Forum: MC1- The Disarmament and International Security Committee

Topic: The Impact of Cybersecurity on International Relations

Presidents: **Victor Radocea**

Alexandru Hodivoianu

Abdul Celik

Introduction

With the world around us modernizing exponentially as new technologies and techniques are invented and used, the western life has now evolved into revolving around the use of personal computers and the Internet. With so much knowledge available at our fingertips, we are living in a golden age of information. However, this comes with some very exploitable consequences.

Ever since the invention of the Internet, that many electronic devices are linked together and share a cloud-space, it has been possible for individuals with a vast knowledge of computing to access anything an individual, company, or governmental institution might hold dear. Personal photos, passwords, business strategies, nuclear launch codes - all of these have the potential of being accessed, obtained and used by hackers. Acts of accessing other people's information or causing havoc through hacking are classed as cyber-crimes. However, in order to prevent these cybercrimes, cyber-security had to evolve massively.

Cybersecurity refers to the techniques generally set forth in published materials that attempt to protect the cyber environment of a user or organization. The principal objective is to reduce the risks, including prevention or mitigation of cyber-attacks.

Definition of key terms

Cybercrime: Criminal activities carried out by means of computers or the Internet.

Cyber-warfare: The act of launching attacks on other states and/or organizations through the usage of computer or the Internet to sabotage their activities and systems.

Cyber-Terrorism: The act of intimidating a government or an organization in order to advance its political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them.

Computer crime: Committing an illegal offense by using computers and the Internet.

Worm (computer worm): A worm is a form of malware that self-replicates and then spreads from computer to computer through networks.

Malware: Software that is specifically designed to disrupt, damage, interfere, or gain access to a computer system.

Software: Programs used by a computer that are installed within the components of a computer (as opposed to hardware which are the parts that make up a computer).

Trojan: A Trojan is something that pretends to be something else -a piece of software that tricks the user into downloading it by looking like something the user would need, such as a fake anti-virus program.

Distributed denial of service (DDOS): A DDOS attack is when a network is attacked through the hacker sending countless (usually million or hundreds of thousands) of requests in very short intervals repeatedly to either view a website or access a file, which overloads its servers and makes the website or file impossible to view and use.

History

Network breaches and malware did exist and were used for malicious ends during the early history of computers, however. The Russians, for example, quickly began to deploy cyberpower as a weapon. In 1986, the German computer hacker Marcus Hess hacked an internet gateway in Berkeley, and used that connection to piggyback on the Arpanet. He hacked 400 military computers, including mainframes at the Pentagon, with the intent of selling their secrets to the KGB. At this point in the history of cyber security, computer viruses began to become less of an academic prank, and more of a serious threat. It had already become clear that cyber security had risen to the pinnacle of world politics when US President Obama went in front of television cameras in December 2014 to publicly accuse the North Korean government of hacking Sony Pictures Entertainment. The hack of the Democratic National Committee by the Russian government and the subsequent publication of confidential emails during the 2016 US presidential election elevated cyber security in the context of international affairs to an unprecedented level in the public's consciousness, not only in the United States but around the world.

Key issues

Cyber issues have been framed as security concerns since the 1980s but became constructed as existential threats to national security only in the post–Cold War era and in particular in the first decade of the 21st century, when uncertainty related to technological innovation, rising powers in the Global South, and transnational terrorism increased. In this context, risks became framed in terms such as “weapons of mass disruption” and “electronic Pearl Harbors”.

Many of us don’t have a very clear understanding of hacking. However, the governments use those with hacking skills to sabotage or espionage foreign powers. With cybersecurity issues becoming more threatening every day, it’s doubtful we’ll see any major improvements in international relations. If anything, integration with technology will no doubt breed additional problems for us to solve.

Perhaps the only comfort is the lack of teeth behind most politicians. They might talk a good game, but they don’t seem too eager to do anything rash when the crime is only data related.

Major parties involved

The United States

The United States remains the only superpower in the world, often setting precedents and standards emulated by other countries, including regarding cyberspace and cyberconflict. In 2010, William Lynn, US deputy secretary of defense at the time, declares cyberspace to be a new operational domain for the US military. Meanwhile, the Obama administration expressed a specific desire for rules of the road for cyberspace in its 2011 international strategy for cyberspace , influenced by a growing sense of vulnerability and an increasing number of states developing military doctrines for cyberspace. he US government’s international vision gained further contour with the 2014 report of the US Department of State’s International Security Advisory Board, outlining the vision for international cyberstability . Five years after, the Pentagon released its new cyberstrategy, acknowledging offensive capabilities , and Secretary of State John Kerry outlined five specific norms to govern behavior in cyberspace in his 2015 speech in South Korea in furtherance of the goal of international cyberstability.

Russia

Russia is one of the most advanced cyberpowers. In 1998, Russia proposed an international cybersecurity treaty and initiated the process at the UN, focusing on the use of information-and-communications technologies in the context of international security, which has become the center of the international community’s discussion about cybersecurity norms today. Meanwhile, Russia’s perspective and approach to cybersecurity differ significantly from that of the United States, which is the focus of three articles written by Russian experts, focusing on the military use of the Internet, international law and norms , and the application of arms control.

Other selected countries and Regions Noteworthy in Cybersecurity Geopolitics

Several other countries must be highlighted in the context of geopolitical trends relating to cybersecurity, given their sophisticated and increasingly sophisticated capabilities such as Israel, North Korea, and Iran, in addition to the world’s great powers

6. Timeline

1988 The Morris Worm spreads across the US, causing massive problems for those infected by it

2002 The Bush administration files a bill to create the Department of Homeland Security, which, among other things, will be responsible for protecting the nation's critical IT infrastructure.

2006 The city of Los Angeles' traffic engineers go on strike with two of the strikers hacking the traffic light systems, causing massive congestions at key intersections

2006 NASA blocks all received emails that have attachments in fear that they could sabotage a shuttle launch

2007 Russia allegedly hacked the Estonian government's systems, causing problems to the country's banking systems and online services

2007 The US secretary of Defence's email was hacked and information which would later lead to attacks on the Pentagon

2007 The US and Taiwan allegedly hacked their way into obtaining files belonging to China's Ministry of State security

2008 Russia allegedly hacked Georgian computer networks using DDOS attacks in order to make certain services unavailable

2009 Russia allegedly hacked into Israel's infrastructure during the Gaza strip offense

2010 The Stuxanet virus was found

2012 Conflicts between Saudi Arabia and Israel based on releasing credit cards online

2013 First edition of the Tallinn Manual was released, which provided a study on how international law applied to cyberspace

2013 Allegedly North Korean hackers hacked financial institutions and a broadcasting channel in South Korea

2013 UNODC Produce the "Comprehensive Study on Cybercrime"

2014 The White House Computer system was hacked- one of the most sophisticated attacks against the US Government

2017 The second edition of the Tallinn Manual was released, so called Tallinn Manual 2.0, which expanded upon the original Tallinn Manual

2017 UK was targeted by hackers that allegedly came from North Korea with the intentions of embezzling money and cripple networking systems

2017 Powerful cyber-attacks using the Petya malware against Ukraine, France, Germany, Italy, Poland, Russia, United Kingdom, United States and Australia targeted towards websites of organizations, including banks, ministries, newspapers and electricity firms.

7. Previous Solutions

A previous attempt is the NATO creating the Cooperative Cyber Defense Centre of Excellence. The goal of the CCDCOE is to develop the defensive capabilities of protecting those at risk from cyber-attacks through the mediums of cyber warfare and cyber terrorism. This has succeeded through its ability to bring states together to cooperate and develop existing defense systems. The CCDCOE is perhaps not a failure in itself, however it is a part of NATO, which limits the members of it, something one can see as counterproductive.

Another previous attempt of stopping cyber-crimes was the creation of the Tallinn Manual and Tallinn Manual 2.0(followed soon after) which is the most comprehensive analysis of how existing international law applies to cyberspace. The drafting of this manual was facilitated by CCDCOE. Despite of how good the Tallinn Manual 2.0 may seem, it has the great drawback of not being legally binding, meaning that it is up to each state whether or not to follow the guidelines it presents.

8. Possible Solutions

Considering it is hard to determine who did what and how they should be punished, due to alliances between many of the great and super powers in the world creating obvious biases, a favorable solution could be to make the UN's International Court of Justice mandate cases where two states are involved in some form of cyber conflict.

Further research and development in computing and defense mechanisms should also be a favorable solution. There is already ongoing cooperation with anti-virus software giants such as

McAfee and Kaspersky, where they help research and develop defense systems. Creating an international research facility for this research could be favorable, but also a bit risky, since this would open a door to spying.

9. Bibliography

https://blog.oup.com/2017/02/impact-cyber-security-international-relations/

https://searchsecurity.techtarget.com/definition/cybersecurity

https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm

https://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/

https://www.policyconnect.org.uk/sites/site_pc/files/report/963/fieldreportdownload/cybersecuritypolicysnapbriefing.pdf

.