International Telecommunication Union

STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS

BULGARIAN ACADEMY OF SCIENCES

NATIONAL LABORATORY OF COMPUTER VIROLOGY

REGIONAL CYBERSECURITY FORUM

7-9 Oct 2008, Sofia

MODERN TRENDS IN THE CYBER ATTACKS AGAINST THE CRITICAL INFORMATION INFRASTRUCTURE

EUGENE NICKOLOV,
PROFESSOR, DOCTOR OF MATHEMATICAL SCIENCES,
CEO, NATIONAL LABORATORY OF COMPUTER VIROLOGY

01. THE CURRENT DEFINITIONS OF THE FUNDAMENTAL TERMS IN THIS FIELD.

A. Cyber-warfare.

B. Infrastructure.

A. CYBER-WARFARE. 01

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

CYBER ATTACK == **CYBER-WARFARE**

A. Cyber-warfare. Also known as *cybernetic war* [1], or *cyberwar* is the use of computers and the Internet in conducting warfare in cyberspace [2].

[1] Jonathan V. Post, "Cybernetic War," *Omni,* May 1979, pp.44-104, reprinted *The Omni Book of Computers & Robots*, Zebra Books, ISBN 0-8217-1276

[2] DOD, Cyberspace, http://www.dtic.mil/doctrine/jel/doddict/data/c/01473.html

1. TYPES OF ATTACKS. 01

There are several methods of attack in cyber-warfare, this list is ranked in order of mildest to most severe.

1.1 CYBER ESPIONAGE.

Cyber espionage is the act or practice of obtaining secrets (sensitive, proprietary of classified information) from individuals, competitors, rivals, groups, governments and enemies for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers.

1. TYPES OF ATTACKS. 01

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

1.2 WEB VANDALISM.

Attacks that deface web pages, or denial-of-service attacks. This is normally swiftly combated and of little harm.

1.3 PROPAGANDA.

Political messages can be spread through or to anyone with access to the internet.

1.4 GATHERING DATA.

Classified information that is not handled securely can be intercepted and even modified,
making espionage possible from the other side of the world.

1. TYPES OF ATTACKS. 01

1.5 DISTRIBUTED DENIAL-OF-SERVICE ATTACKS.

Large numbers of computers in one country launch a DoS attack against systems in another country.

1.6 EQUIPMENT DISRUPTION.

Military activities that use computers and satellites for co-ordination are at risk from this type of attack. Orders and communications can be intercepted or replaced, putting soldiers at risk.

1.7 ATTACKING CRITICAL INFRASTRUCTURE.

Power, water, fuel, communications, commercial and transportation are all vulnerable to a cyber attack.

1.8 COMPROMISED COUNTERFEIT HARDWARE.

Common hardware used in computers and networks that have malicious software hidden inside the software, firmware or even the microprocessors.

2. REPORTED THREATS. 01

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

2.1 The Internet security company McAfee stated in their 2007 annual report that approximately 120 countries have been developing ways to use the Internet as a weapon and the targets are financial markets, government computer systems and utilities.

2. REPORTED THREATS. 01

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

2.2 In activities reminiscent of the Cold War, which caused countries to engage in clandestine activities, intelligence agencies are routinely testing networks looking for weaknesses. These techniques for probing weaknesses in the internet and global networks are growing more sophisticated every year. [3]

[3] Griffiths Peter, "World faces "cyber cold war" threat", Reuters, http://ca.news.yahoo.com/s/reuters/071129/tecnology/tech_britain_internet_col

2. REPORTED THREATS. 01

2.3 Jeff Green the senior vice president of McAfee Avert Labs was quoted as saying "Cybercrime is now a global issue. It has evolved significantly and is no longer just a threat to industry and individuals but increasingly to national security." They predicted that future attacks will be even more sophisticated. "Attacks have progressed from initial curiosity probes to well-funded and well-organized operations for political, military, economic and technical espionage." [4]

[4] "Cyber Crime: A 24/7 Global Battle", Mcafee, http://www.mcafee.com/us/research/criminology_report/default.html

2. REPORTED THREATS. 01

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

2.4 The report from McAfee says that China is at the forefront of the cyber war. China has been accused of cyber-attacks on India and Germany and the United States. China denies knowledge of these attacks. Arguments have been expressed regarding China's involvement indicating, in the methods of computer Hackers who use zombie computers, it only indicates that China has the most amount of computers that are vulnerable to be controlled. [5]

[5] "China 'has 75M zombie computers' in U.S., http://www.upi.com/International_Security/Emerging_Threats/Briefing/2007/09/17/china_has_75m_zombie_computers_in_us/7394/

2. REPORTED THREATS. 01

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

2.5 In April 2007, Estonia came under cyber-attack in the wake of relocation of the Bronze Soldier of Tallinn. Estonian authorities, including Estonian Foreign Minister Urmas Paet accused the Kremlin of direct involvement in the cyberattacks [6]. Estonia's defense minister later admitted he had no evidence linking cyber attacks to Russian authorities [7].

[6] Estonia accuses Russia of 'cyber attack',
http://www.csmonitor.com/2007/0517/p99s01-duts.html

[7] Estonia has no evidence of Kremlin involvement in cyber attacks,
http://en.rian.ru/world/20070906/76959190.html

3. KNOWN ATTACKS. 01

3.1 The United States had come under attack from computers and computer networks situated in China and Russia. See *Titan Rain* and *Moonlight Maze* [8]. It is not clear if attackers originated in those countries or used compromised computers there. [8a]

[8] Jim Wolf,"U.S. Air Force prepares to fight in cyberspace", Reuters, November 3, 2006,
http://en.wikipedia.org/wiki/Reuters

[8a] Cyberwarfare reference materials,
http://staff.washington.edu/dittrich/cyberwarfare.html

3. KNOWN ATTACKS. 01

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

3.2 On May 17, 2007 Estonia came under cyber attack. The Estonian parliament, ministries, banks, and media were targeted. [9]

[9] Ian Traynor, 'Russia accused of unleashing cyber war to disable Estonia, http://www.guardian.co.uk/russia/article/0,,2081438,00.html

3.3 On first week of September 2007, The Pentagon and various French, German and British government computers were attacked by hackers of Chinese origin. The Chinese government denies any involvement. [9a]

[9a] Chinese Official Accuses Nations of Hacking, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/12/AR2007091200791.html

3. KNOWN ATTACKS. 01

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

3.4 On 14 December 2007 the website of the Kyrgyz Central Election Commission was defaced during its election. The message left on the website read "This site has been hacked by Dream of Estonian organization". During the election campaigns and riots preceding the election, there were cases of Denial-of-service attacks against the Kyrgyz ISPs. [10]

[10] Website of Kyrgyz Central Election Commission hacked by Estonian hackers, http://www.regnum.ru/english/932354.html

3. KNOWN ATTACKS. 01

3.5 In the second week of April hackers hacked the Indian MEA computers. [10a]

[10a] MEA Computer Network Hacked,
http://www.india-server.com/news/mea-computer-network-hacked-172.html

3.6 Georgia fell under cyberattacks during the 2008 South Ossetia War. [10b]

[10b] Cyber attacks became part of Russia-Georgia war,
http://www.computerweekly.com/Articles/2008/08/13/231812/cyberattacks-became-part-of-russia-georgia-war.htm

4. CYBER COUNTERINTELLIGENCE. 01

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

4.1 Cyber counterintelligence are measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions. [11]

[11] DOD - Cyber Counterintelligence, http://www.dtic.mil/doctrine/jel/doddict/data/c/01472.html

4. CYBER COUNTERINTELLIGENCE. 01

4.2 The intelligence community is coming to grips with the challenge of cyber warfare intelligence. Much of the advanced infrastructure used in traditional warfare, like satellite imagery, is ineffective in the realm of cyber. New techniques and technologies are required for intelligence agencies to operate in this field. [11a]

[11a] World Wide War 3.0,
http://www.the-diplomat.com/article.aspx?aeid=3301

4. CYBER COUNTERINTELLIGENCE. 01

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

4.3 In May 2008, U.S. Strategic Command's - Col. Gary McAlum chief of staff - of the command's Joint Task Force for Global Network Operations, quoted approvingly from a new intelligence report by Kevin Coleman [11b] of the Technolytics Institute that stated China aims to achieve global "electronic dominance." This report was not released to the public, however it was clear that cyber warfare intelligence was being collected and used to assess the cyber weapons capabilities of each country.

[11b] About: Kevin G. Coleman is an international security and intelligence consultant with Technolytics and has regularly featured articles in DefenseTech.org and International Intelligence Magazine covering homeland security, terrorism, security and intelligence worldwide. For six years he served as a science and technology advisor to the nation's leading research and development center that service the U.S. Department of Defense, Department of Homeland Security and the Intelligence Community. Additionally, he testified before Congress on Cyber Security and Privacy, www.technolytics.com,

http://www.spy-ops.com/Web/Protecting_Your_Computer_in_the_Face_of_Cyber_Attack.pdf

B. INFRASTRUCTURE. 01

INFRASTRUCTURE ==

CRITICAL INFRASTRUCTURE ==

CRITICAL INFORMATION INFRASTRUCTURE

1. TYPE OF INFRASTRUCTURE.

01

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

1.1 TECHNICAL DEFINITION.

Typically refers to the technical structures that support a society, such as roads, water supply, wastewater, power grids, flood management systems, communications (internet, phone lines, broadcasting), and so forth. In the past, these systems have typically been owned and managed by local or central governments. These various elements may collectively be termed civil infrastructure, municipal infrastructure, or simply public works, although they may be developed and operated as private-sector or government enterprises.

1. TYPE OF INFRASTRUCTURE.

01

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

1.2 GENERIC DEFINITION.

A more generic definition of infrastructure is the network of assets "where the system as a whole is intended to be maintained indefinitely at a specified standard of service by the continuing replacement and refurbishment of its components."[12]

[12] Association of Local Government Engineers New Zealand, "Infrastructure Asset Management Manual", June 1998 - Edition 1.1, http://www.nams.org.nz/Home

1. TYPE OF INFRASTRUCTURE.

1.3 INFORMATION TECHNOLOGIES (IT) DEFINITION.

Infrastructure may refer to information technology, informal and formal channels of communication, software development tools, political and social networks, or beliefs held by members of particular groups. Still underlying these more general uses is the concept that infrastructure provides organizing structure and support for the system or organization it serves, whether it is a city, a nation, or a corporation. Economically, infrastructure could be seen to be the structural elements of an economy which allow for production of goods and services without themselves being part of the production process, e.g. roads allow the transport of raw materials and finished products.

2. CRITICAL INFRASTRUCTURE. 01

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

2.1 The term "critical infrastructure" has been widely adopted to distinguish those infrastructure elements that, if significantly damaged or destroyed, would cause serious disruption of the dependent system or organization. Storm, flood, or earthquake damage leading to loss of certain transportation routes in a city (for example, bridges crossing a river), could make it impossible for people to evacuate and for emergency services to operate; these routes would be deemed critical infrastructure. Similarly, an on-line booking system might be critical infrastructure for an airline.

2. CRITICAL INFRASTRUCTURE. 01

2.2 According to etymology online [13], the word infrastructure has been around since 1927 and meant: The installations that form the basis for any operation or system. Originally in a military sense. The word is a combination of "infra", meaning "below" and "structure".

[13] Online Etymology Dictionary, Douglas Harper, Historian, http://dictionary.reference.com/browse/infrastructure

2. CRITICAL INFRASTRUCTURE. 01

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

2.3 The term came to prominence in the United States in the 1980s following the publication of America in Ruins (Choate and Walter, 1981), which initiated a public-policy discussion of the nation's "infrastructure crisis", purported to be caused by decades of inadequate investment and poor maintenance of public works.

2. CRITICAL INFRASTRUCTURE. 01

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

2.4 That public-policy discussion was hampered by lack of a precise definition for infrastructure. The U.S. National Research Council committee cited Senator Stafford, who commented at hearings before the Subcommittee on Water Resources, Transportation, and Infrastructure; Committee on Environment and Public Works; that "probably the word infrastructure means different things to different people." The NRC panel then sought to rectify the situation by adopting the term "public works infrastructure", referring to "...both specific functional modes - highways, streets, roads, and bridges; mass transit; airports and airways; water supply and water resources; wastewater management; solid-waste treatment and disposal; electric power generation and transmission; telecommunications; and hazardous waste management - and the combined system these modal elements comprise.

2. CRITICAL INFRASTRUCTURE. 01

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

2.5 A comprehension of infrastructure spans not only these public works facilities, but also the operating procedures, management practices, and development policies that interact together with societal demand and the physical world to facilitate the transport of people and goods, provision of water for drinking and a variety of other uses, safe disposal of society's waste products, provision of energy where it is needed, and transmission of information within and between communities." [14]

[14] Infrastructure for the 21st Century, Washington, D.C., National Academy Press, 1987

2.6 In subsequent years, the word has grown in popularity and been applied with increasing generality to suggest the internal framework discernible in any technology system or business organization.

02. THE CHANGES FOR THE LAST FEW YEARS IN THE ATTACKING INSTRUMENTS.

A. Malicious Software.

B. Grayware.

1. DEFINITION. 02

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

1.1 Malware, a portmanteau word from the words malicious and software, is software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. [15]

[15] http://www.microsoft.com/technet/security/alerts/info/malware.mspx

1.2 Many computer users are unfamiliar with the term, and often use "computer virus" for all types of malware, including true viruses.

1. DEFINITION. 02

1.3 Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, most rootkits, spyware, dishonest adware, crimeware and other malicious and unwanted software. In law, malware is sometimes known as a computer contaminant, for instance in the legal codes of several American states, including California and West Virginia. [16] [17]

[16] National Conference of State Legislatures Virus/Contaminant/Destructive Transmission Statutes by State, http://www.ncsl.org/programs/lis/cip/viruslaws.htm

[17] jcots.state.va.us/2005%20Content/pdf/Computer%20Contamination%20Bill.pdf [§18.2-152.4:1 Penalty for Computer Contamination

1.4 Malware is not the same as defective software, that is, software which has a legitimate purpose but contains harmful bugs.

1.5 Preliminary results from Symantec sensors published in 2008 suggested that "the release rate of malicious code and other unwanted programs may be exceeding that of legitimate software applications." [18]

[18] "Symantec Internet Security Threat Report, Trends for July-December 2007 (Executive Summary),
http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf

1.6 According to F-Secure, "As much malware [was] produced in 2007 as in the previous 20 years altogether." [19]

[19] F-Secure Corporation (December 4, 2007), "F-Secure Reports Amount of Malware Grew by 100% during 2007, http://www.f-secure.com/f-secure/pressroom/news/fs_news_20071204_1_eng.html

1.7 Malware's most common pathway from criminals to users is through the Internet, by email and the World Wide Web. [20]

[20] "F-Secure Quarterly Security Wrap-up for the first quarter of 2008, http://www.f-secure.com/f-secure/pressroom/news/fsnews_20080331_1_eng.html

2. COMPUTER VIRUSES AND WORMS. 02

2.1 The best-known types of malware, viruses and worms, are known for the manner in which they spread, rather than any other particular behavior.

2.2 The term computer virus is used for a program which has infected some executable software and which causes that software, when run, to spread the virus to other executable software. Viruses may also contain a payload which performs other actions, often malicious.

2.3 A worm, on the other hand, is a program which actively transmits itself over a network to infect other computers. It too may carry a payload.

2. COMPUTER VIRUSES AND WORMS. 02

2.4 These definitions lead to the observation that a virus requires user intervention to spread, whereas a worm spreads automatically. Using this distinction, infections transmitted by email or Microsoft Word documents, which rely on the recipient opening a file or email to infect the system, would be classified as viruses rather than worms.

2.5 Some writers in the trade and popular press appear to misunderstand this distinction, and use the terms interchangeably.

2. COMPUTER VIRUSES AND WORMS. 02

2.6 Before Internet access became widespread, viruses spread on personal computers by infecting programs or the executable boot sectors of floppy disks. By inserting a copy of itself into the machine code instructions in these executables, a virus causes itself to be run whenever the program is run or the disk is booted. Early computer viruses were written for the Apple II and Macintosh, but they became more widespread with the dominance of the IBM PC and MS-DOS system. Executable-infecting viruses are dependent on users exchanging software or boot floppies, so they spread heavily in computer hobbyist circles.

2. COMPUTER VIRUSES AND WORMS. 02

2.7 The first worms, network-borne infectious programs, originated not on personal computers, but on multitasking Unix systems. The first well-known worm was the Internet Worm of 1988, which infected SunOS and VAX BSD systems. Unlike a virus, this worm did not insert itself into other programs. Instead, it exploited security holes in network server programs and started itself running as a separate process. This same behavior is used by today's worms as well.

2. COMPUTER VIRUSES AND WORMS. 02

2.8 With the rise of the Microsoft Windows platform in the 1990s, and the flexible macro systems of its applications, it became possible to write infectious code in the macro language of Microsoft Word and similar programs. These macro viruses infect documents and templates rather than applications, but rely on the fact that macros in a Word document are a form of executable code.

2. COMPUTER VIRUSES AND WORMS. 02

2.9 Today, worms are most commonly written for the Windows OS, although a small number are also written for Linux and Unix systems. Worms today work in the same basic way as 1988's Internet Worm: they scan the network for computers with vulnerable network services, break in to those computers, and copy themselves over. Worm outbreaks have become a cyclical plague for both home users and businesses, eclipsed recently in terms of damage by spyware.

3.1 TROJAN HORSES.

For a malicious program to accomplish its goals, it must be able to do so without being shut down, or deleted by the user or administrator of the computer it's running on. Concealment can also help get the malware installed in the first place. When a malicious program is disguised as something innocuous or desirable, users may be tempted to install it without knowing what it does. This is the technique of the Trojan horse or trojan.

3. TROJAN HORSES, ROOTKITS, AND BACKDOORS. 02

3.2 Broadly speaking, a Trojan horse is any program that invites the user to run it, but conceals a harmful or malicious payload. The payload may take effect immediately and can lead to many undesirable effects, such as deleting all the user's files, or more commonly it may install further harmful software into the user's system to serve the creator's longer-term goals. Trojan horses known as droppers are used to start off a worm outbreak, by injecting the worm into users' local networks.

3.3 One of the most common ways that spyware is distributed is as a Trojan horse, bundled with a piece of desirable software that the user downloads from the Internet. When the user installs the software, the spyware is installed alongside. Spyware authors who attempt to act in a legal fashion may include an end-user license agreement which states the behavior of the spyware in loose terms, and which the users are unlikely to read or understand.

3.4 ROOTKITS.

Once a malicious program is installed on a system, it is often useful to the creator if it stays concealed. The same is true when a human attacker breaks into a computer directly. Techniques known as rootkits allow this concealment, by modifying the host operating system so that the malware is hidden from the user. Rootkits can prevent a malicious process from being visible in the system's list of processes, or keep its files from being read. Originally, a rootkit was a set of tools installed by a human attacker on a Unix system where the attacker had gained administrator (root) access. Today, the term is used more generally for concealment routines in a malicious program.

3.5 Some malicious programs contain routines to defend against removal: not merely to hide themselves, but to repel attempts to remove them. An early example of this behavior is recorded in the Jargon File tale of a pair of programs infesting a Xerox CP-V timesharing system: Each ghost-job would detect the fact that the other had been killed, and would start a new copy of the recently slain program within a few milliseconds. The only way to kill both ghosts was to kill them simultaneously (very difficult) or to deliberately crash the system. [21]

[21] http://catb.org/jargon/html/meaning-of-hack.html

3. TROJAN HORSES, ROOTKITS, AND BACKDOORS. 02

3.6 Similar techniques are used by some modern malware, wherein the malware starts a number of processes which monitor one another and restart any process which is killed off by the operator.

3.7 BACKDOORS.

A backdoor is a method of bypassing normal authentication procedures. Once a system has been compromised (by one of the above methods, or in some other way), one or more backdoors may be installed, in order to allow the attacker access in the future.

3.8 The idea has often been suggested that computer manufacturers preinstall backdoors on their systems to provide technical support for customers, but this has never been reliably verified.

3.9 Crackers typically use backdoors to secure remote access to a computer, while attempting to remain hidden from casual inspection. To install backdoors crackers may use Trojan horses, worms, or other methods.

4. MALWARE FOR PROFIT: SPYWARE, BOTNETS, KEYSTROKE LOGGERS, AND DIALERS. 02

4.1 During the 1980s and 1990s, it was usually taken for granted that malicious programs were created as a form of vandalism or prank (although some viruses were spread only to discourage users from illegal software exchange.) More recently, the greater share of malware programs have been written with a financial or profit motive in mind. This can be taken as the malware authors' choice to monetize their control over infected systems: to turn that control into a source of revenue.

4. MALWARE FOR PROFIT: SPYWARE, BOTNETS, KEYSTROKE LOGGERS, AND DIALERS. 02

4.2 Since 2003 or so, the most costly form of malware in terms of time and money spent in recovery has been the broad category known as spyware.[citation needed] Spyware programs are commercially produced for the purpose of gathering information about computer users, showing them pop-up ads, or altering web-browser behavior for the financial benefit of the spyware creator. For instance, some spyware programs redirect search engine results to paid advertisements. Others, often called "stealware" by the media, overwrite affiliate marketing codes so that revenue goes to the spyware creator rather than the intended recipient.

4. MALWARE FOR PROFIT: SPYWARE, BOTNETS, KEYSTROKE LOGGERS, AND DIALERS. 02

4.3 Spyware programs are sometimes installed as Trojan horses of one sort or another. They differ in that their creators present themselves openly as businesses, for instance by selling advertising space on the pop-ups created by the malware. Most such programs present the user with an end-user license agreement which purportedly protects the creator from prosecution under computer contaminant laws. However, spyware EULAs have not yet been upheld in court.

4. MALWARE FOR PROFIT: SPYWARE, BOTNETS, KEYSTROKE LOGGERS, AND DIALERS. 02

4.4 Another way that financially-motivated malware creators can profit from their infections is to directly use the infected computers to do work for the creator. Spammer viruses, such as the Sobig and Mydoom virus families, are commissioned by e-mail spam gangs. The infected computers are used as proxies to send out spam messages. The advantage to spammers of using infected computers is that they are available in large supply (thanks to the virus) and they provide anonymity, protecting the spammer from prosecution. Spammers have also used infected PCs to target anti-spam organizations with distributed denial-of-service attacks.

4. MALWARE FOR PROFIT: SPYWARE, BOTNETS, KEYSTROKE LOGGERS, AND DIALERS. 02

4.5 In order to coordinate the activity of many infected computers, attackers have used coordinating systems known as botnets. In a botnet, the malware or malbot logs in to an Internet Relay Chat channel or other chat system. The attacker can then give instructions to all the infected systems simultaneously. Botnets can also be used to push upgraded malware to the infected systems, keeping them resistant to anti-virus software or other security measures.

4. MALWARE FOR PROFIT: SPYWARE, BOTNETS, KEYSTROKE LOGGERS, AND DIALERS. 02

4.6 Lastly, it is possible for a malware creator to profit by simply stealing from the person whose computer is infected. Some malware programs install a key logger, which copies down the user's keystrokes when entering a password, credit card number, or other information that may be useful to the creator. This is then transmitted to the malware creator automatically, enabling credit card fraud and other theft. Similarly, malware may copy the CD key or password for online games, allowing the creator to steal accounts or virtual items.

4. MALWARE FOR PROFIT: SPYWARE, BOTNETS, KEYSTROKE LOGGERS, AND DIALERS. 02

4.7 Another way of stealing money from the infected PC owner is to take control of the modem and dial an expensive toll call. Dialer (or porn dialer) software dials up a premium-rate telephone number such as a U.S. "900 number" and leave the line open, charging the toll to the infected user.

5. ACADEMIC RESEARCH ON MALWARE: A BRIEF OVERVIEW 02

5.1 The notion of a self-reproducing computer program can be traced back to 1949 when John von Neumann presented lectures that encompassed the theory and organization of complicated automata. [22] Neumann showed that in theory a program could reproduce itself. This constituted a plausibility result in computability theory.

[22] John von Neumann, "Theory of Self-Reproducing Automata",
Part 1: Transcripts of lectures given at the University of Illinois, Dec. 1949,
Editor: A. W. Burks, University of Illinois, USA, 1966.

5. ACADEMIC RESEARCH ON MALWARE: A BRIEF OVERVIEW 02

5.2 Fred Cohen experimented with computer viruses and confirmed Neumann's postulate. He also investigated other properties of malware (detectability, self-obfuscating programs that used rudimentary encryption that he called "evolutionary", and so on). His doctoral dissertation was on the subject of computer viruses. [23]

[23] Fred Cohen, "Computer Viruses", PhD Thesis, University of Southern California, ASP Press, 1988.

5.3 Cohen's faculty advisor, Leonard Adleman (the A in RSA) presented a rigorous proof that, in the general case, algorithmically determining whether a virus is or is not present is Turing undecidable. [24]

[24] L. M. Adleman, "An Abstract Theory of Computer Viruses", Advances in Cryptology---Crypto '88, LNCS 403, pages 354-374, 1988.

5. ACADEMIC RESEARCH ON MALWARE: A BRIEF OVERVIEW 02

5.4 This problem must not be mistaken for that of determining, within a broad class of programs, that a virus is not present; this problem differs in that it does not require the ability to recognize all viruses. Adleman's proof is perhaps the deepest result in malware computability theory to date and it relies on Cantor's diagonal argument as well as the halting problem.

5.5 Ironically, it was later shown by Young and Yung that Adleman's work in cryptography is ideal in constructing a virus that is highly resistant to reverse-engineering by presenting the notion of a cryptovirus. [25]

[25] A. Young, M. Yung, "Cryptovirology: Extortion-Based Security Threats and Countermeasures,"
IEEE Symposium on Security & Privacy, pages 129-141, 1996

5. ACADEMIC RESEARCH ON MALWARE: A BRIEF OVERVIEW 02

5.6 A cryptovirus is a virus that contains and uses a public key and randomly generated symmetric cipher initialization vector (IV) and session key (SK). In the cryptoviral extortion attack, the virus hybrid encrypts plaintext data on the victim's machine using the randomly generated IV and SK. The IV+SK are then encrypted using the virus writer's public key. In theory the victim must negotiate with the virus writer to get the IV+SK back in order to decrypt the ciphertext (assuming there are no backups). Analysis of the virus reveals the public key, not the IV and SK needed for decryption, or the private key needed to recover the IV and SK. This result was the first to show that computational complexity theory can be used to devise malware that is robust against reverse-engineering.

5. ACADEMIC RESEARCH ON MALWARE: A BRIEF OVERVIEW 02

5.7 Another growing area of computer virus research is to mathematically model the infection behavior of worms using models such as Lotka–Volterra equations, which has been applied in the study of biological virus. Various virus propagation scenarios have been studied by researchers such as propagation of computer virus, fighting virus with virus like predator codes, [26], [27] effectiveness of patching etc.

[26] H. Toyoizumi, A. Kara. Predators: Good Will Mobile Codes Combat against Computer Viruses,
Proc. of the 2002 New Security Paradigms Workshop, 2002

[27] Zakiya M. Tamimi, Javed I. Khan, Model-Based Analysis of Two Fighting Worms,
IEEE/IIU Proc. of ICCCE '06, Kuala Lumpur, Malaysia, May 2006, Vol-I,
Page 157-163

B. GRAYWARE (OR GREYWARE). 02

1.1 General term sometimes used as a classification for applications that behave in a manner that is annoying or undesirable, and yet less serious or troublesome than malware. [28] [29]

[28] "Other meanings", http://mpc.byu.edu/Exhibitions/Of%20Earth%20Stone%20and%20Corn/Activities/Native%20American%20Pottery.dhtml. The term "grayware" is also used to describe a kind of Native American pottery and has also been used by some working in computer technology as slang for the human brain. "grayware definition". TechWeb.com.

[29] "Greyware", What is greyware? - A word definition from the Webopedia Computer Dictionary, http://webopedia.com/TERM/g/greyware.html

B. GRAYWARE (OR GREYWARE). 02

1.2 Grayware encompasses spyware, adware, dialers, joke programs, remote access tools, and any other unwelcome files and programs apart from viruses that are designed to harm the performance of computers on your network. The term has been in use since at least as early as September 2004. [30]

[30] Antony Savvas, "The network clampdown", Computer Weekly, http://www.computerweekly.com/Articles/2004/09/28/205554/the-network-clampdown.htm

1.3 Grayware refers to applications or files that are not classified as viruses or trojan horse programs, but can still negatively affect the performance of the computers on your network and introduce significant security risks to your organization. [31]

[31] Fortinet, WhitePaper - PROTECTING NETWORKS AGAINST SPYWARE ADWARE AND OTHER FORMS OF GRAYWARE, http://www.boll.ch/fortinet/assets/Grayware.pdf

B. GRAYWARE (OR GREYWARE). 02

1.4 Often grayware performs a variety of undesired actions such as irritating users with pop-up windows, tracking user habits and unnecessarily exposing computer vulnerabilities to attack.

1.5 SPYWARE.

That is software that installs components on a computer for the purpose of recording Web surfing habits (primarily for marketing purposes). Spyware sends this information to its author or to other interested parties when the computer is online. Spyware often downloads with items identified as 'free downloads' and does not notify the user of its existence or ask for permission to install the components. The information spyware components gather can include user keystrokes, which means that private information such as login names, passwords, and credit card numbers are vulnerable to theft. Spyware gathers data, such as account user names, passwords, credit card numbers, and other confidential information, and transmits it to third parties.

B. GRAYWARE (OR GREYWARE). 02

1.6 ADWARE.

That is software that displays advertising banners on Web browsers such as Internet Explorer and Mozilla Firefox. While not categorized as malware, many users consider adware invasive. Adware programs often create unwanted effects on a system, such as annoying popup ads and the general degradation in either network connection or system performance. Adware programs are typically installed as separate programs that are bundled with certain free software. Many users inadvertently agree to install adware by accepting the End User License Agreement (EULA) on the free software. Adware are also often installed in tandem with spyware programs. Both programs feed off of each other's functionalities - spyware programs profile users' Internet behavior, while adware programs display targeted ads that correspond to the gathered user profile.

03. THE FUTURE ATTACKING PROCESSES IN THE GLOBAL NETWORK.

A. The Ten Most Important Security Trends of the Coming Year
B. How these trends were determined
C. Experts involved with the project

A. THE TEN MOST IMPORTANT SECURITY TRENDS OF THE COMING YEAR [32]

[32] http://www.sans.org/resources/10_security_trends.pdf

1. MOBILE DEVICES 03

1.1 Laptop encryption will be made mandatory at many government agencies and other organizations that store customer/patient data and will be preinstalled on new equipment. Senior executives, concerned about potential public ridicule, will demand that sensitive mobile data be protected.

1.2 Theft of PDA smart phones will grow significantly. Both the value of the devices for resale and their content will draw large numbers of thieves.

2. GOVERNMENT ACTION 03

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

2.1 Congress and state governments will pass more legislation governing the protection of customer information. If Congress, as expected, reduces the state-imposed data breach notification requirements significantly, state attorneys general and state legislatures will find ways to enact harsh penalties for organizations that lose sensitive personal information.

3. ATTACK TARGETS 03

3.1 Targeted attacks will be more prevalent, in particular on government agencies. Targeted cyber attacks by nation states against US government systems over the past three years have been enormously successful, demonstrating the failure of federal cyber security activities. Other antagonistic nations and terrorist groups, aware of the vulnerabilities, will radically expand the number of attacks. Targeted attacks on commercial organizations will target military contractors and businesses with valuable customer information.

3. ATTACK TARGETS 03

3.2 Cell phone worms will infect at least 100,000 phones, jumping from phone to phone over wireless data networks. Cell phones are becoming more powerful with full-featured operating systems and readily available software development environments. That makes them fertile territory for attackers fueled by cell-phone adware profitability.

3.3 Voice over IP (VoIP) systems will be the target of cyber attacks. VoIP technology was deployed hastily without fully understanding security.

4. ATTACK TECHNIQUES 03

4.1 Spyware will continue to be a huge and growing issue. The spyware developers can make money so many ways that development and distribution centers will be developed throughout the developed and developing world.

4.2 0-day vulnerabilities will result in major outbreaks resulting in many thousands of PCs being infected worldwide. Security vulnerability researchers often exploit the holes they discover before they sell them to vendors or vulnerability buyers like TippingPoint.

4.3 The majority of bots will be bundled with rootkits. The rootkits will change the operating system to hide the attack's presence and make uninstalling the malware almost impossible without reinstalling a clean operating system.

5. DEFENSIVE STRATEGIES 03

5.1 Network Access Control will become common and will grow in sophistication. As defending laptops becomes increasingly difficult, large organizations will try to protect their internal networks and users by testing computers that want to connect to the internal network. Tests will grow from today's simple configuration checks and virus signature validation to deeper analysis searching for traces of malicious code.

B. HOW THESE TRENDS WERE DETERMINED 03

1. Twenty of the most respected leaders in cyber security developed this list.
2. First each proposed the three developments that they each felt were most important.
3. Then they compiled the list of more than 40 trends and voted on which were most likely to happen and which would have the greatest impact if they did happen.
4. That resulted in a prioritized list.
5. To validate their prioritization, they asked the 960 delegates at SANSFire in Washington to each prioritize the 40 trends.
6. More than 340 did so.
7. The SANSFire delegates' input reinforced the experts' prioritization and helped target the Top Ten.

C. EXPERTS INVOLVED WITH THE PROJECT 03

1. Stephen Northcutt, President of the SANS Technology Institute
2. Johannes Ullrich, CTO of the Internet Storm Center
3. Marc Sachs, Director of Internet Storm Center
4. Ed Skoudis, CEO of Intelguardians and SANS Hacker Exploits course director
5. Eric Cole, author of “Hackers Beware” and SANS CISSP Preparation Course Director
6. Jason Fossen, SANS Course Director for Windows Security
7. Chris Brenton, SANS Course Director for Firewalls and Perimeter Protection

C. EXPERTS INVOLVED WITH THE PROJECT 03

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

8. David Rice, SANS Course Director for Microsoft .Net Security
9. Fred Kerby, CISO of the Naval Surface Warfare Center, Dahlgren Division
10. Howard Schmidt, President of ISSA
11. Rohit Dhamankar, editor of the SANS Top 20 Internet Security Vulnerabilities and @RISK
12. Marcus Ranum, inventor of the proxy firewall
13. Mark Weatherford, CISO of Colorado
14. Clint Kreitner, CEO of the Center for Internet Security

C. EXPERTS INVOLVED WITH THE PROJECT 03

15. Eugene Schultz, CTO of High Tower Software
16. Koon Yaw Tan, Security Expert for the Singapore Government
17. Brian Honan, Irish Security Consultant
18. Roland Grefer, Security Consultant
19. Lenny Zeltser, Security Practice Leader at Gemini Systems
20. Alan Paller, Director of Research at the SANS Institute

04. CYBER ATTACKS AGAINST NATIONAL CRITICAL INFORMATION INFRASTRUCTURES.

A. SANS Top-20 2007 Security Risks (2007 Annual Update)
B. B. Best Practices for Preventing Top 20 Risks

A. SANS TOP-20 2007 SECURITY RISKS (2007 ANNUAL UPDATE) [33]

[33] http://www.sans.org/top20/

1. CLIENT-SIDE VULNERABILITIES IN: 04

C1. Web Browsers

C2. Office Software

C3. Email Clients

C4. Media Players

2. SERVER-SIDE VULNERABILITIES IN: 04

S1. Web Applications
S2. Windows Services
S3. Unix and Mac OS Services
S4. Backup Software
S5. Anti-virus Software
S6. Management Servers
S7. Database Software

3. SECURITY POLICY AND PERSONNEL: 04

H1. Excessive User Rights and Unauthorized Devices

H2. Phishing/Spear Phishing

H3. Unencrypted Laptops and Removable Media

4. APPLICATION ABUSE: 04

A1. Instant Messaging

A2. Peer-to-Peer Programs

N1. VoIP Servers and Phones

6. ZERO DAY ATTACKS: 04

Z1. Zero Day Attacks

B. BEST PRACTICES FOR PREVENTING TOP 20 RISKS 04

1. Configure systems, from the first day, with the most secure configuration that your business functionality will allow, and use automation to keep users from installing/uninstalling software
2. Use automation to make sure systems maintain their secure configuration, remain fully patched with the latest version of the software (including keeping anti-virus software up to date).
3. Use proxies on your border network, configuring all client services (HTTP, HTTPS, FTP, DNS, etc.) so that they have to pass through the proxies to get to the Internet.

B. BEST PRACTICES FOR PREVENTING TOP 20 RISKS 04

4. Protect sensitive data through encryption, data classification mapped against access control, and through automated data leakage protection.
5. Use automated inoculation for awareness and provide penalties for those who do not follow acceptable use policy.
6. Perform proper DMZ segmentation with firewalls.
7. Remove the security flaws in web applications by testing programmers security knowledge and testing the software for flaws.

05. PROACTIVE RULES, PRACTICES AND STRATEGIES

Tools That Work [34]

[34] http://www.sans.org/whatworks/

DEFENSIVE WALL 1: PROACTIVE SOFTWARE ASSURANCE 05

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS
BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

1.1 Source Code and Binary Code Testing Tools and Services (White Box Scanners)

1.2 Application Security Scanners (White Box Tools)

1.3 Application Penetration Testing

1.4 Application Security Skills Assessment & Certification

DEFENSIVE WALL 2: BLOCKING ATTACKS: NETWORK BASED 05

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS
BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

- **2.1** Intrusion Prevention (IPS) & Detection (IDS)
- **2.2** Wireless Intrusion Prevention (WIPS)
- **2.3** Network Behavior Analysis and DDoS Monitoring
- **2.4** Firewalls, Enterprise Antivirus and Unified Threat Management
- **2.5** Secure Web Gateways
- **2.6** Secure Messaging Gateways and Anti-Spam Tools
- **2.7** Web Application Firewalls
- **2.8** Managed Security Services

DEFENSIVE WALL 3: BLOCKING ATTACKS: HOST BASED

05

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS

BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

3.1 Endpoint Security

3.2 Network Access Control (NAC)

3.3 System Integrity Checking Tools

3.4 Configuration Hardening Tools

DEFENSIVE WALL 4: ELIMINATING SECURITY VULNERABILITIES

05

International Telecommunication Union

STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS

BULGARIAN ACADEMY OF SCIENCES
NATIONAL LABORATORY OF COMPUTER VIROLOGY

REGIONAL CYBERSECURITY FORUM

4.1 Network Discovery Tools

4.2 Vulnerability Management

4.3 Network Penetration Testing and Ethical Hacking

4.4 Patch and Security Configuration Management and Compliance

DEFENSIVE WALL 5: SAFELY SUPPORTING AUTHORIZED USERS 05

5.1 Identity and Access Management

5.2 Mobile Data Protection and Storage Encryption

5.3 Storage and Backup Encryption

5.4 Content Monitoring

5.5 Data Leak Protection and Digital Rights Management

5.6 Virtual Private Networks (VPNs)

DEFENSIVE WALL 6: TOOLS TO MANAGE SECURITY AND MAXIMIZE EFFECTIVENESS

05

International Telecommunication Union | STATE AGENCY FOR INFORMATION TECHNOLOGY AND COMMUNICATIONS | BULGARIAN ACADEMY OF SCIENCES NATIONAL LABORATORY OF COMPUTER VIROLOGY | REGIONAL CYBERSECURITY FORUM

- **6.1** Log Management and Security Information and Event Management
- **6.2** Media Sanitization and Mobile Device Recovery and Erasure
- **6.3** Security Skills Development
- **6.4** Security Awareness Training
- **6.5** Forensics Tools
- **6.6** Governance, Risk and Compliance Management Tools
- **6.7** Disaster Recovery and Business Continuity

THANK YOU!

PROF. DSC EUGENE NICKOLOV,

CEO, National Laboratory of Computer Virology

1113 Sofia, acad. G. Bontchev St., Building 8,
Tel. 359.2.973.3398, Fax 359.2.971.3710,