GeMUN 2018

Disarmament and International Security Committee (DISEC)

Topic: Question of monitoring cyber and digital tools such as drones and their potential use in cyber warfare

Research Report by Aysha Tafur

INDEX

I. DEFINITION OF KEY TERMS

Cyber: Relating to or characteristic of the culture of computers, information technology, and virtual reality.

Cyberwarfare: the act of using the internet to attack a country's computers in order to damage things such as communication and transport systems or water and electricity supplies.

Cyber weapon: A piece of computer software or hardware used to commit cyberwarfare.

Cyber-attack: an attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network.

Cyber espionage: is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers.

Cyberspace: the internet considered as an imaginary area without limits where you can meet people and discover information about any subject.

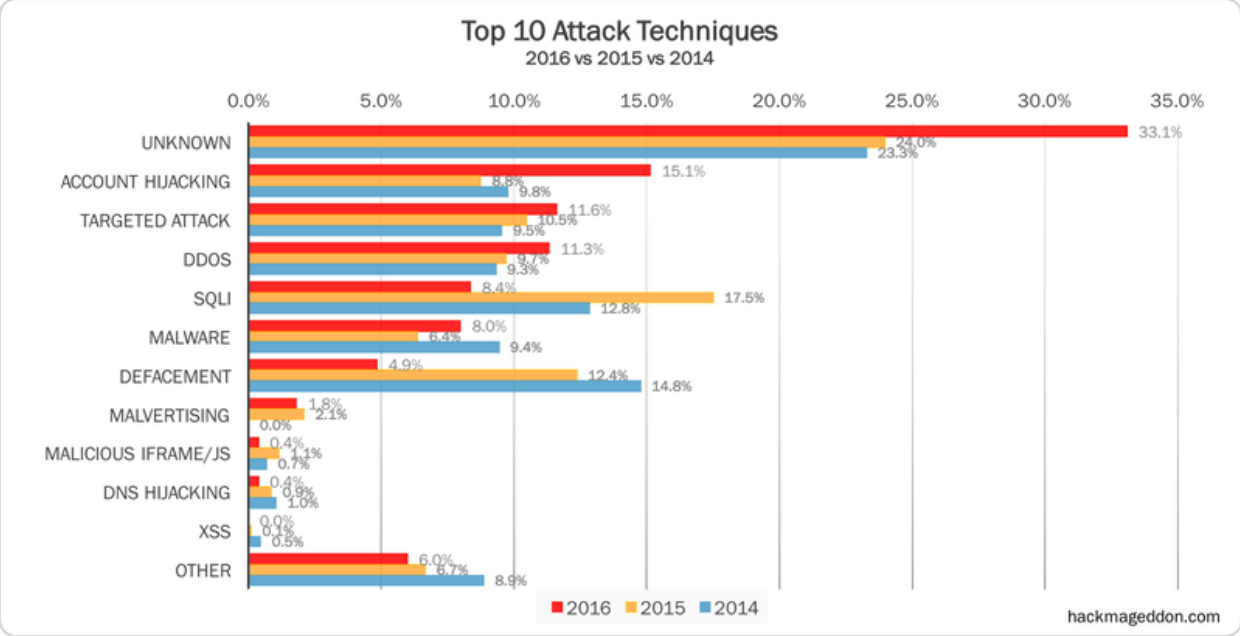
II. INTRODUCTION

Cyberwar is usually undertaken against government and military networks in order to destroy, disrupt, or deny their use. Nowadays western states depend on cyberspace for the everyday functioning of nearly all aspects of modern society. The threat of cyberwar and its effects are a source of great concern for governments and militaries around the world, and the latest cyber attacks can serve as an illustration of a possible cyberwar of the future.

III. BACKGROUND INFORMATION

The cyberspace domain is composed of three layers: the physical layer, syntactic layer, and the semantic layer. Traditional combat methods and weapons can be used for cyberwar attacks against the physical infrastructure of cyberspace. Computers can be destroyed and their networks can be interfered with. Human users of this physical infrastructure can be misled or killed in order to gain physical access to a computer or network. During conventional conflicts, physical attacks occur; for example, in 1999, in the North Atlantic Treaty Organization's (NATO's) Operation Allied Force against Yugoslavia and in 2003, in the U.S.-led operation against Iraq, communication networks, computer facilities and telecommunications were damaged or destroyed. Malware, viruses, worms and spyware are weapons, which are used during cyber attacks against the syntactic layer in order to damage or destroy the software operating the computer systems. Another type of cyber weapons is DDoS, or denial-of-service, in which the attackers, through a malware, take over several computers in order to create a group of "zombie" computers; these computers will attack other computers, preventing their function. This method was used in April and May 2007 in cyber attacks against Estonia and in August 2008 against Georgia. Due to these attacks, governments and citizens of those countries could not access to key sources of information and to external and internal communications.

Drones are another important cyber weapon; they are controlled from the ground by pilots and usually have a pre-programmed mission. The drones are divided into two categories: some are armed with missiles and bombs, others are used to monitor or for reconnaissance purposes. The use of drones has several positive aspects: they can remain aloft for many hours, they are less expensive compared to military aircraft and are piloted from the ground, therefore there is no danger for the crew; for these reasons, the use of drones has increased considerably in recent years.



The graph shows the most used techniques in cyber attacks in the years from 2014 to 2016.

Nowadays cyberwar has assumed a central role in armed conflicts, for example in the Israeli-Hezbollah conflict in Lebanon in 2006 and the Russian invasion of Georgia in 2008. Similarly, in 2007, the cyber attacks against Estonia took place during a political crisis surrounding the removal of a Soviet war memorial from the centre of Tallinn to its suburbs. It is widely believed that cyber war will feature significantly in all future conflicts and it will probably even constitute the opening phases of them; the role of cyberwar in conventional conflicts is notably increasing.

IV. Major Countries Involved

The major countries involved in cyberwarfare are: The United States, North Korea, China, Russia, Israel and Iran.

The United States

The United States depends heavily on the internet; in fact, the country has considerable capacity in terms of power and defence thanks to the military budget and advanced technology. At the same time, however, it is particularly exposed to cyber-attacks; the country faces both internal and foreign enemies, in fact, it has developed important skills. The US Defense Department accepts the use of internet and computers in order to wage war in cyberspace. In 2010, the United States have started to focus on cyber warfare when the US Cyber Command decided to unify the cyber capabilities of the Army, Air Force, Navy and Marines under one roof. In 2011, The White House published an "International Strategy for Cyberspace" that recognized the right to use military force in response to a cyber attack. In 2013, the Defense Science Board (advisory committee to the U.S. Secretary of Defense) stated that cyber threat is serious, with potential consequences and recommended, in response to the most extreme case, the use of nuclear weapons. In June 2010, United States attacked Iran's nuclear facility in Natanz through a cyber-worm called 'Stuxnet', one of the most advanced pieces of malware ever discovered. According to a Business Insider article, it destroyed perhaps over 1000 nuclear centrifuges and Tehran's atomic program back by at least two years. In 2013 Chinese mobile phone companies were hacked by United States government in order to collect text messages and spy on Tsinghua University, one of China's biggest research institutions. Edward Snowden, a former systems administrator for the CIA, provided documents; according to these documents, the headquarters of Huawei was infiltrated in the servers by the National Security Agency (NSA), China's largest telecommunications company and the largest telecommunications equipment maker in the world. The plan was to exploit Huawei's technology in such a way that when the company sold equipment to other countries, the NSA could surveil through their telephone networks and computer.

North Korea

North Korea is considered to be responsible for a number of cyber attacks. A South Korean lawmaker declared that the North had victoriously broken into the South's military networks to steal war plans in 2014. The most famous cyber-attack took place against Sony Pictures Entertainment, in order to block the release of a movie that satirized Mr Kim. A few weeks before the attack on Sony, North Korea has hacked a British television network, blocking the transmission of a drama about a nuclear scientist kidnapped in Pyongyang. North Korea, thanks to ransomware, digital bank heists, online cracking video games, hacks of South Korean Bitcoin exchanges, earns hundreds of millions of dollars a year.

China

China was accused by Western countries of espionage, but it has denied accusations of cyber warfare and has accused the United States of engaging a cyberwar against it. In 2007, information about the rocket and space technology organization to China was passed by the Russian executive; due to this fact he was sentenced. In 2008, according to an article in the Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies by Jason Fritz, China was involved in a notable number of cases of espionage primarily through the use of a "decentralized

network of students, engineers people, businessmen, scientists, diplomats and from within the Chinese Diaspora. Even though it is considered to be responsible for cyber attacks on a number of public and private institutions in the United States, India, Russia, Canada, and France, Chinese government denies being involved in cyber-spying campaigns. In recent years, China acquired foreign military technology in order to expand its cyber and capabilities military technology. Amitai Etzioni, a member of the Institute for Communitarian Policy Studies calls on the United States and China to work together in order to agree on a policy of moderation with respect to cyberspace.

Russia

It is believed that Russia security services organised a number of denial of service attacks as a part of their cyber-warfare against other countries. In 2007, various websites of Estonian organisations in Russia were victims of a cyber attack including Estonian parliament, banks, ministries, newspapers and broadcasters; during this period there was also the problem of relocating the Bronze Soldier of Tallinn. In 2008, Azerbaijani, Georgian and South Ossetian sites were attacked by hackers during South Ossetia War. In 2014, the Russian cyber weapon called Snake attacked the Ukrainian government systems. In April 2015, CNN declared that Russian hackers penetrated into the White House Computers; probably Russian hackers worked for the Russian government.

Israel

Israel is a world leader in computer skills; it obtained an evaluation of 4.5 out of 5 stars in a report that examined the cybernetic preparation, receiving positive comments. In 2006, Israel declared that the cyber war was part of the war against Hezbollah; many Russian hackers and scientists worked on behalf of some countries in the Middle East according to the Israel Defence Forces. In 2007, Syria was the victim of an aerial bombing; this operation took the name of Operation Orchard. The US hypothesizes the fact that Israel used the cyber war in order to get their planes unnoticed by the radars in Syria. In May 2013, Israel was the victim of a cyber-attack by a group called the Syrian Electronic Army. In 2014, the collective Anonymous attacked schools, banks, non-profit organisations, newspapers and websites. In both cases, Jerusalem was prepared; in fact, the attacked websites worked perfectly. Israel proved to be ready to face every possible situation.

Iran

Iran is developing cyber capabilities and it is seen as the responsible for several attacks in the region. Iran is a country that in addition to being attacked several times in cybernetic operations, is beginning to attack, in fact, it is considered an emerging military power. In 2010, Israel was the victim of an attack through a worm called Stuxnet; it is the most advanced worm ever discovered and is only distributed in Israel and the United States. The attack was aimed at the Natanz nuclear enrichment facility. In 2012, Iranian hackers struck Saudi Arabia's national oil company, Saudi Aramco, bringing the company close to collapse. Since 2014 one Iranian group, named as Rocket Kitten has been reported by many in the cybersecurity industry and has been linked to numerous attacks. It is possible that they are associated with the Iranian Revolutionary Guard.

V. UN INVOLVEMENT

For the past 15 years, the United Nations has been trying to achieve guidelines on international cybersecurity. Two important resolutions passed in 2003 and 2004. Resolution 57/239 **(1)** of 2003 invites nations to raise responsibility and awareness in order to prevent, respond and detect

cybersecurity threats. Resolution 58/199 **(2)** of 2004 encourage member nations with national cybersecurity strategies to share and establish similar strategies with other member nations. In 2010, a UN Group of Governmental Experts formed by diplomats from Russia, the United States and China, declared that cybersecurity threats are one of the main challenges of the 21st century. In 2015, Russia, China, and other members of the Shanghai Cooperation Organization sent a letter to the Secretary-General in order to prevent members using cyberspace for cyber attacks.

VI. BIBLIOGRAPHY

https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf (1)
https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf (2)

https://www.britannica.com/topic/cyberwar

https://en.wikipedia.org/wiki/Cyberwarfare

https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/

https://globalriskadvisors.com/blog/united-nations-cyber-warfare/

https://en.oxforddictionaries.com/definition/cyber

https://dictionary.cambridge.org/dictionary/english/cyber-warfare

https://en.oxforddictionaries.com/definition/cyberweapon

https://dictionary.cambridge.org/dictionary/english/cyberspace

https://en.wikipedia.org/wiki/Cyberwarfare_in_the_United_States

https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html

https://en.wikipedia.org/wiki/Cyberwarfare_in_China

https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

http://www.meforum.org/6399/israeli-defense-in-the-age-of-cyber-war

https://en.wikipedia.org/wiki/Cyberwarfare_by_Russia

https://dronewars.net/aboutdrone/

http://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/