Forum: General Assembly First Committee

Issue: Question of cyber security and measures to prevent cyber warfare

Student Officer: Ji Hannah Nan

Position: Chair of General Assembly First Committee

Introduction

Computer security, also known as cyber security and IT security, is the protection of computer systems and information from harm, theft, and unauthorized use. Computer hardware is typically protected by the same means used to protect other valuable or sensitive equipment: serial numbers, doors and locks, and alarms. The protection of information and system access, on the other hand, is achieved through other tactics, some of them quite complex.

The security precautions related to computer information and access address four major threats. The first major threat is theft of data, such as that of military secrets from government computers. The second threat is vandalism, including the destruction of data by a computer virus. The third major threat is fraud, such as employees at a bank channeling funds into their own accounts; and finally, invasion of privacy, such as the illegal accessing of protected personal financial or medical data from a large database. Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. A range of traditional crimes are now being perpetrated through cyberspace. This includes the production and distribution of child pornography and child exploitation conspiracies, banking and financial fraud, intellectual property violations, and other crimes, all of which have substantial human and economic consequences.

Computer security has become increasingly important since the late 1960s, when modems (devices that allow computers to communicate over telephone lines) were introduced. The proliferation of personal computers in the 1980s compounded the problem because they enabled hackers to illegally access major computer systems from the privacy of their homes. The development of advanced security techniques continues to diminish such threats, though concurrent refinements in the methods of computer crime pose ongoing hazards.

Definition of Key Terms

Hardware

Computer Hardware is the physical parts or components of a computer. A combination of hardware and software forms a usable computing system.

Software

Computer software is a part of a computer system that consists of data or computer instructions, in contrast to the physical hardware from which the system is built.

Machine Language Instructions

Machine code or machine language is a set of instructions executed directly by a computer's central processing unit (CPU). Each instruction performs a very specific task.

Central Processing Unit (CPU)

Central processing unit (CPU) refers to the principal part of any digital computer system, generally composed of the main memory, control unit, and arithmetic-logic unit. All input data are transferred via the main memory to the arithmetic-logic unit for processing.

Binary Values

A binary number refers to a number expressed in the base-2 numeral system or binary numeral system, which uses only two symbols: 0 and 1. 0s and 1s can be represented in electromechanical devices with two states—such as "on-off," "open-closed," or "go–no go".

Data Encryption

Data encryption, also called encryption or encipherment, the process of disguising information as "ciphertext," or data unintelligible to an unauthorized person. Conversely, decryption, or decipherment, is the process of converting ciphertext back into its original format. Computers encrypt data by applying algorithm.

Common Vulnerabilities and Exposures (CVE) database

The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures. The National Cybersecurity FFRDC, operated by the Mitre Corporation, maintains the system, with funding from the National Cyber Security Division of the United States Department of Homeland Security.

Backdoor

A backdoor, or a cryptosystem, is any secret method of bypassing normal authentication or security controls. They may exist for a number of reasons, including by original design or from poor configuration. They may have been added by an authorized party to allow some legitimate access, or by an attacker for malicious reasons; but regardless of the motives for their existence, they create a vulnerability.

Denial of Service Attack (DoS)

Denial of service attacks are designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims, such as by deliberately entering a wrong password for consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once.

Direct Access Attack

An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating system modifications, installing software worms, keyloggers, covert listening devices or using wireless mice

Malware

Malware, short for malicious software, is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.

Spoofing

Spoofing is the act of masquerading as a valid entity through falsification of data (such as an IP address or username), in order to gain access to information or resources that one is otherwise unauthorized to obtain.

Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Social Engineering

Social engineering aims to convince a user to disclose secrets such as passwords, card numbers, etc. For example, impersonating a bank, a contractor, or a customer. A common scam involves fake CEO emails sent to accounting and finance departments.

General Overview

Cyberwar

Cyberwar, also called cyberwarfare or cyber warfare, refers to the war conducted in and from computers and the networks connecting them, waged by states or their proxies against other states. Cyberwar is usually waged against government and military networks in order to disrupt, destroy, or deny their use.

Computers and the networks that connect them are collectively known as the domain of cyberspace. Western states depend on cyberspace for the functioning of nearly all aspects of modern society, and developing states are becoming more reliant upon cyberspace every year. Everything modern society needs to function—from critical infrastructures and financial institutions to modes of commerce and tools for national security, depends to some extent upon cyberspace.

Therefore, the threat of cyberwar and its purported effects are a source of great concern for governments and militaries around the world, and several serious cyberattacks have taken place that, while not necessarily meeting a strict definition of cyberwar, can serve as an illustration of what might be expected in a real cyberwar of the future.

Cyberspace Domain

The cyberspace domain is composed of three layers.

The first is the physical layer, including hardware, cables, satellites, and other equipment. Without this physical layer, the other layers cannot function. The second is the syntactic layer, which includes the software providing the operating instructions for the physical equipment. The third is the semantic layer and involves human interaction with the information generated by computers and the way that information is perceived and interpreted by its user. All three layers are vulnerable to attack.

Cyberspace Attack

Despite its increasing prominence, there are many challenges for both attackers and defenders engaging in cyberwar. Cyber attackers must overcome cyber defenses, and both sides must contend with a rapid offense-defense cycle. Nevertheless, the offense dominates in cyberspace because any defense must contend with attacks on large networks that are inherently vulnerable and run by fallible human users. In order to be effective in a cyberattack, the perpetrator has to succeed only once, whereas the defender must be successful over and over again.

Physical attack

Physical attacks usually occur during conventional conflicts, such as in the North Atlantic Treaty Organization's (NATO's) Operation Allied Force against Yugoslavia in 1999 and in the U.S.-led operation against Iraq in 2003, where communication networks, computer facilities, and telecommunications were damaged or destroyed.

Syntactic Attack

Attacks can be made against the syntactic layer by using cyber weapons that destroy, interfere with, corrupt, monitor, or otherwise damage the software operating the computer systems. Such weapons include malware, malicious software such as viruses, Trojans, spyware, and worms that can introduce corrupted code into existing software, causing a computer to perform actions or processes unintended by its operator. For example, in March 2011, the wide use of FinFisher, also known as FinSpy by governments faced political resistance after Egyptian protesters raided State Security Investigations Service and found letters from Gamma International UK Ltd., confirming that SSI had been using a trial version for five months.

Semantic Attack

Semantic cyberattacks, also known as social engineering, manipulate human users' perceptions and interpretations of computer-generated data in order to obtain valuable information (such as passwords, financial details, and classified government information) from the users through fraudulent means.

For example, on October 8th, 2009, US and Egyptian authorities have charged 100 people in "the largest international phishing case ever conducted". The US and Egyptian fraudsters were accused of using phishing scams to steal account details from hundreds, possibly thousands, of people, and transferring about $1.5 million into fake accounts they controlled.

Cyber defense

Despite these challenges, defending against cyberwar has become a priority for many nations. The key features of any major cyber defense include firewalls to filter network traffic, encryption of data, tools to prevent and detect network intruders, physical security of equipment and facilities, and training and monitoring of network users. For example, in the United States, the Twenty-fourth Air Force has been set up to defend Air Force networks. Similarly, the U.S. Navy has formed the Fleet Cyber Command, part of the recommissioned Tenth Fleet, in order to protect its networks. n the United Kingdom the Government Communications Headquarters (GCHQ) created a Cyber Security Operations Centre (CSOC) in September 2009, and France set up its Network and Information Security Agency in July 2009. More specifically in relation to cyber defense tactics, one of DHS (Department of Homeland Security)'s key technologies is EINSTEIN. The goal of the NCPS EINSTEIN set of capabilities is to provide the federal government with an early warning system, improved situational awareness of intrusion threats to federal civilian Executive Branch networks, near real-time identification of malicious cyber activity, and prevention of that malicious cyber activity. Moreover, DHS's Continuous Diagnostics and Mitigation (CDM) program is a dynamic approach to fortifying the cybersecurity of government networks and systems. CDM provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. Congress established the CDM program to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources.

Cyberterrorism

Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political gains through intimidation. It is also sometimes considered an act of Internet terrorism where terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, computer worms, phishing, and other malicious software and hardware methods and programming scripts.

Cyber terrorism takes many forms. One of the more popular is to threaten a large bank. The terrorists hack into the system and then leave an encrypted message for senior directors, which threatens the bank. In essence, the message says that if they do not pay a set amount of money, then the terrorists will use anything from logic bombs to electromagnetic pulses and high-emission radio frequency guns to destroy the banks files. What adds to the difficulty to catch the criminals is that the criminals may be in another country. A second difficulty is that most banks would rather pay the money than have the public know how vulnerable they are. For example, Cyber-terrorists often commit acts of terrorism simply for personal gain. Such a group, known as the Chaos Computer Club, was discovered in 1997. They had created an Active X Control for the Internet that can trick the Quicken accounting program into removing money from a user's bank account. This could easily be used to steal money

from users all over the world that have the Quicken software installed on their computer. This type of file is only one of thousands of types of viruses that can do everything from simply annoy users, to disable large networks, which can have disastrous, even life and death, results.

UN Involvement, Relevant Resolutions, Treaties and Events

In 22th January 2001, the General Assembly established the resolution of Combating the criminal misuse of information technologies. This is a resolution adopted by the General Assembly in 2001 in light of the United Nations Millennium Declaration, especially for new information and communication technologies. It outlines the necessary guidelines and regulations needed to be established in 2001. The following year on 23th January 2002, the First General Assembly again debated and rewrote the resolution Combating the criminal misuse of information technologies. This resolution directly brings the issue of criminal misuse of information technologies to front. However, this resolution is not successful in setting up specific regulations or establishing a consensus. On 31st January 2003, a resolution on the Creation of a global culture of cybersecurity was approved. This addresses how each member states could contribute to establish a global culture of cybersecurity, including outlining the responsibility of participants, security assessments etc. This resolution is successful in setting up specific procedures that help cultivate cybersecurity globally. On 30th January 2004 followed the Creation of a global culture of cybersecurity and the protection of critical information infrastructures. This resolution was successful in suggesting possible elements for protecting political infrastructure. Finally, in 17th March 2010, the First General Assembly passed the resolution 'Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures'. This resolution provides more detail with how national action and legislation could help protect cyber security in information infrastructure. It is also more specific than previous resolutions in detail, for example, the mention of specific time range before a security check, specific organizations responsible for conducting these evaluations etc.

Timeline of Events

Date	Description of event
November 2nd, 1988	Robert Morris and the first computer worm In 1988, only 60,000 computers were connected to the Internet. Most were mainframes, minicomputers and professional workstations. On 2 November 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers – the first internet "computer worm". The software was traced back to 23-year-old Cornell University graduate student Robert Tappan Morris, Jr. who said 'he wanted to count how many machines were connected to the Internet'.

1994	Rome Laboratory In 1994, over a hundred intrusions were made by unidentified crackers into the Rome Laboratory, the US Air Force's main command and research facility. Using trojan horses, hackers were able to obtain unrestricted access to Rome's networking systems and remove traces of their activities. The intruders were able to obtain classified files, such as air tasking order systems data and furthermore able to penetrate connected networks of National Aeronautics and Space Administration's Goddard Space Flight Center, Wright-Patterson Air Force Base, some Defense contractors, and other private sector organizations, by posing as a trusted Rome center user.
January 22nd, 2002	The resolution of Combating the criminal misuse of information technologies This resolution Invites Member States, when developing national law, policy and practice to combat the criminal misuse of information technologies, to take into account, as appropriate, the work and achievements of the Commission on Crime Prevention and Criminal Justice and of other international and regional organizations. It invites Member States to take them into account in their efforts to combat the criminal misuse of information technologies
January 31st, 2003	Creation of a global culture of cybersecurity United Nations General Assembly (UNGA) Resolution 57/239 was adopted on January 31, 2003, recognizing that, in a manner appropriate to their roles, government, business, other organizations, and individual owners and users of information technologies must be aware of relevant cybersecurity risks and preventive measures and must assume responsibility for and take steps to enhance the security of these information technologies. Therefore, the General Assembly invites Member States and all relevant international organizations to take these elements and the need for a global culture of cybersecurity into account, in their efforts to develop throughout their societies a culture of cybersecurity in the application and use of information technologies.
January 30th, 2004	Creation of a global culture of cybersecurity and the protection of critical information infrastructures This Resolution invites Member States to use, if and when they deem appropriate, the annexed voluntary self-assessment tool for national efforts to protect critical information infrastructures in order to assist in assessing their efforts in this regard to strengthen their cybersecurity, to highlight areas for further action, with the goal of increasing the global culture of cybersecurity; encourages Member States and relevant regional and international organizations that have developed strategies to deal with cybersecurity and the protection of critical information infrastructures to share their

best practices and measures that could assist other Member States in their efforts to facilitate the achievement of cybersecurity by providing such information to the Secretary-General for compilation and dissemination to Member States.

March 17th, 2010

Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures

This Resolution invites Member States to use, if and when they deem appropriate, the annexed voluntary self-assessment tool for national efforts to protect critical information infrastructures in order to assist in assessing their efforts in this regard to strengthen their cybersecurity, to highlight areas for further action, with the goal of increasing the global culture of cybersecurity; encourages Member States and relevant regional and international organizations that have developed strategies to deal with cybersecurity and the protection of critical information infrastructures to share their best practices and measures that could assist other Member States in their efforts to facilitate the achievement of cybersecurity by providing such information to the Secretary-General for compilation and dissemination to Member States.

2013

Global surveillance disclosures

In early 2013, documents provided by Edward Snowden were published by The Washington Post and The Guardian exposing the massive scale of NSA global surveillance. It was also revealed that the NSA had deliberately inserted a backdoor in a NIST standard for encryption and tapped the links between Google's data centres.

Possible Solutions

There are several possible solutions to combat cyberattacks and cyberterrorism.

The first solution is through establishing national and international community workshops to raise awareness, and educating the public about cyber security and cyberattacks. This would be very effective in establishing fundamental, public and basic knowledge about the risks and precautions needed as the first 'firewall' against cyberattacks and cyberterrorism. This could be achieved by the government's collaboration with domestic organizations and respective NGOs to set up events, create medias that inform and educate the public about this issue. This however, needs to be done on a case by case basis, as each country's political situation and stance is different.

The second solution is to call for governmental actions to support academic colleges and universities, federal and local agencies, non-profit organizations and other agencies to develop anti-cyberattack programs. This again, would be effective in promoting rapid technological improvement and growth, especially in the fields of cyber defense. It would also demonstrate the governments acknowledgement and support of this vital issue, encouraging more talented professionals to tackle in this field.

This final solution is establishing more IT or cyber security work forces, including the Department of Homeland Security (DHS). This is especially effective because cyber security work forces could specialize in this field and act as a stronghold for professionals, research projects and potential collaborations and strategic alliances between different NGOs and organizations. This could be achieved by the government contributing a larger percentage of its revenue or the nation's GDP on cyber defense, it could also be achieved through collaboration with respective NGOs and private organizations.

Bibliography

"Cybersecurity Jobs." Department of Homeland Security, 28 June 2016, www.dhs.gov/topic/cybersecurity-jobs.
https://www.dhs.gov/topic/cybersecurity-jobs

"Log in." Britannica School, school.ebonline.com/levels/high/article/cyberwar/488833#296421.toc.
https://school.ebonline.com/levels/high/article/cyberwar/488833#296421.toc

"Computer security." Wikipedia, Wikimedia Foundation, 14 Nov. 2017, en.wikipedia.org/wiki/Computer_security#Computer_protection_.28countermeasures.29.
https://en.wikipedia.org/wiki/Computer_security#Computer_protection_.28countermeasures.29

"United Nations Official Document." United Nations, United Nations, www.un.org/en/ga/search/view_doc.asp?symbol=A%2FRES%2F64%2F211.
http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211