerability is the time from when the security hole was introduced or manifested in deployed software, to when a security fix was available or deployed. Constructs in programming languages that are difficult to use properly can be a large source of vulnerabilities."[54]

If the theory of reliability[55] [56] is considered, this long explanation about the main physical component of the Internet shows that it is very difficult to have no failures in the Internet. By no failures, it meant no troubles within the Internet. In fact, "the failure rate for a complex system is simply the sum of the individual failure rates of its components."[57]

Finally, in order to understand the way how the technical aspect of Cyberspace is working, the concept of the OSI (Open Systems Interconnection Reference) model should be understood. The technical aspect of this model is a little bit difficult for non specialists. But this concept shapes the behaviour of computers, routers, networks, the Internet and Cyberspace. OSI model is an abstract description for layered communications and computer network protocol design. It was developed as part of the Open Systems Interconnection (OSI) initiative.[58]In its most basic form, it divides network architecture into seven layers which, from top to bottom, are the Application, Presentation, Session, Transport, Network, Data-Link, and Physical Layers. It is therefore often referred to as the

[54] "Vulnerability (computing)," Wikipedia, http://en.wikipedia.org/wiki/Vulnerability_(computing)#Examples_of_vulnerabilities (accessed May 15, 2009).
[55] "Theory of Reliability," Research Methods Knowledge Base, http://www.socialresearchmethods.net/kb/reliablt.php (Accessed May 15, 2009).
[56] E. Straub, "Application of reliability theory to insurance," Casualty actuarial society, http://www.casact.org/library/astin/vol6no2/97.pdf (Accessed May 15, 2009).
[57] "Failure rate," Wikipedia, http://en.wikipedia.org/wiki/Failure_rate#Additivity (accessed may 15, 2009).
[58] "Recommendation X.200 (07/94)," International telecommunication union, http://www.itu.int/rec/T-REC-X.200-199407-I/en (accessed May 15, 2009).

OSI Seven Layer Model.[59] The most important thing to retain is the concept of layers. In fact, everything in the Internet is organised according to this model. In order to make the system work all the layers are needed. If one layer is damaged the system could not work. An example illustrates very well the concept of layers. Two people from different countries (French and Spanish) want to share information. They have a translator (French- English for the French and Spanish-English for the Spanish), a secretary and a fax. The first layer is the information they want to share. The second is the translators, the third is the secretaries and the fourth is the faxes. The combination of the four layers allows sending the information. The message needs to go through these layers. If someone wants to stop the message, he can only attack one layer. This principle of layers shapes how the Internet works and how Cyberspace works too. Direct attack is not the only way.

The 13 DNS

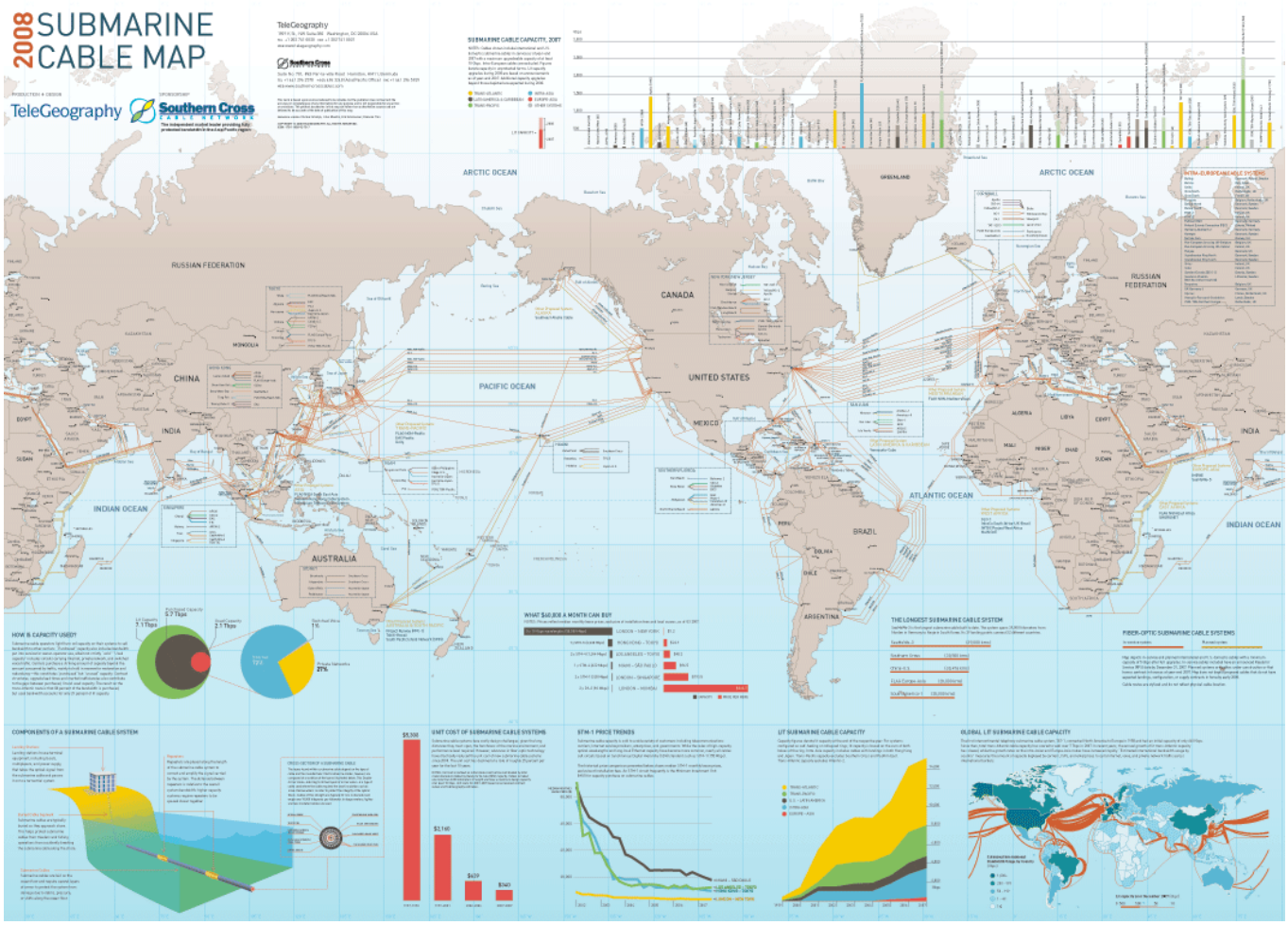
"The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource participating in the Internet. It associates different information with domain names assigned to such participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices world-wide. An often used analogy to explain the Domain Name System is that it serves as the "phone book" for the Internet by translating human-friendly computer hostnames into IP addresses. For example, www.example.com translates to 208.77.188.166."[60] By its central role, the DNS is an excellent target for hackers. In fact, the DNS system is a strategic component of the Internet. This system is composed of thirteen root servers. These servers are all over the world. Seven are in the USA, and the six others are shared between the USA and other states. All Internet addresses, all accesses and the running of the Internet depend on these thirteen root DNS.
The number thirteen is due to a physical limitation of computer science. In fact it is due to the size of data packets. In 2002, a big attack directed on these root servers stopped nine root servers in the world. It generated a big slow down of the traffic on the Internet. Even only one root DNS can manage all the demand; this attack demonstrated the vulnerability of the system. However, the international community decided to protect them against this type of attack by securing more servers. This example demonstrates that the physical component of Cyberspace can be exploited.

[59] "OSI model," Wikipedia, http://en.wikipedia.org/wiki/OSI_model (accessed May 15, 2009).
[60] "Domain name system," Wikipedia, http://en.wikipedia.org/wiki/Domain_name_system#Security_issues (accessed May 15, 2009).

Cables under the sea

95% of telecommunication goes through cables under the sea. All continents are linked by these cables. They are the backbone of the international telecommunications network. Almost 100% of the transoceanic Internet is sent via submarine cables. By the volume of data they allow to transmit between continents, and by their position under the sea, these cables appear to be strategic for the Internet, telecommunication and governments. It is the reason why they are protected by laws:

- The international convention for protection of submarine cables (1884)[61]
- The Geneva conventions of the continental shelf and high sea (1958)[62]
- The United Nations law of the sea convention (1982)[63]



All the cables are on maps, and it should be impossible to cut them, but:

> "In December 2008, when three cables under the Mediterranean Sea were damaged, Internet service began to wink out across the Middle East and parts of Southeast

[61] "Convention for the Protection of Submarine Telegraph Cables," International cable protection society, http://www.iscpc.org/information/Convention_on_Protection_of_Cables_1884.pdf (accessed May 15, 2009).
[62] "Convention on the High Seas," United Nations treatys collection, http://untreaty.un.org/ilc/texts/instruments/english/conventions/8_1_1958_high_seas.pdf (accessed May 15, 2009).
[63] "United Nations Convention on the Law of the Sea," United Nations website, http://www.un.org/Depts/los/convention_agreements/texts/unclos/unclos_e.pdf (Accessed May 15, 2009).

Asia. Egypt suffered terribly, losing as much as 80 percent of its network. E-mail and Web access were disrupted in Saudi Arabia and other Gulf states, while services fluttered in countries as far away as Malaysia and Taiwan. India's enormous outsourcing industry—the customer-service backbone of the Western world—was also hampered, with the humble fax machine making a brief but crucial comeback until traffic was rerouted around the breaks. The same thing had also happened in January and February, disrupting Internet access to homes and businesses throughout the region for days.

The incidents reveal a surprising fact about the Internet: that it requires constant physical maintenance."

When the Middle East cables went down the first time back in January and February of last year observers assumed it was sabotage. Why? Because that kind of scenario had been rehearsed before.

"During the Cold War, lots of attention was paid to undersea cables," says James Lewis, director and senior fellow of the Technology and Public Policy Program at the Centre for Strategic and International Studies (CSIS) in Washington, D.C. Communications lines were prime military targets for both sides, and the strategic severing of cables was considered a prelude to full invasion. In the early 1970s, the U.S. even managed to successfully tap a cable on the ocean floor and eavesdrop on Soviet chatter.

None of the Middle East cuts were deliberate, however. The December outage appears to have been caused by undersea seismic activity and, in the January and February incidents, stray anchors were to blame. But according to Lewis, "the [January-February] cuts affected the ability of CentCom [U.S. military Central Command] to send communications from Afghanistan and Iraq. Video and data streams are crucial parts of military operations, and they need that fibre-optic cable infrastructure." CentCom quickly rerouted around the gaps, but the incident exposed vulnerability.

The Middle East is particularly prone to faults because the ties that bind it to the rest of the Internet are thin when compared with the connection between the U.S. and northern Europe or Asia. The cables that went down last year carry upward of 75 percent of the traffic between Europe and the Middle East. A single break in this region is immediately noticeable; two could be crippling; three could have been catastrophic if providers had not diverted traffic away from the cuts, located off the coast near Alexandria, Egypt, through Asia.

> The Middle East is not the only place where the Internet's undersea cable network hits a bottleneck. In December 2006, an earthquake ripped cables running through the Luzon Strait, in the South China Sea between Taiwan and the Philippines, disabling 90 percent of the region's telecommunications capacity. Basic services were restored in a day or two, but full repairs to the cable system took more than a month.[64]

Finally, Sherry Sontag and Christopher Drew wrote in their book Blind Man's Bluff that submarines were used in order to tape cables under the sea in order to spy on other countries.[65] In May 2009, "the U.S. Navy has found its place in defending the Internet; underwater. That's where most of the planets Internet traffic spends most of its time, as it travels from continent to continent via fiber-optic cables. The navy proposes to undertake more aggressive operations to prevent terrorists, or hostile nations, from trying to cut these cables."[66]

These extracts demonstrate that submarine cables are strategic and they can be vulnerable in the physical component within Cyberspace.

Critical Infrastructures

Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy:

- electricity generation, transmission and distribution;
- gas production, transport and distribution;
- oil and oil products production, transport and distribution;
- telecommunication;
- water supply (drinking water, waste water/sewage, stemming of surface water (e.g. dikes and sluices));
- agriculture, food production and distribution;
- heating (e.g. natural gas, fuel oil, district heating);
- public health (hospitals, ambulances);
- transportation systems (fuel supply, railway network, airports, harbours, inland shipping);
- financial services (banking, clearing);
- Security services (police, military). [67]

In one of the physical components of Cyberspace, the Internet, both hardware and software systems - wired, fibre optic and microwave links, along with routing equipment, the accompanying

[64] James Geary, "Who Protects The Internet?" Popsci.com, http://www.popsci.com/scitech/article/2009-03/who-protects-intrnet (Accessed May 15, 2009).
[65] Sherry Sontag, and Christopher Drew, *Blind Man's Bluff, the untold story of American submarine espionage* (New-York: PublicAffairs, 1998).
[66] "Guarding The Internet ," Strategy page, http://www.strategypage.com/htmw/htsub/20090509.aspx (accessed May 29, 2009).
[67] "Critical infrastructure," Wikipedia, http://en.wikipedia.org/wiki/Critical_infrastructure (accessed May 15, 2009).

critical software services like the Domain Name System (DNS), Email, website hosting, authentication and authorization, storage systems, and database servers are considered critical Internet components.[68]

It is obvious that the Internet, and therefore, Cyberspace need electricity to work. And Cyberspace is a huge consumer of power – "Once at full capacity, one Google data plant in Oregon could use the same power as every home in Newcastle put together"[69] -, it is the reason why, the most important data centres are near the power station. In fact, the growth of Cyberspace has increased the interconnection of critical Infrastructures. Cyberspace, as it was explained before, is not limited to the Internet. Cyberspace interconnects everything in order to create the other components, for sharing information and knowledge. This interconnection is so developed that the physical component of Cyberspace becomes a critical infrastructure itself due to the interconnection of all the critical infrastructures.

Electricity grid is a very good example, and it demonstrates exactly the concept of critical infrastructure from a Cyber point of view. In the beginning of 2009, "cyber spies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system."[70] "In 2000, a disgruntled employee rigged a computerized control system at a water-treatment plant in Australia, releasing more than 200,000 gallons of sewage into parks, rivers and the grounds of a Hyatt hotel."[71]

Robert McMillan wrote in Computer world:" Computer systems that run the world's critical infrastructure are not as secure as they should be, according to a new survey.

The survey, released yesterday, asked 199 management, network engineers and administrators in nine infrastructure industries about the state of cybersecurity in the U.S., Canada and Europe. Insiders said that all of these industries, except for financial services, were unprepared for cyberattacks. These industries included water, utilities, oil and gas, telecommunications, transportation, emergency services, chemical and the shipping industry."[72]

> *"Critical infrastructure is comprised of all of the computer systems that could be targets of criminal threats, industrial espionage and/or politically motivated sabotage... the power grid, the water supply, railways, nuclear energy plants, etc. Attacks on these networks can cause loss of life, threaten the public safety, impact national security, create economic upheaval, or environmental disasters.*

---

[68] "Critical internet infrastructure," Wikipedia, http://en.wikipedia.org/wiki/Critical_Internet_infrastructure#cite_note-0 (accessed May15, 2009).

[69] Bobbie Johnson, "Google's power-hungry data centres," Guardian, http://www.guardian.co.uk/technology/2009/may/03/google-data-centres (accesed May 15, 2009).

[70] Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies," TheWallstreet journal, http://online.wsj.com/article/SB123914805204099085.html (Accessed May 15, 2009).

[71] Ibid.

[72] Robert McMillan, "Study: Critical infrastructure often under cyberattack," Computer word, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9119838 (accessed May 15, 2009).

It is estimated that the destruction from a single wave of cyber attacks on U.S. critical infrastructures could exceed $700 billion USD -- the equivalent of 50 major hurricanes hitting U.S. soil at once. (Source: US Cyber Consequences Unit, July 2007)

Because of today's interconnected world, these systems are targets for attack from both inside and outside the organization:

1. *Thrill seekers*
2. *Botnet owners*
3. *Contractors and other temporary workers*
4. *Cyber criminals*
5. *Disgruntled insiders*
6. *Foreign intelligence services*
7. *Industrial spies*
8. *Phishers, spammers, and spyware authors*

Industry and government regulations have been developed to provide guidance on how to secure critical infrastructure."[73]

Finally, as David G. Kamien wrote, the most important threat is Critical Infrastructure and interdependency. He concludes that "The interdependence of Infrastructures, and thus their vulnerability, seems to be increasing."[74] His approach demonstrated that "the use of IT to "enable" infrastructure provides enormous opportunities but can also increase vulnerability when IT does not perform as expected and infrastructure management is unprepared for that contingency."[75]
It is demonstrated that there are threats on critical infrastructures inside and outside Cyberspace. Interconnection creates vulnerability and threats.

The information approach (the players)

For the information approach, the key players will be studied. They are the entities which fly within the Cyberspace. They will be studied under the lens of the threat they provide inside Cyberspace.

Hackers

According to Oxford dictionary a hacker is:

- A computer enthusiast

[73] "Securing Critical Infrastructure - Protecting Our Way of Life," Secure computing, http://www.securecomputing.com/cybersecurity/ (accessed May 15, 2009).
[74] David G. Kamien, *The McGraw-Hill Homeland security handbook* (New York: The McGraw-Hill companies, 2006), 519-545.
[75] Ibid.

- A microcomputer user who attempts to gain unauthorized access to proprietary computer systems.

Hackers' world is a fascinating world for people who study Cyberspace and Cyber culture. They created their own culture. Some scientists tried to study them, and one of them, Marc Rogers - Graduate Studies, Dept. of Psychology, University of Manitoba – wrote:

> "It goes without saying that the fact that some individuals within the hacker community choose to engage in criminal activities is problematic. Psychological theories of crime postulate that because a hacker sub-culture or sub-class exists, and the activity is being reinforced (i.e., media attention, high paying jobs, movies), criminal hacking will not disappear on its own but will continue to flourish if left unchecked (Gattiker & Kelly, 1997).
>
> The security industry, law enforcement, and governments need to be extremely cautious not to generalize findings from the limited research to the entire hacker community. There is no generic profile of a hacker (Denning, 1998, Parker, 1998; Post, 1996). A great deal more research is required to determine if psychological profiles can be derived for any of the sub-categories, which seem to exist within the larger hacker community.
>
> If criminal hackers are indeed the "dreaded enemy" of the Internet and general network security, then it is paramount that they be better understood and not just conveniently applied a meaningless label. As Sun Tzu stated in his book The Art of War, "..If you know yourself but not the enemy, for every victory gained you will also suffer a defeat".[76]

Kamien defined Hackers like this:

> *"Hackers come in several shades. White hat hackers are hired by an organization to probe its digital security perimeter and are considered good guys. Gray-hat hackers are not authorized to break into systems or programs but do so anyway, they say, to publicize security vulnerabilities so that the holes can be patched. Gray hats argue that they are good guys too. Black-hat hackers are intruders, including criminals and terrorists. Black hats are bad guys, and their hacking is a felony in the United States and most other countries. Crackers is a derogatory term reflecting disgust at the theft and vandalism of the early hacking gang."*[77]

However, when they find vulnerability in Cyberspace, they can sell it and fall on the side of the Cyber criminality.

---

[76] Marc Rogers , "A New Hacker Taxonomy," http://homes.cerias.purdue.edu/~mkr/hacker.doc (accessed May 16, 2009).

[77] David G. Kamien, *The McGraw-Hill Homeland security handbook* (New York: The McGraw-Hill companies, 2006),562.

Cyber criminals – Cyber criminality

Today, cyber criminality is a business. As has been written before, Cyberspace was from the outset a world for Hackers. Today there are new countries under development such as Russia, China, India and Brazil which have more and more people who work in computers. The main problem is that these countries cannot give a job to all these people. In Russia, for example, there are ten programmers for only one place. It is obvious that the nine others can be attracted to undertake work for criminals. As a result, a parallel economy was created:

- Fraud (credit card, bank account, etc);
- Spam;
- Theft of data;
- Blackmail.
- Copies of DVD
- Etc.

Another problem of Cyber criminality is the application of law. It will be seen later in this paper that in Cyberspace there are no borders. It is easy today for Cyber criminals to act from countries which have different laws.

Cyber terrorists – Cyber terrorism

"Cyber terrorism is the convergence of terrorism and cyberspace."[78]
According to the Information Warfare Site, "The intentional use or threat of use, without legally recognized authority, of violence, disruption, or interference against cyber systems, when it is likely that such use would result in death or injury of persons, substantial damage to physical property, civil disorder, or significant economic harm."[79] [80]
In fact, some terrorist organisation can use Cyberspace in order to spread terror.
"The Monterey group – a company specialised in cyber security - defined three levels of cyber terror capability:

- Simple-Unstructured: The capability to conduct basic hacks against individual systems using tools created by someone else.

[78] Dorothy E. Denning, "CYBERTERRORISM," Department of computer science of Georgetown. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (accessed May 17, 2009).
[79] The information warfare site, http://www.iwar.org.uk/cyberterror/ (accessed May 17, 2009).
[80] Lech J Janczewski, Andrew, M. Colarik, *Cyber warfare and Cyber terrorism* (London: Information Science Reference, 2007), 15.

- Advanced-Structured: The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools.
- Complex-Coordinated: The capability for coordinated attacks capable of causing mass-disruption against integrated, heterogeneous defences (including cryptography).”[81]

Al-Qaeda “was using the Internet to do at least reconnaissance of American utilities and American facilities. If you put all the unclassified information together, sometimes it adds up to something that ought to be classified.”
Richard Clark, Former Chairman, President’s Critical Infrastructure Protection
Board, February 13, 2002 [82]

Cyber terrorism should not be considered as the only way to make a terrorist attack. It can be used in combination with other methods in order to multiply the effect of an attack:

> *“Had Shoko Asahara and the Aum Shinrikyo group been able to crack the Tokyo power system and stop the subways, trapping passengers on the trains, the number of casualties caused by their 1995 Sarin gas attack might have been singnificantly larger. (Noble, 1999)”*[83]

Finally, it is difficult to find any connection between Cyber terrorists and states, but it can be guessed that some states which support terrorist organisations support cyber terrorist actions by giving access to cyberspace.

Nations-states

The first part of this paper stated that Cyberspace is an environment for operations. It means that states can use it as they use land, sea, air and space. Nearly all information goes through Cyberspace all over the world. It is obvious that cyberspace is a wonderful environment for gathering intelligence as it can be done on all the different environments. One of the most powerful and famous system for gathering intelligence in Cyberspace is ECHELON. This system, implemented by USA and UK, allows these states to spy on satellites which carry “the vast majority of global civilian, diplomatic, and governmental phone and fax communications.”[84] It is in fact a network of satellite antennae disseminated on different continents. A sophisticated system of computers checks key words in the different communications. When there is an association messages are copied to each Intelligence agency’s headquarters.

---

[81] Dorothy E. Denning, “CYBERTERRORISM,” Department of computer science of Georgetown, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (accessed May 17,2009).
[82] “Cyber operations and Cyber terrorism,” Information for the Defence community, http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA439217&Location=U2&doc=GetTRDoc.pdf (accessed May 16, 2009).
[83] Lech J Janczewski, Andrew, M. Colarik, *Cyber warfare and Cyber terrorism* (London: Information Science Reference, 2007),9.
[84] Ibid. 455.

Remembering the case of the thirteen DNS and the localisation of these servers it can be assumed that it is easy for some states to spy directly through these servers on all the Internet traffic.
It can be concluded that as in the other environments, Cyberspace is a place where Information can be gathered and if Nations-states don't take care to protect it, Cyber espionage is a threat.

Users

In Cyberspace many people consider only the "bad guys" or the bad side. But a key player of Cyberspace is only the user. The most interesting thing is that players use their assets to be cyber user or to "fly" inside the Cyberspace. Why could they be a threat inside cyberspace? Because their assets can be used by the other key players of Cyberspace in order to use stealth, to wage a war or a cyber attack. It means that the way that people use their assets has an implication into Cyberspace.
According to specialists, users are the weak point of the system.[85] In fact, it is proven by the massive contamination of the Internet. Thanks to users and the network, a virus can spread all over the world in 12 hours.[86]

Threat Agent	*Methodology*	*Intent*
Hackers	☒ Develop/use damaging code to break into private networks	☒ Malicious or criminal intent Theft, fraud, denial of service, and extortion
Organized crime	☒ Exploits online activity, hires hackers, bribes insiders Uses more structure/resources than hackers	☒ Monetary gain
Terrorists	☒ Hacking Exploitation of Internet	☒ Acquire information for planning physical or cyber attacks C2
Nation-states	☒ Offensive cyber capabilities Technical and operational capabilities for widespread impact limited to only a few	☒ Espionage Cyber warfare

87

[85] Eric Domage, "Securite informatique: Eduquer l'utilisateur suffit-il?" *Defense nationale et securite collective* mai 2008: 74.
[86] Ibid.
[87] Office of Homeland security, National Strategy for homeland security Washington DC, government printing office July 2002.

The dangerous cocktail

All these players were sorted in a wanted order. The base of players in the cyberspace are Hackers. In fact, threats depend on the combination of these players.
The lowest threat is a lone hacker who operates for its own benefice, self esteem or for money. It could be groups which create malwares – "a portmanteau from the words malicious and software is software designed to infiltrate or damage a computer system without the owner's informed consent"[88] - in order to prove what they are capable of doing. The second one is small criminality. In fact, they use their Cyber ability to swindle people by using scams – mainly be emails.
The mid danger threat is the use of Cyberspace by terrorist organisations or for spying on companies or against national security. Targets are people, companies, nations or regions.
The last one is the highest threat. All the power of a state is used:

- Cyber attacks against another country (Estonia)
- Use of cyberspace in order to prepare a conventional attack (Georgia)

Then the most likely threat is the connection between Cyber criminality and terrorist organisations. Terrorist organisations will realise that cyberspace is ready to be exploited and they need Cyber criminals to do this business. Finally, cyber criminals need hackers to do their own business.
In his book, The Art of deception and The art of Intrusion, Kevin Mitnick a famous hacker of the 1990s wrote that there was a connection between hackers and terrorist organisations. His conclusion is:
"The combination of determined terrorists and fearless kid hackers could be disastrous for this country – USA -. This episode left me wondering how many other Khalids are out there recruiting kids (or even unpatriotic adults with hacking skills) and who hunger after money, personal recognition, or the satisfaction of successfully achieving difficult tasks."[89]

The cognitive approach (the tools)

The cognitive component is the main threat to Cyberspace. It gathers all the means which allows people to "fly" inside Cyberspace. As it was written before, the threats are:

- Hacking
- Spin doctoring: act of propaganda.
- Intelligence (spying, stealing etc.)
- Information warfare

[88] "Malware," Wikipedia, http://en.wikipedia.org/wiki/Malware (accessed May 19, 2009).
[89] Kevin Mitnick, *The art of intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers* (Somerset: Wiley Publishing, 2005), 41.

- Social engineering
- Vulnerabilities of software
- Computer network operations

In fact, Cyberspace is powerful thanks to the cognitive component which allows interconnecting everything through all the layers of Cyberspace. But this strength of Cyberspace created its own vulnerability.

Knowing the threats and having strategies will give opportunities to exploit Cyberspace.

By knowing the threats we can exploit them in order to exploit Cyberspace.

OODA Loop - Effects-based approach – Comprehensive approach - Deterrence?

Colonel John Richard Boyd, a pilot from the US Air Force invented the concept of the OODA loop – Observation, Orientation, Decision, and Action:

- Orientation: the adversary has to be observed in order to obtain information;
- Orientation: the attacker must orient himself in the context, in the situation;
- Decision: the attacker has to take a decision;
- Action: the attacker has to act.

To what extend is this loop well adapted to Cyber warfare? In fact, the type of attacks which were evoked before in this paper demonstrates that OODA loop is the way that hackers plan their attack.

The most important parameter is time. In fact, if an organisation wants to take the advantage on an enemy, it should get in advance in this loop. Time is the most important constraint and allows for the gaining of information superiority.
The example used in this paper at page 12 – A critical attack and its planning process – shows exactly that Cyber warriors use an OODA-like planning process.
The other approach could be the Effect-based approach. Effect-based approach is “a process for obtaining a desired strategic outcome or effect on the enemy through the synergistic and cumulative application of the full range of military and non-military capabilities at all levels of conflict”.[90]
Finally, another approach could be the Comprehensive approach:
“A Comprehensive Approach is based on 4 guiding principles:

[90] Lieutenant Colonel Allen W. Batschelet, “Effects-based operations: A New Operational Model?” The Information Warfare Site. http://www.iwar.org.uk/military/resources/effect-based-ops/ebo.pdf (accessed May 26, 2009).

- Proactive Engagement. Proactive engagement between actors, if possible ahead of a crisis, enables coordinated approaches to complex situations and allows more sensitive responses…
- Shared Understanding. A shared understanding between parties, including the military, is essential to optimize the effectiveness of their various capabilities. Each contributes distinct professional, technical and cultural disciplines, together with discrete values and perceptions, which offer additional perspectives, depth and resilience…
- Outcome-Based Thinking. All participants involved in crisis resolution need to base their thinking on outcomes and what is required to deliver a favourable situation, when planning and conducting activities...
- Collaborative Working. Institutional familiarity, generated through personal contact and human networking, enhances collaborative working and mutual trust. ..."[91]

About deterrence, DR, Martin C. Libicki wrote:

> "Deterrence is tough, and it is even tougher when dealing with the ambiguities of Cyberspace…There may be circumstances where some attempt to establish deterrence in cyberspace in hard to avoid, notably where attacker virtually dares you to strike back. But here the gap between theory and practice is wide and must be carefully bridged: measure twice, cut once"[92]

Could Strategies in the real world be applied in Cyberspace?

These previous strategies are applied in the other environments: Air, Land, Maritime and Space. It is never mentioned specifically that they can only be applied in these environments. The definition of Cyberspace given in the first part of this paper proves that Effect-base approach, OODA loop, Comprehensive approach and deterrence can be applied to Cyberspace because:

- Cyberspace is composed by several components which are linked and similar to the real world;
- The concept of layers given in page 18 proves it is the same as the "real" world because everything is linked.

Finally, as Collin S. Gray wrote:" Cyberwarfare is warfare: Clausewitz rules! We know that future warfare will be waged in cyberspace as well as in at least one of the other environments for war… The theory of war developed by Sun-tzu and Clausewitz in particular, holds cyber power as it does for every other mode of combat."[93]

---

[91] United Kingdom, Ministery of Defence, British defence doctrine, 1-8.
[92] Martin. Libicki, "Deterrence in Cyberspace." *High frontier, the journal for space & missile professionals*, volume 5, no 3 (May 2009).
[93] Collin S. Gray, *Another bloody century* (London: Phoenix, 2006), 328.

The second part of this paper demonstrates that there are some opportunities to exploit Cyberspace. Firstly, analysis of the threats on the three components shows that they could be exploited in order to wage operations inside Cyberspace. Secondly, by using the threats, Cyberspace can be exploited. Thirdly, exploiting Cyberspace is very close to the real world, the real strategy.
However States should be organised themselves in order to exploit Cyberspace.

HOW SHOULD STATES BE ORGANISED IN ORDER TO EXPLOIT CYBERSPACE?

From the two previous parts of this paper, it is obvious that cyberspace is an environment for operations, and as in all environments, it is open to exploitation. In this last part of the paper, it will be studied how states should be organised themselves in order to exploit Cyberspace. Firstly, organisations of some states will be studied. Secondly it will be established that education is a big challenge. Thirdly, the defensive and offensive aspect will be proposed. Finally, the legal aspect of operating in Cyberspace and its application in an organisation will be evoked.

Case studies: China, USA, France, Europe, Russia

Some countries in the world shaped an organisation in order to manage Cyberspace. The way they do it demonstrates how a state should be organised.

China

China develops its military and civilian infrastructures in order to apply its theories. It is done via the modernisation of military services.
Firstly, China decided to train its servicemen in several centres in the country (Zhengzhou, Wuhan, Changsha…).
Secondly, under the responsibility of the Army, reserve units were created and developped pockets of excellence in different domains (telecommunications, networks…). In Shanghai, for example, the reserve forces are specialised in wireless networks and cryptography. This local expertise can be coordinated in order to form a corps of “network warriors” for defending the country or attacking other countries.

Thirdly, Chinese strategists advise in order to create a Net Force - as sea, land or air - with the ability to fight in high technology in the future. The role of this component would be to protect the sovereignty of China in Cyberspace and be prepapered to be engaged in conflicts.[94]
More information about the organisation in China is difficult to obtain. Information shows that China has all the tools – from schools to strategy via operational and tactical level – for fighting in Cyberspace.
The last, but not least, in May 2009, it was discovered that China developed its own operating system.[95] This news is very important, because it means that China has acquired a technical ability which allows her to control and to deny access to its own cyberspace.
Finally, China has a strong control of all Internet access.

USA

USA is the home of the Internet. Bill Clinton decided to protect the critical infrastructures. At the beginning the task was done by the FBI in the NIPC – National Infrastructure Protection Centre- with the ambition to have at the same place FBI, Ministry of Defence, Secret Services, Ministry of Energy, Ministry of Transport and intelligence agencies. It did not work.
The law of Homeland security settled the department of Homeland security and other agencies were created later. Too many agencies and too much administration immobilized the system.
In 2008, the presidential National Security Directive proposed:

- A new governmental centre in order to keep a watch on the critical infrastructures which are on the Internet
- The extension of the use of the program Einstein – surveillance and detection of suspect activities on the networks – to all the administrations
- To decreased the number of access point to the Internet of the administration
- The creation of a National Cyber Security Centre
- The extension of the National Cyber Investigative Joint task force inside the FBI
- The strengthening of the system fro acquiring technology.

In 2007, the Cyber command was born. The aim of this command was to regroup all military services devoted to Cyberwar at the same place. It should have been operational in October 2008, but due to a lack of competence and problem of recruitment, the project was postponed. In fact, there are some disagreements about the exact role of this command. The disagreements are about domains of responsibilities – only Air Forces or all the services.

[94] Daniel Ventre, "Guerre de l'information en Chine." *Multi-system & Internet security cookbook*, no 23 (2006): 4-8.
[95] Bill Gertz, "China blocks U.S. from cyber warfare," The Washignton Times. http://www.washingtontimes.com/news/2009/may/12/china-bolsters-for-cyber-arms-race-with-us/ (accessed May 20, 2009).

But the US Air Force is still in advance in the doctrinal thinking about Cyberspace. A doctrinal paper, *Victory in Cyberspace*[96] exposes exactly the view of the US Air Force about Cyberspace – a domain on its own, description of Cyber attacks, "a perfect battlefield", Military territory; netwar in Iraq…This paper is exhaustive and shows how the US Air Force knows this domain. The website of Cybercommand is still open under the name Air Force Cyber command.[97]
Finally, Cyberwarfare is taught to the young cadets in the US military schools in order to give to these future leaders a taste of what is meant by fighting in Cyberspace.[98]
The organisation is as follows:

- Political strategy
- Multi agencies approach
- Specialized services
- Training and exercises.

France

The strategy of France can be read in the White paper published in 2008. The White paper describes basically how France will be organised in order to exploit Cyberspace:

> "Yet "cyberspace", consisting of the networking of all networks, is radically different from physical space in that it has no frontiers, is constantly changing and anonymous, making it hard to identify an aggressor with certainty. The threat takes many forms, ranging from malevolent blocking, physical destruction, neutralisation of computer systems, data theft or distortion, or even taking control of a system for hostile purposes. ... With regard to attacks emanating from States, several countries have already mapped out offensive cyber-warfare strategies and are effectively putting in place technical capabilities with the aid of hackers. Covert attempted attacks are highly probable in this context. Massive overt actions are also plausible over the next fifteen years. Technological developments and the interconnection of networks are rendering simple passive and perimeter defensive strategies less and less effective, even though these remain necessary. The transition from a passive defensive strategy to an active defensive strategy in depth, combining intrinsic systems protection with permanent surveillance, rapid response and offensive action, calls for a strong governmental impetus and a change in mentalities. The State must powerfully develop, maintain and disseminate its information systems security expertise among economic actors, and particularly among network operators. ... Cyberspace has become a new area of action, in

[96] Rebecca Grant, "Victory in Cyberspace," Air Force Association. http://www.afa.org/media/reports/victorycyberspace.pdf (Accessed May 20, 2009).
[97] Air Force Cyber Command. http://www.afcyber.af.mil/ (accessed May 20, 2009).
[98] Corey Kilgannon, "Cadets Trade the Trenches for Firewalls," The New York Times, http://www.nytimes.com/2009/05/11/technology/11cybergames.html?_r=2&ref=technology (accessed May 20, 2009).

which military operations are already taking place. France therefore needs to develop a fighting capacity in this space. It will be necessary to formulate rules of engagement, making due allowance for legal considerations pertaining to this new environment."[99]

Prevention is also considered:

"Early-warning systems will be developed to detect cyber attacks by setting up a detection centre in charge of the permanent monitoring of critical networks and implementation of appropriate defence mechanisms."[100]

"Acquire active, in-depth cyber-defence capability, combining the intrinsic protection of systems, constant monitoring of critical networks and a rapid response in the event of attack."[101]

Even offensive is considered:

"The effectiveness of defence and security forces at all levels depends, and will depend increasingly in the future, on the proper functioning of their information systems. ... Before any physical target is destroyed, a defence system can be disrupted and partially incapacitated by means of targeted stealth attacks. In the IT field more than any other, defence will mean knowing how to attack. France will need to be aware of the many and diversified forms and techniques used in these potential attacks (Trojan horses, worms, malicious software, etc.), and be able to retaliate against the adversary behind the attack using offensive capabilities. We therefore need the capability to neutralise attacks inside the very operations centres used by our adversaries: this is the objective of offensive cyber-war. ... Our forces must be ready to carry out offensive actions and will need to invest over the long-term in the following key areas:

— Definition, by the Joint Staff, of an overarching concept incorporating all actions involved in cyber-war;

— Development of specialised tools;

— Formulation of a body of doctrine for offensive cyber-war capabilities;

— Introduction of appropriate and regularly updated training for selected personnel, to be used flexibly in specialised units, overriding administrative considerations."[102]

Europe

As an international organisation, it is interesting to evoke Europe. Though, in the Defence White Paper, France wrote:

[99] Jacob Odile, *The French White Paper on Defence and National Security* (New-York : Odile Jacob Publishing Corporation, 2008).
[100] Ibid, 48.
[101] Ibid, 190.
[102] Jacob Odile, *The French White Paper on Defence and National Security* (New-York: Odile Jacob Publishing Corporation, 2008), 199.

> "Coordinating Europe's defence against Cyber attacks,
> European interests and national interests are closely interwoven in the cyber world. France therefore believes it is indispensable to strengthen operational cooperation among Member States within the European Union and to make it as responsive as possible in the face of cyber attacks. It will also propose that the Commission impose rules on operators to toughen their networks and procedures designed to make them far more resilient. In addition, the European Network and Information Security Agency (ENISA) needs to be made significantly more effective. In particular, this agency should contribute to the implementation by the Commission of a cyber security strand in all European institutions' projects and programmes."[103]

Russia

In Russia, Cyberwarfare is considered as a way for military operations under the unique responsibility of the Ministry of Defence. Russia only sees information warfare from an aggressive angle. Destruction, disorganisation, damages and control are their definitions. This aggressive attitude aims C2 systems by using electronic warfare and Cyber warfare. For them, fighting in Cyberspace is a Cold-war like war.
Last but not least, information warfare doesn't replace any other type of warfare. Russia said that she would reply with nuclear weapons if threatened with a Cyber attack.

All these examples demonstrate that some countries are organised in order to exploit Cyberspace. It is interesting to note that conventional forces can be used too.

Education

The idea on education is not well shared in the community of cybersecurity.
On one hand, Kamien proposed in his ten guidelines for information security programs that the first one should be the investment in cybersecurity training and education.[104] On the other hand, Eric Domage wondered if to educate users is enough. According to him, although users are the weakest point of cybersecurity, he proposed to progress from education to a monitoring system. The idea is to use systems that prevent users from a danger in cyberspace. He recognized that education is the first step, but not the only one for Cybersecurity.[105]

[103] Ibid.
[104] David G Kamien, *The McGraw-Hill Homeland security handbook* (New York: The McGraw-Hill companies, 2006), 576.
[105] Eric Domage, "Securite informatique: Eduquer l'utilisateur suffit-il?" *Defense nationale et securite collective*, mai 2008: 69-81.

But in this domain, former hackers such as Kevin Mitnick are much more qualified and should be quoted:

> "In this age of terrorism, we clearly need to be doing a better job of stitching up the holes. Episodes like the one recounted here raise an issue we need to face: how easily the talents and knowledge of our own unwitting teenagers can be turned against us to endanger our society. I believe that school kids should be taught the principles of computer ethics starting when they are being introduced to computing in elementary school."[106]
>
> "It is essential to educate and train employees about the threat and how to protect themselves from being dupes into assisting the intruders…. The human element has been proven to be information security's weakest link for ages."[107]

Therefore the first wall against attacks in Cyberspace is the education of users in order to give them the basic knowledge to not make mistakes.

If a country needs to fight in Cyberspace, it needs to train or recruit people in order to have "Cyber warriors". Most hackers, who were caught, came to the good side of Cyberspace and are specialists in Cybersecurity.

Cyberdefence

There are a few open sources documents about the exact concept of Cyberdefence. On the one hand, there must be automatic systems of protection. However they are insufficient because they can be skirted. So there must be active systems in order to watch over Cyberspace and adapt the protection from the threat. For example, as in the Air Force, Cyberspace defence centres could be created – on the same structure as the control reporting centre which surveys the airspace above a country. However it is proven that this defence concept is not strong enough to protect Cyberspace completely.

Some specialists argue that for a strong defence in Cyberspace, knowing how to attack is important. In fact, as in other environments, there must be Cyber superiority in order to deter a potential enemy. The only way to gain Cyber superiority or Cyber dominance is Education (refer to above) and technology which is very expensive. For example, ciphering data is strategic for a state. It is the reason why modern states try to develop quantum cryptography.[108] [109] By acquiring this technology they will have a possibility of obtaining the Cyber dominance.

In the world of Cyber specialists it is said: "A good administrator is a good hacker". This principle should be applied to the concept of defence/attack.

---

[106] Kevin Mitnick, *The art of intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers* (Somerset: Wiley Publishing, 2005), 47.
[107] Ibid., 245.
[108] Roberto Alvarez, "La physique quantique au service de la securite," Universite de Geneve, http://home.etu.unige.ch/~alvarra0/Documents/TM.pdf (Accessed May 292009).
[109] "Quantum Cryptography," Wikipedia, http://en.wikipedia.org/wiki/Quantum_cryptography (accessed May 29, 2009).

It is the reason why that some countries try to recruit hackers in order to create their own Cyberdefence.[110]

It was demonstrated in the different case studies that Cyberdefence should be implemented thanks to a multi agency approach. As written in the previous parts of this paper that everything is linked in Cyberspace. It is obvious that Cyberdefence can only be operated in this way.

As Colin S. Gray wrote:

> "Cyber warfare is not going to deliver defeat or victory. But it is going to play an increasingly important, even literally vital, role as an enabler and force multiplier for the modes of warfare that do draw blood and break things"[111]

In this part of Cyberdefence, the concept of resilience in Cyberspace should be studied. As it was done for the other environments[112], this concept should be extended to Cyberspace. As it was stated before in this paper, Cyberspace is not a reliable environment. This environment is naturally unsecured. Are States ready to offset a big failure of this environment? No because there should be inherent the concept of resilience.

Thoughts about Cyberdefence are changing. Well equipped nations thought that it could be possible to wage a war in Cyberspace. USA for example spoke about "Cybergeddon"[113] because "CYBER attacks pose the greatest threat to the United States after nuclear war and weapons of mass destruction - and they are increasingly hard to prevent".[114] Does it mean that the world, or a Nation would collapse in the event of a massive Cyber attack? The case of Estonia, for example, demonstrated that the answer is no. In this case, and in the future, Cyberwar will be only a force enabler or a force multiplier. Even specialists in Cyberspace say that Nations should not waste their funds preparing Cyberwar:

> Marcus Ranum, chief security officer of Tenable Network Security said "The billions of dollars spent on researching Cyberwarfare can be put to better use because Cyberwar is never going to be as effective as conventional war"
>
> "A small country, even with an army of hackers on its side, is never going to be able to defeat a big country with an extensive land, air and sea military force by attacking through the Internet."[115]

Finally, this month (May 2009), "The United States' top commanding officer for the space and cyber domains told reporters last week that a cyber attack could merit a more conventional military

---

[110] Gabizon Cecilia. "Les pirates du net au service des etats". Le Figaro. 07 May 2009.
[111] Collin S Gray, *Another bloody century* (London: Phoenix, 2006), 328.
[112] United Kingdom, Ministry of Defence, Joint doctrine publication, Operations in the UK: The Defence Contribution to Resilience.
[113] Sebastian Smith, "FBI concerned about 'cybergeddon'," New.com.au, http://www.news.com.au/technology/story/0,28348,24886793-5014239,00.html (accessed May 29, 2009).
[114] Ibid.
[115] "Don't waste funds preparing for cyberwars," The Star online, http://star-techcentral.com/tech/story.asp?file=/2008/10/31/technology/20081031200416&sec=technology (accessed May 29, 2009).

response."[116] [117] It means that the concept of Cyberdefence should be linked to the "real" world and will never replace conventional or nuclear attack as Russia warned.
The concept of Cyberdefence is not so clearly divulged by the different nations. Some axis can be guessed, but Cyberdefence is definitely connected to the real world. The last key approach of Cyberspace is its legal statute.

A legal approach: Existence and protection of Cyberspace

Indeed, one of the most important problems today for Cyberspace as an environment for operations and for waging wars or attacks is its legal statute.
Indeed, as Daniel Ventre wrote: How do we preserve in Cyberspace the principle of sovereignty which is the fundamental principle of the international law since the treaty of Westphalia in 1648 which gives to each nation the exclusive authority inside its borders?[118]
Legally, if there is a neutral country between two conflicting states, the neutrality should be guaranteed. But in Cyberspace, it is possible to use the Cyberspace of other countries with no authorisation.
What about humanitarian rights? Civilians could be killed by collateral effects of a Cyber conflict. When military communications use civilian infrastructures during a conflict, is an attack against these civilian infrastructures a breach of the code of war?
Maybe the international community should give a special statute to some components of Cyberspace whose usage is mixed.
In the magazine *PC PLUS*, a journalist wondered if botnets could be considered as Weapons of Mass destruction.[119] In fact, it is assessed that these programs are so powerful that they can damage on a large scale:

- "Because botnets represent such a real threat to our domestic cyberspace and all the assets that those Internet-accessible computers control, it is a vital national interest to secure the domestic Internet." [120]
- "A personal computer could disrupt cellular communications in a city, and a botnet could do the same to the entire U.S"[121]

With this potential threat of eWMDs in Cyberspace, it could be important to create a NPT-like treaty under UN sponsorship because Cyberspace is an environment which covers a large part of the

[116] Robert Lemos, "Cyber attack could bring US military response," The register. http://www.theregister.co.uk/2009/05/13/us_cyber_attack_response/ (accessed May 29, 2009).
[117] Robert Lemos, "Cyber attack could bring U.S. military response," Security focus, http://www.securityfocus.com/brief/961/ (accessed May 29, 2009).
[118] Daniel.Ventre,*La guerre de l'information* (Paris: Lavoisier, 2007), 266.
[119] "Botnets: The new WMD?" *PC PLUS*, no 279 (March 2009), 12.
[120] Kelly, John J. and Almann, Lauri. "eWMDs." Policy review, A publication of the Hoover Institution, no 152 (December 2008 & January 2009).
[121] Ibid.

world. Collateral effects could be dramatic for people and countries which are not involved in a Cyber conflict.

Some people begin to propose that borders should be projected in Cyberspace:

> "By requiring each nation police their own cyberspace, we set a precedent for holding governments responsible for their policies on the Internet, including their own military doctrines regarding information warfare. Until governments are willing to assume the same responsibility for cyberspace that they do for their airspace and territorial waters, they should not be surprised nor outraged by the attempts of security and intelligence professionals to identify who's responsible by other means."[122]

The third part of this paper gives ideas on how states should be organised in order to exploit Cyberspace. Firstly, some countries are organised in order to exploit Cyberspace, and the way they do it are nearly the same. Secondly, education is a key element if a state wants to exploit Cyberspace. Thirdly, even the concept of Cyberdefence is hardly protected by secrecy, some tracks can be guessed at and technology is at the heart of the problem. The last but not least, the legal statute of this fifth environment should be taken into consideration by states and International communities.

CONCLUSION

This paper demonstrated that Cyberspace is an environment for military operations due to its three components:

- the physical component;
- the information component;
- the cognitive component.

These components give opportunities for exploitation. Firstly, analysis of the threats on the three components shows that they could be exploited in order to wage operations inside Cyberspace. Secondly, by using the threats, Cyberspace can be exploited. Thirdly, exploiting Cyberspace is very close to the real world and the definitive strategy. Finally the last part of this paper gave ideas on how states should organise in order to exploit Cyberspace. Firstly, some countries organised to exploit Cyberspace, and the way they did shows great similarity. Secondly, education is a key element if a state wants to exploit Cyberspace. Thirdly, even the concept of Cyberdefence is hardly protected by secrecy and some tracks can be guessed at and where technology is at the heart of the problem. Last and not least, the legal statute of this fifth environment should be taken into consideration by states and International communities.

[122] Jeffrey Carr. "Projecting Borders into Cyberspace." Security focus. http://www.securityfocus.com/columnists/500 (accessed May 29, 2009).

Finally, this paper demonstrates that even Cyberspace is an environment for operations; the way to use it is very close to reality. The birth of Cyberspace did not revolutionize the concept of war. Only by thinking that winning war inside Cyberspace is possible and could lead to a victory in the real world is a mistaken conception. People in charge of Cyberspace must have a global knowledge of Defence and should consider Cyberspace as the other environments of Land, Maritime, Air and Space:

> *"Too often we let the novelty of cyberspace and Cyberwar distract us from the reality it represents. Cyberspace is simply another terrain. Operations in cyberspace mirror those in real space and thus should fall under the same rules. Before the Internet, the famous Nigerian 419 scam was conducted via the mail. Financial fraud is financial fraud; how you conduct it does not change that fact; so too with acts of terrorism, war and conflict. We do not need new laws or permissions to take proactive steps to protect our citizenry. If you treat cyberspace simply as another terrain, the existing frameworks will guide you through the analysis.*
> *We know the general limits and range of attack and consequences in this terrain. We also know the general limits and range of responses. What we need is to craft the Rules of Engagement now. People need to know that they will not be allowed to freely attack our citizens and infrastructure without the fear of reprisal. We are at war and a defence-only posture has never worked. "*[123]

[123] "Offensive Operations in Cyberspace," White Wolf Security, http://www.whitewolfsecurity.com/publications/offensive_ops.php (accessed May 18, 2009).

BIBLIOGRAPHY

Books:

Counter-terrorism Taskforce, *Cyberterrorism-the use of the Internet for terrorist purposes*. Strasbourg: Council of Europe Publishing, 2007

Cordesman, Anthony H. *Cyber-threats, information warfare, and critical infrastructure protection*. Westport: Praeger publisher, 2002

Libicki, Martin. *Conquest in Cyberspace*. New York: Cambridge University Press, 2007

Arpagian, Nicolas. *La Cyberguerre, la guerre numerique a commence*. Paris: Vuibert, 2009

Ventre, Daniel. *La guerre de l'information*. Paris: Lavoisier, 2007

Janczewski, Lech J., Colarik, Andrew, M. *Cyber warfare and Cyber terrorism*. London: Information Science Reference, 2007

Verton, Dan. *Black ice – The invisible threat of Cyber-terrorism*. Emeryville: McGraw-Hill, 2003

Alexander, Yonah and Swetnam, Michael. *Cyber terrorism and information warfare: Threats and responses*. Ardsley: Transnational Publishers, 2001

Gibson, William. *Neuromancer*. London: HarperCollins publishers, 1995

Gray, Collin S. *Another bloody century*. London: Phoenix, 2006

Weimann, Gabriel. *Terror on the Internet, the new arena, the new challenges*. Washington: United States Institute of peace, 2006

Kamien, David G. *The McGraw-Hill Homeland security handbook*. New York: The McGraw-Hill companies, 2006

Forno, Richard and Baklar, Ronald. *The art of information warfare*.

Martel, William C. *The technological arsenal*. London: Smithsonian institution press,2001

Goldman, Emily O. *National security in the information age*. London: Frank Cass,2004

Halpin, Edward and Trevorrow, Philippa and Webb, David and Wright, Steve. *Cyberwar, Netwar and the Revolution in Military Affairs*. New York: Palgrave Macmillan, 2006

Greenberg, Lawrence T. and Goodman, Seymour E. and Soo Hoo, Kevin J. *Information warfare and international law*. Washington: Library of congress, 1998.

Hall, Wayne Michael. Stray Voltage – War in the information age. Annapolis: Naval institute press, 2003.

Denning, Dorothy E. Information warfare and security. Oxford: ACM Europeam service center, 1999.

Martin Dodge, Rob Kitchin. *Mapping Cyberspace*. Abingdon: Routeledge, 2001

Mitnick, Kevin. *The art of deception: Controlling the Human Element of Security* . Somerset: Wiley Publishing, 2003

Mitnick, Kevin. *The art of intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. Somerset: Wiley Publishing, 2005

Erickson, Jon Mark. *Hacking: The Art of Exploitation*. No Starch Press, 2003.

United Kingdom. Development, concepts and doctrine. *United Kingdom glossary of Joint and Multinational Terms and definitions*. Joint Doctrine Publication 0-01.1. 7th ed. Shrivenham: DCDC, 2006.

United Kingdom. Development, concepts and doctrine. *The DCDC Global Strategic Trends Programme 2007-2036.* Shrivenham: DCDC, 2007.

Sontag, Sherry and Drew, Christopher. *Blind Man's Bluff, the untold story of American submarine espionage.* New-York: PublicAffairs, 1998

United states of America, Department of defence, Joint publication 1-02, 17 October 2008.

Articles:

Caron, Pierre. "La cybercriminalite aujourd'hui." *Multi-system & Internet security cookbook*, no 41 (2009): 18-24.

Ventre, Daniel. "La puissance militaire de la republique populaire de Chine: Rapport 2008 du department de la defense des Etats-unis." *Multi-system & Internet security cookbook*, no 38 (2008): 26-35.

"Cyber-terrorism: fiction ou menace reelle ?" *Multi-system & Internet security cookbook*, no 6 (2003): 6-11.

Ventre, Daniel. "Conflit Russo-georgien et guerre de l'information." *Multi-system & Internet security cookbook*, no 40 (2008): 04-13.

Ventre, Daniel. "Guerre de l'information en Chine." *Multi-system & Internet security cookbook*, no 23 (2006): 4-8.

Ventre, Daniel. "Guerre de l'information au Japon." *Multi-system & Internet security cookbook*, no 29 (2007): 10-21.

Raynal, Frederic. "L'information, nouveau nerf de la guerre ?" *Multi-system & Internet security cookbook*, Hors serie no 1 (2007): 4-12.

Ventre, Daniel. "La guerre de l'information en Russie." *Multi-system & Internet security cookbook*, no 30 (2007): 26-35.

Evrard, Philippe and Filiol, Eric. "Guerre, guerrilla et terrorisme informatique : fiction ou realite ?" *Multi-system & Internet security cookbook*, no 33 (2007): 09-17.

"Operation italienne : analyse d'une vague d'attaques europeennes par le biais d'un honeynet." *Multi-system & Internet security cookbook*, no 33 (2007): 18-21.

Evrard, Philippe and Filiol, Eric. "Les acteurs de la lutte informatique offensive : les bons, les brutes et les truands…" *Multi-system & Internet security cookbook*, no 36 (2008): 22-31.

"La guerre pour l'information." *Multi-system & Internet security cookbook*, no 7 (2003): 18-51.

Brassier, Marc. "Le lobbying sur Internet." *Multi-system & Internet security cookbook*, no 17 (2005): 20-27.

Ventre, Daniel. "L'Inde et la guerre de l'information." *Multi-system & Internet security cookbook*, no 26 (2006): 4-11.

Ventre, Daniel. "Defense et securite nationales : Ou en est la guerre de l'information en France ?" *Multi-system & Internet security cookbook*, no 42 (2009): 4-7.

Puel, Gilles and Ullmann, Charlotte. "Les noeuds et les liens du reseau internet : approche geographique, econonomique et technique." *L'Espace geographique*, no 2 (2006): 97-114.

Douzet, Frederick. "Les nouvelles frontiers du cyberspace." *Geopolitique, Revue de l'institut international de geopolitique*, no 104 (2009): 69-76.

"Botnets: The new WMD?" *PC PLUS*, no 279 (March 2009): 12

Kelly, John J. and Almann, Lauri. "eWMDs." Policy review, A publication of the Hoover Institution, no 152 (December 2008 & January 2009)

Libicki, Martin. "Deterrence in Cyberspace." High frontier, the journal for space & missile professionals, volume 5, no 3 (May 2009).

Electronic sources:

Bruce Sterling. "The Hacker Crackdown." Massachusetts Institute of Technology. http://www.mit.edu/hacker/hacker.html (accessed May 29, 2009).

"U.S. Air Force Prepares for War in Cyberspace." ABCnews. http://blogs.abcnews.com/theblotter/2007/07/us-air-force-pr.html (accessed May 29, 2009).

Dr Dan Kuehl. "From Cyberspace to Cyberpower: Defining the problem." US Army war college. http://www.carlisle.army.mil/DIME/documents/Cyber%20Chapter%20Kuehl%20Final.doc (accessed May 28,2009).

Col. Alan Campen, USAF (Ret.). "What is cyberspace and why should you care?" CyberInfoware.com. http://www.cyberinfowar.com/ (accessed May 4, 2009).

Internet world stats. http://www.internetworldstats.com/stats.htm (accessed May 07, 2009).

Jake Wallis. "Cyberspace, information literacy and the information society." Centre for Digital Library Research. http://cdlr.strath.ac.uk/pubs/wallisj/jw200501.htm (accessed May 21, 2009).

"Blog." Wikipedia. http://en.wikipedia.org/wiki/Blog (accessed May 21, 2009).

"Twitter". Twitter. http://twitter.com/ (accessed May 21, 2009).

"Twitter." Wikipedia. http://en.wikipedia.org/wiki/Twitter (accessed May 21, 2009).

"Facebook". Facebook. http://www.facebook.com/ (accessed May 21, 2009).

"Facebook." Wikipedia. http://en.wikipedia.org/wiki/Facebook (accessed May 21, 2009).

"Social engineering." Wikipedia. http://en.wikipedia.org/wiki/Social_engineering_(security) (accessed May 27, 2009).

"Kevin Mitnick." Wikipedia. http://en.wikipedia.org/wiki/Social_engineering_(security)#Kevin_Mitnick (accessed May 27, 2009).

Adrian Blomfield. "Russia accused over Estonian 'cyber-terrorism'." The Telegraph. http://www.telegraph.co.uk/news/worldnews/1551850/Russia-accused-over-Estonian-cyber-terrorism.html (accessed May 14, 2009).

John Leyden. "Estonia fines man for DDoS attacks." The register. http://www.theregister.co.uk/2008/01/24/estonian_ddos_fine/ (accessed May 14, 2009).

Genevieve Carbery. "Student's Wikipedia hoax quote used worldwide in newspaper obituaries." IrishTime.com. http://www.irishtimes.com/newspaper/ireland/2009/0506/1224245992919.html (accessed May 21, 2009).

Guerric Poncet. "INTERNET - Un étudiant trompe la presse mondiale grâce à Wikipédia." Lepoint.fr. http://www.lepoint.fr/actualites-technologie-internet/2009-05-07/un-etudiant-trompe-la-presse-mondiale-grace-a-wikipedia/1387/0/341294 (accessed May 21, 2009).

"Maurice Jarre." Wikipedia. http://en.wikipedia.org/w/index.php?title=Maurice_Jarre&oldid=280558491 (accessed May 21, 2009).

"Maurice Jarre, Doctor Jivago video." Daily radar. http://movieblips.dailyradar.com/video/maurice_jarre_doctor_zhivago/ (accessed May 21, 2009).

Noah Shachtman. "Air Force Releases 'Counter-Blog' Marching Orders." The wired. http://www.wired.com/dangerroom/2009/01/usaf-blog-respo/ (accessed May 21, 2009).

"Cyber Warfare." Security Gurus. http://www.security-gurus.de/papers/cyberwarfare.pdf (accessed May 25, 2009).

"Computer." Wikipedia. http://en.wikipedia.org/wiki/Computer (accessed May 15, 2009).

"Router." Wikipedia. http://en.wikipedia.org/wiki/Router (accessed May 15, 2009).

"Operating system." Wikipedia. http://en.wikipedia.org/wiki/Operating_system (accessed May 15, 2009).

"Server." Wikipedia. http://en.wikipedia.org/wiki/Server_(computing) (accessed May 15, 2009).

"Personal area network." Wikipedia. http://en.wikipedia.org/wiki/Personal_area_network (accessed May 15, 2009).

"Local area network." Wikipedia. http://en.wikipedia.org/wiki/Local_area_network (accessed May 15, 2009).

"Campus area network." Wikipedia. http://en.wikipedia.org/wiki/Campus_area_network (accessed May 15, 2009).

"Metropolitan area network." Wikipedia. http://en.wikipedia.org/wiki/Metropolitan_area_network (accessed May 15, 2009).

"Metropolitan area network." Wikipedia. http://en.wikipedia.org/wiki/Metropolitan_area_network (accessed May 15, 2009).

"Wide area network." Wikipedia. http://en.wikipedia.org/wiki/Wide-area_network (accessed May 15, 2009).

"Protocal (computing)." Wikipedia. http://en.wikipedia.org/wiki/Protocol_(computing) (accessed May 15, 2009).

"Vulnerability (computing)." Wikipedia. http://en.wikipedia.org/wiki/Vulnerability_(computing)#Examples_of_vulnerabilities (accessed May 15, 2009).

"Theory of Reliability." Research Methods Knowledge Base. http://www.socialresearchmethods.net/kb/reliablt.php (Accessed May 15, 2009).

E. Straub. "Application of reliability theory to insurance." Casualty actuarial society. http://www.casact.org/library/astin/vol6no2/97.pdf (Accessed May 15, 2009).

"Failure rate." Wikipedia. http://en.wikipedia.org/wiki/Failure_rate#Additivity (accessed May 15, 2009).

"Recommendation X.200 (07/94)." International telecommunication union. http://www.itu.int/rec/T-REC-X.200-199407-I/en (accessed May 15, 2009).

"OSI model." Wikipedia. http://en.wikipedia.org/wiki/OSI_model (accessed May 15, 2009).

"Domain name system." Wikipedia. http://en.wikipedia.org/wiki/Domain_name_system#Security_issues (accessed May 15, 2009).

"Convention for the Protection of Submarine Telegraph Cables." International cable protection society. http://www.iscpc.org/information/Convention_on_Protection_of_Cables_1884.pdf (accessed May 15, 2009).

"Convention on the High Seas." United Nations treatys collection. http://untreaty.un.org/ilc/texts/instruments/english/conventions/8_1_1958_high_seas.pdf (accessed May 15, 2009).

"United Nations Convention on the Law of the Sea." United Nations website. http://www.un.org/Depts/los/convention_agreements/texts/unclos/unclos_e.pdf (Accessed May 15, 2009).

James Geary. "Who Protects The Internet?" Popsci.com. http://www.popsci.com/scitech/article/2009-03/who-protects-intrnet (Accessed May 15, 2009).

"Guarding The Internet ." Strategy page. http://www.strategypage.com/htmw/htsub/20090509.aspx (accessed May 29, 2009).

"Critical infrastructure." Wikipedia. http://en.wikipedia.org/wiki/Critical_infrastructure (accessed May 15, 2009).

"Critical internet infrastructure." Wikipedia. http://en.wikipedia.org/wiki/Critical_Internet_infrastructure#cite_note-0 (accessed May 15, 2009).

Bobbie Johnson. “Google's power-hungry data centres.” Guardian. http://www.guardian.co.uk/technology/2009/May/03/google-data-centres (accesed May 15, 2009).

Siobhan Gorman. “Electricity Grid in U.S. Penetrated By Spies .” TheWallstreet journal. http://online.wsj.com/article/SB123914805204099085.html (Accessed May 15, 2009).

Robert McMillan. “Study: Critical infrastructure often under cyberattack.” Computer word. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9119838 (accessed May 15, 2009).

“Securing Critical Infrastructure - Protecting Our Way of Life.” Secure computing. http://www.securecomputing.com/cybersecurity/ (accessed May 15, 2009).

Marc Rogers . “A New Hacker Taxonomy.” http://homes.cerias.purdue.edu/~mkr/hacker.doc (accessed May 16, 2009).

Dorothy E. Denning. “CYBERTERRORISM.” Department of computer science of Georgetown. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (accessed May 17, 2009).

The information warfare site. http://www.iwar.org.uk/cyberterror/ (accessed May 17, 2009).

Dorothy E. Denning. “CYBERTERRORISM.” Department of computer science of Georgetown. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html (accessed May 17, 2009).

“Cyber operations and Cyber terrorism.” Information for the Defence community. http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA439217&Location=U2&doc=GetTRDoc.pdf (accessed May 16, 2009).

“Malware.” Wikipedia. http://en.wikipedia.org/wiki/Malware (accessed May 19, 2009).

Lieutenant Colonel Allen W. Batschelet. “Effects-based operations: A New Operational Model?” The Information Warfare Site. http://www.iwar.org.uk/military/resources/effect-based-ops/ebo.pdf (accessed May 26, 2009).

Bill Gertz. “China blocks U.S. from cyber warfare.” The Washignton Times. http://www.washingtontimes.com/news/2009/May/12/china-bolsters-for-cyber-arms-race-with-us/ (accessed May 20, 2009).

Rebecca Grant. “Victory in Cyberspace.” Air Force Association. http://www.afa.org/media/reports/victorycyberspace.pdf (Accessed May 20, 2009).

Air Force Cyber Command. http://www.afcyber.af.mil/ (accessed May 20, 2009).

Corey Kilgannon. “Cadets Trade the Trenches for Firewalls.” The New York Times. http://www.nytimes.com/2009/05/11/technology/11cybergames.html?_r=2&ref=technology (accessed May 20, 2009).

Roberto Alvarez. “La physique quantique au service de la securite.” Universite de Geneve. http://home.etu.unige.ch/~alvarra0/Documents/TM.pdf (Accessed May 29, 2009).

“Quantum Cryptography.” Wikipedia. http://en.wikipedia.org/wiki/Quantum_cryptography (accessed May 29 ,2009).

Sebastian Smith. “FBI concerned about 'cybergeddon'.” New.com.au. http://www.news.com.au/technology/story/0,28348,24886793-5014239,00.html (accessed May 29, 2009).

“Don’t waste funds preparing for cyberwars.” The Star online. http://star-techcentral.com/tech/story.asp?file=/2008/10/31/technology/20081031200416&sec=technology (accessed May 29, 2009).

Robert Lemos. “Cyber attack could bring US military response.” The register. http://www.theregister.co.uk/2009/05/13/us_cyber_attack_response/ (accessed May 29, 2009).

Robert Lemos. “Cyber attack could bring U.S. military response.” Security focus. http://www.securityfocus.com/brief/961/ (accessed May 29, 2009).

Jeffrey Carr. “Projecting Borders into Cyberspace.” Security focus. http://www.securityfocus.com/columnists/500 (accessed May 29, 2009).

“Offensive Operations in Cyberspace.” White Wolf Security. http://www.whitewolfsecurity.com/publications/offensive_ops.php (accessed May 18, 2009).