Lecture 20. Computers in the Wrong Hands: Cyber Hackers, Criminals, and Warriors

Note: in cases I were unable to find the primary source of an image or determine whether or not an image is copyrighted, I have specified the source as "unknown". I will provide full information about images and/or obtain reproduction rights when such information is available to me.

Fig. 1. Cybercriminal. Source: [3].

Introduction

In just half a century from the beginning of the computer industry in the 1950s, computer and information technologies have completely penetrated all aspect of our private and public activities. Our dependence on these technologies is critical which means that sudden collapse of computer infrastructure would immediately result in economic meltdown and endangering our very existence. Shutting down Internet for even a day or two would have devastating effects on global economy and security causing a major, global and long lasting economic and political crisis.

We do understand quite well that computer and information technologies are tools through which social, economic, and even political progress can be achieved. There are some who believe that these technologies contain seeds of new "higher" and more just frameworks of social organization.

We do understand that these technologies can also be molded to produce the opposite effects. Our dependency on cyber-space makes computers both the objects of attack and powerful weapons more destructive than conventional arsenals. Computers used as tools of crime, repression, and destruction can lead to social, economic, and political instability. Computers can help to enslave and destroy everybody who disagrees with some political or religious doctrine.

A rather obvious conclusion from these observations is that these are not computers which are good or evil but rather **us** who use them for good or evil purposes.

This lecture takes a look at computing technologies as tools of crime and cyber-destruction. Other significant and related issues such as computer ethics, privacy, intellectual property, censorship, legislating and policing the Internet, or its commercialization and militarization, are left for future discussions.

Computer crime and criminals: the early years

Computer crime is not easy to define, since such a definition depends upon social and political views, norms, and laws defining "right" and "wrong", "legal" and "illegal". What in one country may be considered a basic human right can be considered a crime against the state in another.

Of course when a person is using a computer to gain an unauthorized access to bank accounts of other people and transfers money from these accounts into his or her own account without leaving much of a trace, then such an activity is criminal. Other instances of computer use are not as clear cut cases of computer abuse, misuse, and crime.

Since a computer criminal is a person who is involved in computer crime activity, computer crime can be committed by an individual, a loose group of hackers, or even a governmental organization involved in an illegal espionage activities.

To make things worse, a public image of (and fascination with) computer crimes is much different when compared to other, more "traditional" forms of robbing banks or disposing of an incriminating evidence. Computer robbers, as their masked predecessors, do rob banks because, obviously, this is where money is supposed to be. But when a robber of a bank is satisfied with just a few thousand dollars after a dengerous work with a crowbar or a gun, computer robbers steal millions of dollars with a single attack while drinking a cup of coffee and to the applause of general public, excited and ready to equate the robbery with some kind of social justice, "beating the system", "getting even", when the computer criminal targets a large corporation.

Romantic image of cyber "Robin Hoods" attacking servers of large corporations and governmental institutions, shutting them down for hours causing a lot of damage is frequently mislead for a fight for a utopian cyber-freedom and against digital forms of control, domination, and oppression. Elusive hacking cultures fuel interests of younger generations of computer users to explore the "dark side" of the Internet.

who was stealing first and what...

In the early years of computing in North America (1950s–1960s) computer crime was not clearly defined in law although it mostly involved stealing computer time. At that time it was a standard practise that programmers were using corporate computers for their own purposes (e.g. writing and playing games, executing small computer jobs) when the computers were idle. The companies knew about and tolerated that practice until things got out of hand and, in some instance, 2/3 of total computer time and storage was used for "private" rather than corporate purposes. The first convictions soon followed but they spoke of computer abuse and misuse rather than crime.

Furthermore, early programmers did not consider sharing programs and programming ideas between themselves as illegal either, perhaps because they were not the ones who paid for the software's development. This would all start to change when companies began to realize that their business critically

depended on computing and when computing expenditures would account for a large chunk of their operational costs. Corporate secrets would start to include not only data but computer software.

By the early 1970s, a large sector of the North American economy was computerized and new forms of computer-related crimes started to appear such as using computers for corporate fraud and theft as well as for sabotage and espionage.

There is no concrete data to show how wide spread the computer crime was since, as it is still true today, companies do not freely report on computer attacks as that could undermine public confidence in them and result in even more serious loses. The only thing that is left from that era are the first research reports on computer crimes and court records in cases when perpetrators were brought to justice.

The 1973 Equity Funding case can serve as example. The Equity Funding computers were used to create 64,000 fake insurance policies (out of the total 97,000). Fake policies were resold bringing 2.1 billion dollars (out of $3.2 billion in total assets). After the scheme fall apart, 22 top managers and auditors were convicted.

first reports on computer crime

In 1971, Stanford Research Institute (SRI) produced a report *Computer-Related Crime and Data Security*

> *that identified threats of computer abuse and misuse. It recommended that computer centers segregate sensitive duties, secure backup of systems and data, and establish physical barriers to unauthorized entry into computer centers.*

Since in the early 1970s, computers were not networked to any large-scale network, the main concerns were about corporate and governmental espionage through illegal access to computers.

Conferences and meetings on the subject of computer abuse and crime have been organized since the early 1970s. One of the earliest public reports on computer abuse entitled *Computer Abuse* was prepared by SRI International

in 1973 (cf. [1]). The purpose of the report was to "alert business and government users of computers–as well as the technological, law, and sociological research communities–about the serious nature, extent, and potential of computer abuse as a growing social problem." [1]

One of the interesting predictions stated in the report was that computer crime would diminish in time as computers and software became increasingly complicated and expensive. Unfortunately, this prediction, as many others concerning future development of computer technologies and their impact on the society, turned out to be false.

First, already at the time of the writing of the 1973 report the first small, easy to use, and inexpensive microcomputers were being shown around the world and soon would give rise to a forceful computer hacker culture. Since 1980s, young hackers were beginning to exercise their microcomputer power to tamper with the established digital social order.

Second, since the beginning of the commercial Internet, powerful organizations funded by corporations and possibly, some governments, have been involved in industrial and military espionage and sabotage using cyberspace. They are well-funded, equipped, and employ individuals with state-of-the-art expertise.

what? Citibank again?

It is now evident that computer crime evolves and will continue to do so at the speed of computer and information technologies' development. As the recent history of Citibank clearly indicates, devastating attacks can now come from any place on the globe.

In 1994, a group of Russian hackers led by Vladimir Levin successfully attacked Citibank and defrauded the bank of (allegedly) $10.7 million by accessing apparently unprotected systems and transferring funds to accounts set up by in various regions of the world. The hacker was brought to justice.

The attacks from East European Internet sites would continue and, as reported by *New York Times News Services* on May 13, 2002, the hackers were dealing with tens of thousands of stolen credit card numbers weekly adding to, approximately, $1 billion in loses a year.

In 2009, Citigroup's Citibank subsidiary was attacked again by cyber-robbers. The attack was detected over the summer of 2009 and, according to some reports, tens of millions of dollars were lost (of course, the information about lost money was denied by the bank).

Fig. 2. Did Russians attack Citygroup? *The Telegraph*, 23 Dec 2009.

It seems that the bank didn't learn its lesson in computer security since two years later, once again, it was hit by a hacker attack. The bank confirmed that some 360,000 North American credit card accounts were affected (hacked!). Customers names, email addresses, contact information, and account numbers were accessed by hackers. To minimize already catastrophic damage, the assured consumers that they wont have to pay for any fraudulent purchases resulting from the attack.

Robin Hoods & artists of the digital underworld

In the 1960s, social philosophers (such as Marshall McLuhan) argued that new media (e.g. television) would transform societies into a global village where "instant information creates involvement in depth." ([1], p. 161)

Thirty years later, the Internet and WWW have created a global cyber village. However, having an unlimited and instant access to information has not created a massive movement of those "involved in depth" for a number of reasons (e.g. over-saturation with unreliable, inconsistent, incomplete, and irrelevant information while significant and reliable information is difficult to access or identify, etc.).

Instead, the Internet has created vast legions of computer hackers and activists (the so-called hacktivists) determined to guard (at all costs) a free and just development of the Web. Others would transform their hacking activities into new forms of individual expression in fine arts, film, and music.

Before we continue, let us clarify some terminology.

In the 1970s and early 1980s, the noun *hacker* was frequently used in reference to a computer hobbyist working hard on some innovative application. Even today, *Thesaurus* defines the noun as "someone proficient at computers, especially a hobbyist."

Since the mid 1980s, we have began to use the noun *hacker* in a different sense: as "a person who gains unauthorized access to data in a system or computer" (see, for instance, *Oxford Dictionary.*) Indeed, the hackers of the

1980s were working hard but on developing and infecting Apple and PC computers with first viruses, causing all sorts of problems for the users.

It would not be until the commercial and public acceptance of the Internet when hackers would start launching devastating attacks on large corporations and organizations. Some hackers were motivated by profit, some were inspired by hacking culture that rewarded on-line hacking with fame. Yet others hacked neither for profit nor for fame but as a form of Internet activism.

We have already seen examples of profit-driven hacking in the previous section. To illustrate hacking as a way of making a name for himself in a hacking world, let us meet a Montreal teenager Michael Calce who in 2000 was going by the hacker name of MafiaBoy.

From the early childhood, MafiaBoy had found computers intoxicating and empowering. On February 8, 2000, he left for school leaving his computer running a program that, apparently, he had downloaded from a file-sharing repository a few days earlier which he "supplemented" with a few URL addresses of companies such as eBay, eTrade, CNN.com, Yahoo!, (then the top search engine company), Dell.com, and Buy.com. His computer initiated an attack that shut down all these sites resulting in several million dollars of lost revenues.

The MafiaBoy's attack was of the highest hacking calibre and was extensively covered in media all over the world. In spite of being identified and caught, he has earned an entry in Wikipedia.com and a prominent position in the top ten "most popular cyber-criminals the world has ever known" (cf. http://www.howiteasy.com).

The Robin Hoods

Fig. 3. One of the images produced by (or in support of) the Anonymous hacker group. Source: well, I won't tell you...

To some hacktivists, the Internet has been the last bastion of freedom worth defending against "oppressive forces" of profit-seeking commerce, censors, and regulators. They have been using Internet itself as a powerful tool to fight for their own vision of Internet freedom.

Since the 1990s, cyber Robin Hoods would attack sites of corporations and governmental institutions whose practices were deemed unfair or unethical such as collecting and selling information about site users (without users' consent) to corporate and government agencies.

Robin Hoods do not seek profits; they want free and fair Internet for everybody and at all costs. Robin Hoods do attack; they target large corporations, religious, social, and political organizations. They launch attacks to demonstrate and assert their role as guardians of freedom and justice.

On, August 17, 1996, something was wrong with the home page of the United States Department of Justice (DOJ). Instead of the department's logo and name, the page showed a Nazi swastika with a text "United States Department of Injustice."

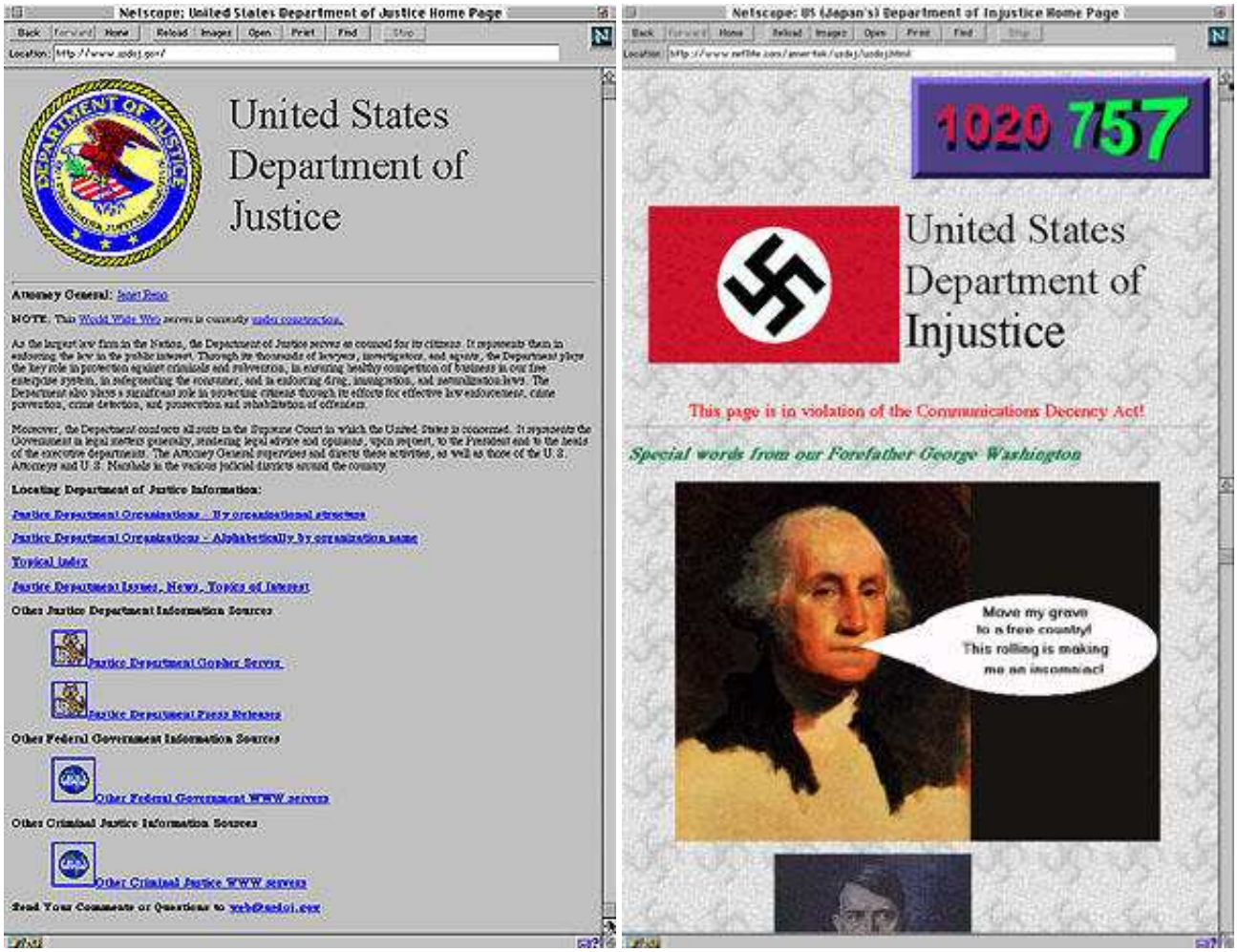

Fig. 4. The 1996 home page of the United States Department of Justice (left) and its hacked August 17th replacement (right). (Source: unknown.

An unknown group of cyber Robin Hoods hacked and changed the contents of DOJ's home page in protest of the current administration's attempt to regulate the Internet.

Similar attacks occurred on home pages of CIA, *New York Times*, and other institutions.

Electronic activism practised in the West in the 1980s and 1990s also included large organizations. PeaceNet (founded in San Francisco in 1986) and GreenNet (founded in London, UK, in 1985) are two examples of influential, international, computer communication networks created to support autonomous social and political activism. (For more information on these organizations see [12] and [13].)

Fig. 6. Anonymous hactivists protesting the Church of Scientology. Source: unknown.

Perhaps the most publicized group of hacktivists is the Anonymous hacker group created on the imageboard 4chan in 2003. Since 2008, a loose at first Anonymous collective of think-a-likes has became political and ready to act.

This is our world now. We exist without nationality, without religious bias. We have the right to not be surveilled, not be stalked, and not be used for profit. We have the right to not live as slaves.

We are anonymous

We are legion

We do not forgive

We do not forget

Expect us

reads a short manifesto used, for instance, during the announcement of an attack on Facebook on 2011.

Fig. 5. We are anonymous. We are legion. Image by ipott.

The group first attracted much attention with an attack on the Church of Scientology in 2008.

> *Hello, Leaders of Scientology. We are Anonymous.*
>
> *Over the years, we have been watching you. Your campaigns of misinformation; your suppression of dissent; your litigious nature, all of these things have caught our eye.*

"Anonymous is an idea, a global protest movement, by activists on the streets and by hackers in the network," the hackers said through the Twitter account. "Anyone can be Anonymous, because we are an idea without leaders who defend freedom and promote free knowledge." (quoted after [8])

Since the 2008 attack on the Church of Scientology, Anonymous carried out hundreds of increasingly bold strikes against corporate and governmental organizations (such as law enforcement agencies, Internet security companies, and opponents of the whistle-blower site WikiLeaks) as well as conventional protests of masked individuals worldwide.

In August 2011, the group announced its attack on Facebook to take place on November 5th.

> *Attention citizens of the world,*
>
> *We wish to get your attention, hoping you heed the warnings as follows:*
>
> *Your medium of communication you all so dearly adore will be destroyed. If you are a willing hacktivist or a guy who just wants to protect the freedom of information then join the cause and kill facebook for the sake of your own privacy.*
> *...*
> *Think for a while and prepare for a day that will go down in history. November 5 2011, ... Engaged.*

In the end, Facebook survived. In spite of the arrests of several key members of Anonymous in 2011 and 2012, the organization continues to hit one significant target after another across the globe. (See also [14])

from hacking to creating

The era of computer hobbyists ended in mid 1980s but the excitement about computers and computing did not diminish, it only started to grow stronger when new forms of computing interaction and computer-based subcultures begun to emerge.

Among the new (and pre-WWW) activities, BBS systems attracted most attention in both North America and Europe. Since their introduction in the late 1970s, they almost instantly generated virtual communities where cyberkidz were hanging around and exploring new possibilities, some legal, some not, and some too new to be classified in one way or another.

BBS systems had strong impact on the formation and development of diverse sub-cultures, impacting hundreds of thousands of young computer enthusiasts. European Demoscene of the 1980s and 1990s can serve as an example, with its roots in illegal hacking and code breaking and its flowers reaching new forms of artistic expression in the areas of computer graphics, film, and music.

Fig. 7. Aura for Laura by Soopadoopa. Source: http://meonline.hu/archivum/demoscene-kozosseg

Demoscene started in the early 1980s in Europe by game "crackers" who wanted to gain access and copy commercial computer games. After a game was successfully cracked, the software-pirate would then insert an additional code that displayed a special page informing a game player about the identity (assumed, of course) of the game cracker who "freed" the land of gamers from the necessity of paying for this particular game. These introductory pages, called demos, would feature interesting graphics and electronic music.

Soon, the designing and showing the demos would become more important activity than game cracking itself. Specially organized demoparties could bring hundreds of computer artists to show their deomscene art.

Fig. 8. Assembly 2002 Demoparty, August 1, 2002, Finland. Photograph by Joneikifi. Source:
http://en.wikipedia.org/wiki/File:Assembly_demo_party_2002_panorama.jpg

Cyber warfare

In the 21st century, using computers to steal credit card numbers or insurance records, which was state-of-the-art hacking activities of the 1980s, is left to young hackers as home assignments in their progress through the ranks of cyber-pirating. Another type of homework assignment is the design and launch of a new computer virus or a worm.

Some experts estimate that, at present, there are hundreds of thousands of malicious software (or malware) circulating the Web in search for new targets (i.e. computers) to gain unauthorized access and either disrupt computers' operation, gather, modify, or destroy information, and broadcast information and software.

But there is more. Some countries use their cyber-capabilities to penetrate, exploit, and attack computer installations and networks owned by other organizations and countries. On November 24, 2014, Sony Pictures Entertainment was hacked by the hacker group "Guardians of Peace" and, as a result, confidential data regarding the company's operations was released. "Guardians of Peace" demanded that the release of a controversial film *The Interview* by Sony was cancelled. Intelligence experts point their finger at North Korea.

Many countries, including Canada, are developing advanced cyber warfare capabilities. In February 2015, *The New York Times* reported that the Chinese army is hacking into Americas most sensitive computer networks from a complex located outside Shanghai. In March 2015, the documents apparently leaked from the National Security Agency by Edward Snowden, contain claims claims that even Canada could perform "computer network exploitation" and "computer network attack" operations. (Information quoted after http://gizmodo.com/leaked-documents-reveal-canadas-advanced-cyber-warfare-1693054429)

While until 1990s cyber warfare was mostly the subject of sci-fi fantasy, in the second decade of this century it has emerged as one of the most significant, global, and dangerous applications of computer and information technologies. Since almost all aspects of military and governmental activities are computer-based (from information infrastructure to strategic planning and operation) it is inevitable that future international conflicts will be initiated, conducted, and resolved in the cyber-field to a vary large extent. Cyber attacks on Georgia by Russia during the Russo-Georgian conflict in 2008 can serve as an example. Let us look at a few more.

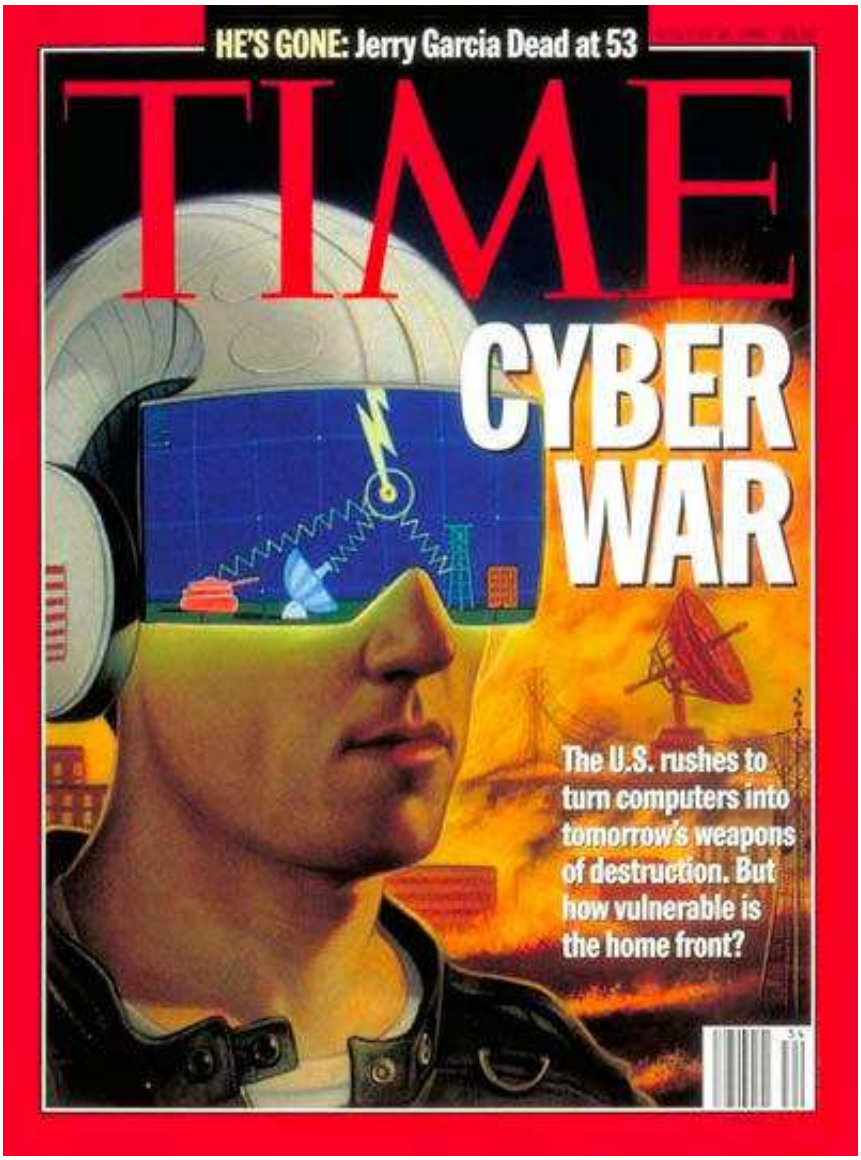

Fig. 9. The cover of August 21, 1995 *Time* magazine.

One of the earliest large-scale cyber-attacks on American governmental agencies begun in early 1998 and continued into the next year. Computer hackers traced to the Russian Academy of Sciences successfully attacked computer systems at the Pentagon, NASA, Energy Department, several universities, and research labs (see [10, 11]). The attackers managed to obtain

vast amounts of data, possibly including classified and most sensitive data. According to Front Line, this the attack, named Moonlight Maze, was

> a highly classified incident [named Moonlight Maze] in which ... the invaders were systematically marauding through tens of thousands of files – including maps of military installations, troop configurations and military hardware designs. The Defense Department traced the trail back to a mainframe computer in the former Soviet Union but the sponsor of the attacks is unknown and Russia denies any involvement. [As of 20003,] Moonlight Maze is still being actively investigated by U.S. intelligence. [See [10]]

Fig. 10. Are these soldiers playing computer games during a study break? Source: http://coalporter.blogspot.com/2011/01/governments-need-to-plan-for-cyber.html U.S. soldiers on virtual missions (IMAGE U.S. Army)

STUXNET: According to *New York Times* January 15, 2011 article, it appears that a sophisticated computer worm called Stuxnet was deployed as a result of joint American and Israeli effort to undermine Iran's nuclear program. Stuxnet, launched in 2010, was "a destructive program that appears to have wiped out roughly a fifth of Irans nuclear centrifuges and helped delay, though not destroy, Tehrans ability to make its first nuclear arms." (see [2]).

When Stuxnet was deployed, its first objective was to navigate through networks (without affecting anything on its way, only collecting information) and to arrive at a specific target computer in Iran. That computer was in control of a very specific process of enriching uranium. When there, Stuxnet rewrote a portion of the process-controlling software to cripple the process itself. And, of course, it did so without being detected for some time.

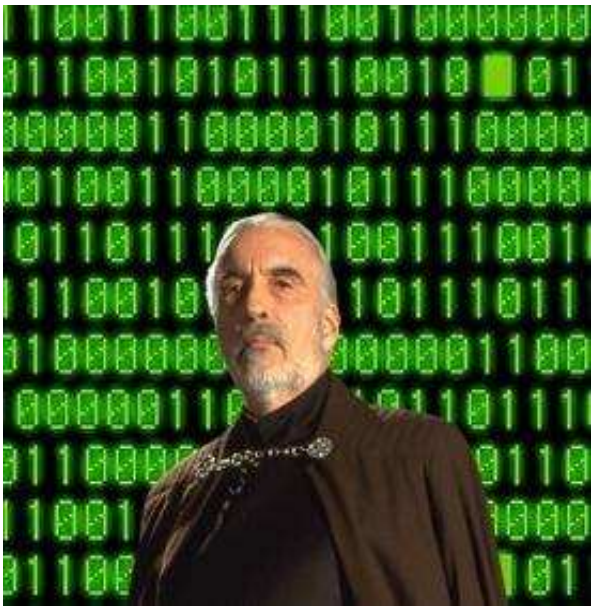

Fig. 11. Dooku worm. Source: image from
http://www.starwars.com/explore/encyclopedia/characters/asajjventress
superimposed on image from unknown source.

Stuxnet represents a malware of a new generation, more sophisticated than any other cyberwar software ever deployed, one that signals "the beginning of a new era of warfare that targets the enemys infrastructure instead of the populace at large." [3]

Stuxnet is not the only malware of its kind. A Stuxnet cyber-relative by the name of Duqu (does the name sound familiar? as in "Count Dooku", one of Star Wars villains?) Duqu was most likely created to gathers information to guide future Stuxnet-like attacks.

The UK newspaper *The Guardian* reported on 17 January 2011 that "the United States was preparing for cyber conflict and had launched its own military cyber command. The UK in October 2010 had rated cyber attacks as one of the top external threats, promising to spend an extra 650 million pounds (one billion US dollars) on the issue."

O Canada

How does Canada compare to other countries in terms of readiness for possible cyber strikes? Events from the last two years alone indicate that our country is not ready at all. I have already mentioned recent (March 2015) reports on the Canadian involvement in the development of advanced cyber warfare capabilities of deployment of such cyber-tools. Let us briefly review other significant cyber-attacks that occurred during this decade.

In Fall 2010, the Government of Canada suffered cyber attacks by foreign hackers using IP addresses from China. The hackers infiltrated computers in the Canadian government's Finance Department, Treasury Board, and Defense Research and Development Canada, stealing highly classified federal information.

The attacks resulted in the government cutting off Internet access in the departments affected when the attacks were discovered in January 2011 (cf. [6])

Cyber-forensics gurus pointed their fingers at a large-scale cyber spying network dabbed the GhostNet and traced to People's Republic of China. The GhostNet, discovered in March 2009, was going after major political and eco-

nomic targets in several countries, including Canada. The network is elusive and no definite evidence has been provided to link GhostNet to either the Chinese government or other national and international organizations.

That's Canadian government. And how about Canadian corporate world, are our companies ready to defend themselves from cyber-attacks? The answer seems to be no, again.

The GhostNet attacked Canadian computers again in November 2011, this time targeting prominent Bay Street law firms and other companies to get insider information on an attempted $38-billion takeover of Potash Corporation of Saskatchewan.

Both attacks are examples of the most serious cases of political and economic espionage to date. That's why cyber-defense occupies the central place in policy planning all over the world.

In 2014, the computer network at National Research Council (NRC) was the subject of a highly sophisticated cyber-attack from China. This, of course, was not the first time that a Canadian governmental or industrial organization fell victim to a cyberattack attributed to servers located in China. The attack on NRC was the first time when the Canadian government unequivocally blamed China for its sponsorship.

What's next? Are there malware installed, undetected, and dormant on sensitive networks, waiting for signals to awake them to do their dirty job? Stay tuned by following the University of Toronto-based *The Information Warfare Monitor*,
http://www.infowar-monitor.net/

References

1. D.B. Parker, The Dark Side of Computing: SRI International and the Study of Computer Crime, *Annals of the History of Computing.* vol. 29, no. 1 (2007), pp. 3–15.

2 W.J. Broad, J. Markoff, and D.E. Sanger, Israeli Test on Worm Called Crucial in Iran Nuclear Delay, *The New York Times*, January 15, 2011.

3 S.C. Webster, U.S. officials: Stuxnet launched the next generation of warfare. *The Raw Story*, March 5, 2012. http://www.rawstory.com/rs/2012/03/05/u-s-officials-stuxnet-launched-the-next-generation-of-warfare

4 M.J. Schwartz, 3 Lessons Learned From Duqu Malware, *InformationWeek*, October 20, 2011, http://www.informationweek.com/news/security/cybercrime/231901299

5 J. Markoff, Vast Spy System Loots Computers in 103 Countries, *The New York Times*, March 28, 2009, http://www.nytimes.com/2009/03/29/technology/29spy.html?_r=1

6 G. Weston, Foreign hackers attack Canadian government Computer systems at 3 key departments penetrated, *CBC News*, Feb 16, 2011 http://www.cbc.ca/news/politics/story/2011/02/16/pol-weston-hacking.html

7 K. Elfimov, Brief History of Russian Speccy Demoscene and the story of Inward, 2008, http://www.mustekala.info/node/921

8 N. Perlroth and J. Markoff, In Attack on Vatican Web Site, a Glimpse of Hackers Tactics, *The New York Times*, February 26, 2012.

9 S. Levy, *Hackers, heroes of the computer revolution*, O'Reilly, 2010.

10 "Cyber War!", PBS Frontline, 24 April 2003. See http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar.

11 G. Vistica, "We're in the middle of a cyberwar", *Newsweek*, 20 September 1999, p. 52.

12 John D.H. Downing, Computers for Political Change: PeaceNet and Public Data Access, *Journal of Communication* 39, no. 3 (Summer 1989), pp. 154-62.

13 GreenNet's history page on http://www.gn.apc.org/about/history, last accessed December 2013.

14 Kim Zetter. Did leader's arrest kill Anonymous? *Wired*, 10 June, 2014. See also http://www.wired.co.uk/news/archive/2014-06/10/anonymous-sabu