The use of cyber warfare: detection, monitoring, prevention, and response

Forum: 3rd Committee (Disarmament and International Security)

Student Officers: Maksim Shcheglov, Ksenia Matrosova

INDEX

Introduction

In the 21st century, the confrontation between countries is moving to a new level. Previously, the threat posed by nuclear weapons, hydrogen bombs. Today the army, navy, nuclear weapons can be powerless against a new kind of attacks – cyberattacks. Cyber warfare involves the actions of a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks. Such attacks can break down computer networks not only of global corporations but also modern computer systems of governments of countries. Although cyberwarfare refers to cyber attacks perpetrated by one nation-state on another, it can even describe attacks by terrorist groups or hacker groups aimed at furthering the goals of particular nations. It can be difficult to definitively attribute cyber attacks to a nation-state when those attacks are carried out by advanced persistent threat (APT) actors, but such attacks can often be linked to specific nations. Cyber attacks could hack the stock exchanges and cause a stock market crash and this can furthermore lead to the global crisis. Moreover, the most dangerous aspect in this case is that with the help of cyber attacks it is possible not only to influence the internal political situation of the country but even to unleash the Third World War. That is why today systems for protecting servers and computers are being actively developed. However, this issue requires strict regulation by countries intending to create a mechanism for responding with defensive measures to counter and regulate cyberattacks, like the Geneva Conventions on waging wars.

Definition of key terms

Cyberface — the notional environment in which communication over computer networks occurs.

Cyber Warfare — a military action, carried out electronically, and not physically, where the weapon acts as information, and the tools are computers and the Internet. The task of this kind of war is to achieve certain goals in the economic, political, military, and other fields, by influencing society and the authorities with carefully prepared information.

The Internet — any set of computer networks that communicate using the Internet Protocol.

Cyberattack — a type of threat where immediate damage or disruption caused are the main concern.

Cyber Espionage — a type of threat which can provide the information needed to make a successful cyberattack or scandal and launch an information warfare.

Malware — malware, or malicious software, is any program or file that is harmful to a computer user. Malware includes computer viruses, worms, Trojan horses, and spyware. These malicious programs can perform a variety of functions, including stealing, encrypting, or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission.

Background Information

Cyberwarfare could be represented as viruses, computer worms, and malware that can take down water supplies, transportation systems, power grids, critical infrastructure, and military systems. Another kind of cyberwarfare is denial-of-service (DoS) attacks, cybersecurity events that occur when attackers take action that prevents legitimate users from accessing targeted computer systems, devices, or other network resources. The most common type of cyberwarfare is ransomware that holds computer systems hostage, which usually affects the computer system at the household level. However, according to the latest research, more and more cyber attacks are aimed at hacking and theft of critical data from institutions, governments, and businesses which cause serious problems to the global community.

One of the earliest widely-known instances of a nation waging cyberwar was the Stuxnet worm, which was used to attack Iran's nuclear program in 2010. The malware targeted SCADA (supervisory control and data acquisition) systems. SCADA was spread with infected USB devices. According to some sources of information (SearchSecurity website), the United States and Israel have both been linked to the development of Stuxnet. However, nations have formally acknowledged its role.

Another widely-spread cyberattack is associated with the government of North Korea, that were blamed for the 2014 cyber attack on Sony Pictures after Sony released the film The Interview, which portrayed the North Korean leader Kim Jong-un in a negative way. During its investigation into the hack, the FBI noted that the code, encryption algorithms, data deletion methods, and compromised networks were similar to malware previously used by North Korean hackers. Besides, the hackers used several IP addresses associated with North Korea.

A 2015 attack on the German parliament, suspected to have been carried out by Russian secret services, caused massive disruption when the attack infected 20,000 computers used by German politicians, support staff members, and civil servants. Sensitive data was stolen, and the attackers demanded several million euros to clean up the damage. Although a group of Russian nationalists who wanted the government of Berlin to stop supporting Ukraine claimed responsibility, some sources of information (SearchSecurity, Techopedia, BBC, DW, Netzpolitik.org etc.) consider that, perhaps, members of the Russian intelligence were also reported to be involved.

Moreover, the process of viruses and malicious software rapidly development is not only in terms of technology - they also evolve qualitatively, entering new markets and "work" spheres. From the qualitative point of view, the modern activity can be divided into three levels:

- Cyber threats or the level of B2C (Business to consumers).
- Target attacks or B2B level (Business to business).
- Cyber weapons or I2B (Business to industrial).

Major countries and organisations involved

As it was stated by 'McAfee', the developer of antivirus software, nowadays, approximately 120 countries have been developing ways to use the Internet as a weapon and target financial markets, government computer systems and utilities.

Mikko Hypponen, F-Secure Corporation's Chief Research Officer, ranked the United States, Israel, Russia, China, Iran, and North Korea as the countries with the most powerful cyber capabilities. Nevertheless, such countries as India, Philippines, South Korea, Saudi Arabia, Estonia, Germany, Netherlands, Norway, Sweden, Ukraine, and the United Kingdom were as well recognised as cyber-attacker or cyber-victim countries in recent years.

International cooperation against cybercrime: United Nations (UN), Group of Eight (G8), Council of Europe, The International Telecommunication Union (ITU), International Multilateral Partnership Against Cyber Threats (IMPACT), The North Atlantic Treaty Organisation Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), Asia-Pacific Economic Cooperation (APEC), The Organisation for Economic Co-operation and Development (OECD), The Economic Community of West African States (ECOWAS), European Union, Commonwealth, the Arab League and Gulf Cooperation Council (GCC).

Relevant treaties and UN resolutions

- Council of Europe's 2001 Budapest Convention on Cybercrime.
- UN Resolutions Related to Cybersecurity:
    - Resolution 55/63, January 2001

      Combating the criminal misuse of information technologies
    - Resolution 56/121, January 2002

      Combating the criminal misuse of information technologies
    - *Resolution 57/239, January 2003*

      Creation of a global culture of cybersecurity
    - *Resolution 58/199, January 2004*

      Creation of a global culture of cybersecurity and the protection of critical information infrastructures
    - *Resolution 64/211, March 2010*

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

- *Resolution 70/237, December 2015*

  Developments in the field of information and telecommunications in the context of international security

Previous attempts to solve the issue

- 2004: The Council of Europe's 2001 Budapest Convention on Cybercrime (came into effect in 2004);
- 2009: A group of cybersecurity experts began to work on the first Tallinn Manual, a non-binding study on how international law might been applied to cyber warfare;
- 2010: In order to efficiently prepare for a possible cyberwar the USA has launched a simulation called Cyber ShockWave which simulate cyber attacks;
- 2011: Developing a Convention on the Conduct of Cyberwar;
- 2011: "International code of conduct for information security" by the Shanghai Cooperation Organization, which did not pass because it enabled much internet censorship according to many western countries;
- 2015: Draft global electronic nonaggression pact;
- Establishment of a cyberwar-hotline which should be used in a crisis situation to prevent an accidental cyberwar (by USA and Russia).

Possible solutions

Cyber attacks can be prevented with two different types of measures: the first class intending to deter states from carrying out cyber attacks and the second type being measures to increase the security of the networks which have the highest risked of being attacked.

One of the most relevant possible solutions might be calling for Geneva Convention for cyber warfare.

Creating a strong focus on public-private cooperation against cybercrime is essential. Each state should increase its security measures against cyber attacks. In order to do this as efficiently as possible governments should establish, if not yet done so, an agency whose sole focus is on the cyberspace and cyber attacks.

Two very controversial ideas that may be introduced are the kill switch and the electrical wall. The kill switch could shut down the internet in specific areas, whether it only concerns a company, a city or a whole country, in case of serious cyber attacks. The electrical wall intends to inspect every data package coming into the country's network and compares it to known signatures and in case

of a match does not let them through. Both these ideas can be beneficial and even save lives. However, they can violate fundamental human rights by censoring certain parts of the internet.

A new conceptual framework for the conduct of countries in the information sphere should be developed, precisely oriented towards the effective integration of states into the global information society. Also, the non-use principle of the identified vulnerabilities in products of commercial companies for the commission of cyber attacks and other illegal actions in cyberspace must be introduced. Moreover, the state should report vulnerabilities to the manufacturer, so that he can eliminate them.

In general, all states should consider their possibilities with care as the internet is a symbol of freedom and a country interfering with the internet could lead to protest of the civilians. Because the internet connects everyone worldwide, each state is equally affected.

Reliable and Useful Sources

https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/assets/HomePage/ODAPublications/OccasionalPapers/PDF/OP19.pdf

https://www.itu.int/en/action/cybersecurity/Pages/default.aspx

http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

https://ccdcoe.org/publications/2012proceedings/2_3_Arimatsu_ATreatyForGoverningCyber-Weapons.pdf

https://www.icrc.org/en/international-review/article/get-my-cloud-cyber-warfare-international-humanitarian-law-and

https://link.springer.com/article/10.1007/s13347-017-0271-5