GLOBAL FOUNDATION FOR CYBER STUDIES AND RESEARCH

OPINION PAPER

THE CURRENT POSTURE

OF CYBER WARFARE AND CYBER TERRORISM

PAPATHANASAKI MARIA

LEANDROS MAGLARAS

About the Authors

Papathanasaki Maria is currently a student of the postgraduate program "Computational Medicine and Biology; Informatics with applications on Security, Big Data & Simulation" in the department of Computer Science and Biomedical Informatics of the University of Thessaly. She received the B.Sc. degree in Computer Science from University of Thessaly in 2020.

Dr. Leandros A. Maglaras, is a policy analyst at the Global Foundation for Cyber Studies and Research. He is a Senior Lecturer in the School of Computer Science and Informatics of De Montfort University conducting research in the Cyber Security Centre. He obtained the B.Sc. (M.Sc. equivalent) in Electrical and Computer Engineering from the Aristotle University of Thessaloniki, Greece in 1998, M.Sc. in Industrial Production and Management from the University of Thessaly in 2004 and M.Sc. and Ph.D. degrees in Electrical; Computer Engineering from University of Thessaly, in 2008 and 2014 respectively. In 2018 he was awarded a second Ph.D. in Intrusion Detection in SCADA systems from University of Huddersfield. He served on the Editorial Board of several international peer-reviewed journals such as IEEE Access and Wiley Journal on Security and Communication Networks. He is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE) and author of more than 130 papers in scientific magazines and conferences and is a senior member of IEEE.

About GFCyber

Global Foundation for Cyber Studies and Research is an independent, non-profit and non-partisan policy research think tank for Cybersecurity studies, located in the Washington D.C, USA.

GFCyber does not express any opinion of its own, all opinions expressed in the publications are a sole intellectual representation and responsibility of the author(s).

Cover Design: Muhammad Babar Khan
Styling Credit: Amanullah Quadri

Citation Style

M. Papathanasaki, L. Maglaras, “The Current Posture of Cyber Warfare and Cyber Terrorism”, Global Foundation for Cyber Studies and Research, June 2020.

The Current Posture of Cyber Warfare and Cyber Terrorism

Abstract

Cyberspace has a dark side, including terrorism, bullying, and other types of violence. It is essential to note that Cyberwarfare is still a kind of virtual war that causes the same destruction to a state that a physical war would also do. In this article, we discuss about cyber Warfare and Cyber Terrorism and outline their different types, motivation and countermeasures. The article concludes with the key findings from the literature and suggests avenues for future research efforts.

Cyber Warfare

From the first years of its existence, people undeniably benefit from the Internet. However, only a few comprehend that the e-world is fraught with danger. Unfortunately, Cyberspace has a dark side, including terrorism, bullying, and other types of violence. The dark web is becoming more and more popular among the youth and a portion of criminals [1]. According to V. Giannakopoulos [2], Cyberwarfare is every action that takes place in Cyberspace and targets against the power of a country or other non-governmental entity (companies, organizations, etc.). Cyberwarfare can cause physical destruction via computers. It is actually accomplishing military operations using virtual means. This way, countries manage to achieve missions that would require the physical presence of the army. For instance, China has been accused of performing cyber-attacks against Taiwan to weaken the economy of the country. It is essential to note that Cyberwarfare is still a kind of virtual war that causes the same destruction to a state that a physical war would also do. Of course, there is a huge possibility that an e-war can lead to a physical one, causing even more destruction. In summary, we could say Cyberwarfare is the techniques and tactics a country uses virtually and physically, simultaneously or alternately, for an extended period against another state.

Cyber Warfare Types

There are many types of warfare that act individually or combined. Most important of them are presented below:

i. Espionage

Several countries have been accused of spying over others using their secret agencies by recording phone calls in countries like the Bahamas, Afghanistan, Mexico, and others. Whereas, some countries resorted to spying on the electronic diplomatic communication channels.

ii. Sabotage

To better understand that type of cyber warfare, we will talk about Stuxnet. In June 2010, a virus named Stuxnet made its appearance in power plants, traffic control systems, and factories around the world. Stuxnet appears to be twenty times more complex than the most complex virus until then and has many strengths; one of those was the ability to turn up the pressure inside nuclear reactors. Basically, it is a weapon made entirely out of code. What makes Stuxnet even scarier is its capability to make everything seem normal to the engineers. That virus could enter into the systems by security gaps that system creators were unaware of, named zero days. Such gaps can be sold on the black market for $100.000, and Stuxnet bought twenty of them. The creator of the virus targeted a nuclear factory in Iran and managed to shut down a thousand centrifuges in the reactors, leading the Iranian government to suspend the work of all its nuclear facilities without any explanation. Months later, the government stated that, indeed, Stuxnet infected their nuclear factories, and should nobody noticed that, it would lead to a national electricity blackout. What was Iran's response to the attack? They made an open call for hackers to join the Iranian Revolutionary Guard, creating the second-largest online army worldwide. To this day, we do not know for sure who was behind the attack [3]. Nine months after the attack, Stuxnet was redesigned, this time even better, to be able to destroy oil pipelines or power grids, and it is available to anyone to download. Stuxnet is an open-source weapon, free for everyone to play with, including the next person who will use it against a nation.

iii. Denial of service attack

Such type of attack aims to make people unable to reach a network resource or make a machine unavailable to users. Attackers often target banks, credit card payment gateways, and other high-profile web servers.

iv. Electrical power grid

An electrical power grid is a network for delivering electricity from producers to consumers. A country can infiltrate another country's electrical grid and leave inside any virus that can disrupt the whole system, like the attack against the U.S. in April 2009. Another example is the attack against half of Turkey, causing a power outage for twelve hours. The most recent attack was made against Russia in June 2019, fortunately without consequences because of the Russian government's prompt actions. It is recommended that all countries disconnect the power grid from the Internet and run the net with droop speed control, to avoid such attacks [4].

v. Propaganda

Cyber propaganda is any type of misinformation, and psychological control of people, using the Internet. According to Jowett and O'Donnell, "propaganda is the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist" [5]. People who try to propagandize others often use any way possible to brainwash internet users in order to make them serve their purposes.

vi. Economic disruption

In 2017 a huge attack took place in Ukraine's and U.S.'s National Health Service, using malicious software to make disruptions. Those attacks aim to harm a company's economy, which is also referred to as financial crime [6].

vii. Surprise cyber attack

Such attacks have as a primary goal to draw attention. The bigger the attention they get, the more successful the attack is. A well-known surprise cyberattack was al-Qaeda's 9/11 attack against the USA, which was broadcasted worldwide.

Motivation and Ethics

What makes Cyberwarfare appealing to more and more countries is a very simple reason. As always, money counts, and in the case of a war, they count even more. Cyberwar costs less than a physical one, and it also offers the opportunity to weaken another nation without risking people's lives. Most of the attacks are politically motivated. For instance, in 2008, hackers attacked CNN. The same year hackers attacked the Georgian government website while the Georgian army was in South Ossetia.

Another motivation for causing a cyber-attack is the sabotaging Internet itself. Hackers are trying to break into web servers, communication links, businesses, and homes, harming internet service providers, electrical grids, financial networks, etc.

Some attacks are used to produce income for the attacker. Some ransomware can be used by countries to ensure a noticeable profit causing long-term damages to their targets. From the other side of the coin, some organizations are motivated by the need of our time for web safety. For example, Kaspersky Lab examines the issue of Cyberwarfare and tries to raise awareness amongst the internet community. Traditional wars are guided by the Just War Theory (JWT). Several well-defined principles state when a nation is ethically justified to go to war and remain ethical during one. However, are these principles applicable when it comes to cyber-warfare?

It is essential to mention that a physical war should be avoided until all other options have been exhausted. On the other side, a Cyberwar is preferable against a physical one, since bloodshed and material damage do not directly occur. People from different nations may not kill each other as it is used to happen in real wars, but a cyberattack against power and food supplies can lead to numerous deaths too. Currently, there are no agreed ethical guidelines for Cyberwarfare. Some researchers have tried to transfer the existing legislature into the cyber world, but to this day, warfare ethics are unstable.

Opposing Cyber Warfare

Modern society depends on the Internet more than ever. To ensure our safety, it has been stated that sub-webs should be built since rebuilding the whole Internet is extremely difficult. Sub-webs are going to be equipped with the latest safety protocols. In 2012 a company named Artemis expressed interest in creating such a "secure place". The user had to type ‘secure’ at the end of the site address he wanted to visit and was part of the Artemis sub-web. However, Artemis offered safety only to the websites and not the users themselves, exposing them to any kind of malware. Up to date, nobody has managed to make a sub-web safe enough for users.

Another solution is to cut the Internet off from an area that is being attacked. That would be a great solution if it were not for the citizens of that area who would not appreciate the inability to connect to the Internet. An attack that took place in 2012 worldwide almost led the FBI to shut down the connection of the infected area in which more than a million computers existed. To avoid that, they installed two of their own internet servers until they arrested the attackers. All organizations ought to have emergency servers to use in case of an attack. Last but not least, we have to understand the limits of each country into Cyberspace. There are limits to every state power in Cyberspace and should not be exceeded. Moreover, each government has to reorganize its Cybersecurity and try through a new curriculum to help young people acquire more developed critical thinking.

Cyber Terrorism

In 1997 Dr. Barry C. Collin proposed the term “Cyberterrorism” for the first time. He described it initially as a premeditated attack on computer systems and data by terrorists. A few years later, all internet terrorism activities were included in the definition of that term. Today, cyber terrorism is considered as every terrorism that uses the Internet as a tool or the network as an attack target [7]. According to FBI, cyber terrorism is a *“premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents”.*

But is Cyberterrorism worth such fear from us? To this day, no attacks related to physical war have taken place, making Cyberterrorism probably a misnomer. P.W. Singer and Allan Friedman in their book [8], mention that "Cyberterrorism is like a famous T.V. program named "Shark Week," in which is shown that people every year are more likely to die by an accident involving a toilet, than a shark”. Despite this fact, people are more afraid of dying by a shark than a toilet. Why is that happening? Apparently, we are more afraid of what media, films, or others make us fear. We can easily compare the sharks to Cyberterrorism attacks. People nowadays are terrified of that term as much as other reasons for death. However, as it is mentioned above, Cyberterrorism has not killed or hurt anyone physically yet. What is the reason that makes people afraid of Cyberterrorism? Unfortunately, ignorance is a significant enemy of somebody's composure. Most internet users cannot distinguish the real danger from an insignificant threat.

Cyberterrorism tries to inflame rebellions in the heart of a nation, destroying its peace. However, Cyberterrorism is not only about national infrastructure sabotaging. For example, even a warning message for a bomb in a public building is considered to be Cyberterrorism. Also, that term refers to acts that hackers do against people in order to spread fear, show off their powers, or even destroy their lives by blackmailing them.

It is significant to make a distinction between Cyberterrorism and Cybercrime. Although they are similar terms, they should contend with a different approach by society. Cyberterrorism, in particular, most of the time, has political motives, but Cybercrime, by contrast, takes place on a more personal level. Certainly, both of the purposes of the terms are to cause harm, but the reasons that lead to that are different. The main goal of Cyberterrorism is to discourage the masses from raising their voice and propagandize them.

Cyber Terrorism Types

Cyberterrorism depending on the way of technology is used to cause harm, can be categorized into six parts, according to Susan Brenner [9]:

I. Weapons of mass destruction

According to S. Brenner, such attacks are not realistic, since computers do not own the power to provoke physical destruction directly to any kind of property. However, they can foment indirect ways that are going to provoke the physical destructions eventually. She also mentions that the Chernobyl disaster in 1986, could have easily been caused by cyber terrorists. For example, they could have broken into the security systems and make the reactors explode. Then they would take advantage of the deaths that happened and turn the people against the government.

II. Weapons of mass distraction

To better understand this category, let’s re-inspect the terrorist attacks of the 11th of September 2001 wherein, a terrorist group ‘Al-Qaeda’ (meaning: The Foundation) hijacked four passenger airplanes, setting them out to fly into both world trade center (Twin Towers) and the Pentagon. As a result, the attacks caused the death of 2986 people, including the hijackers, and at least 10.000.000.000$ in infrastructure damage. Millions of Americans where watching live the attacks on television, and even more, were trying to reach CNN's official website to get more information about the hijacks. So, what is the factor that would make al-Qaeda terrorism a weapon of mass destruction? Imagine the people who visited the CNN website, instead of seeing the real front page, to see a mirror of that page that shows fake news about other attacks worldwide. That would make people scared even more, and probably it would trigger more terrorist attacks and riots, making computers the real mass destruction weapons.

III. Weapons of mass disruption

Mass disruption weapons aim to make public infrastructure (means of mass transportation, health services, financial institutions, etc.) unreliable to citizens. This time cyber terrorists are trying to cause mental damage to people instead of physical. For example, let's take the "Botnet" malware that managed to turn the Seattle's Northwest Hospital into chaos. In January 2005, Christopher Maxwell, a twenty-year-old young man from California, infected the hospital network, blocking surgery room doors, moreover doctors' beeper and intensive care unit's machines stopped working.

IV. Cyberwarfare

It has been clear from the previous section what Cyberwarfare is and how it affects modern society.

V. Hybrid warfare

Hybrid warfare is a kind of Cyberwarfare that apart from uninformed people, others participate too. To be more specific, hybrid warfare combines the army with diplomats, hackers, journalists, and even civilians. All these forces combined, make an extraordinary powerful group that can easily propagandize people. On the 21st of November 2013 in Crimea (Ukraine), civilians rose in protest against the President of Ukraine, because of his denial to sign his country's union with more than four million people were united under one force to fight against the president. Who managed to gather that massive amount of people, though? We cannot be sure who provoked the upheaval, but we know that whoever did this was preparing the whole mission for a long time until the time was right to attack. As Cyberwarfare evolves, more and more hybrid attacks occur, and a new term is born: Unlimited Warfare.

VI. Unlimited Warfare

That kind of war is an upcoming way to attack another nation without any barrier. It is said that the first rule of Unlimited Warfare is the absence of rules and limits. Apparently, that "rule" violates any ethical border and leads people to act without any reservations. Unrestricted warfare can be extremely dangerous to modern society due to the lack of respect amongst developed countries. Undeniably the sense of justice and safety is affected during a war. In the case of unlimited warfare, we are talking about a total demolition of what current societies have built.

Cyber Terrorism in Social Media

Cyber Terrorism in social media is used for identity theft, online fraud, cyber-attacks, and other reasons. What are the threat categories in social media for cyber terrorism, and how do attackers use social media? As it has been mentioned before, Cyberterrorism is a premeditated electronic attack against civilians to cause harm or spread fear.

Because social media are accessible for people of all ages worldwide, cyberterrorists can easily approach someone and detach useful information, making 90% of Cyberterrorism to happen through social media. According to Lockheed Martin Corporation, the stages of intrusion kill chain (IKC) are four:

i. Information Gathering: collecting information.
ii. Weaponization: Developing malicious code.
iii. Exploitation: Execution of the malicious code.
iv. Installation: Installation of malicious programs.

Usually, cyber terrorists are trying to harm somebody’s reputation, destroy his life, or weaken his mental balance. They also aim to cause more extensive harm, like destroying a company’s public profile.

Opposing Cyber Terrorism

The Internet is being used more and more every day by people. What measurements should we take to keep ourselves safe, and what do governments ought to do to maintain their stability?

On a personal level, we have to be careful with the information we share. Moreover, we should block any spam accounts we detect and avoid chatting with unknown to us people. We also have to stop using hashtags because they make our profile easier to find. When we face misinformation, we should report them, and double-check the news we read online. It is essential to get informed from reliable sites, and never reading just the title of an article because it could be misleading.

A new growing phenomenon in social media is ‘crowdturfing’ (crowdsourcing + astroturfing). Crowdturfing uses misleading "posters," which present to their page followers, making them build a negative or positive opinion about a subject by presenting fake views of others. That way of propagandizing can help the spread of cyber-rumors about a person or a company. Crowdturfing puts information integrity and authenticity into risk, so we should have critical thinking before making any decision. For instance, social media can use a pop-up that reminds users about the misinformation consequences, aiming their ethical logic [10]. It goes without saying that all computers with internet access should have installed updated antivirus software, and all users have to protect their passwords and their sensitive information. As Marwan Albahar stated*:*

“if technology can take us to the moon, a breakdown or compromise of the same will ensure that we stay there forever and never return” [11].

Research into conducting and understanding cyber warfare and cyber terrorism is extensive and wide-ranging [12], yet research into restoring peace after cyber warfare has recently been addressed [13]. Attribution of cyber-attacks is an open issue [14] and the correct norms and procedures are yet to be discovered. Some solutions for security the systems and specifically Critical Infrastructures must be put forward in National or International level [15].

References

[1] V. M. Vilić, "https://www.ceeol.com," 1 10 2017. [Online]. Available: https://www.ceeol.com/search/article-detail?id=648914. [Accessed 5 5 2020].

[2] Β. Γιαννακόπουλος, "Κυβερνοπόλεμος: υπαρκτή παγκόσμια ασύμμετρη απειλή.," [Online]. Available: http://www.geostrategy.gr. [Accessed 12 05 2020].

[3] R. Langner, Interviewee, Cracking Stuxnet, a 21st-century cyber weapon. [Interview]. 1 03 2011.

[4] M. Halpern, "OBSERVER," 22 04 2015. [Online]. Available: https://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/. [Accessed 30 05 22].

[5] G. S. Jowett and V. O'Donnell, Propaganda and Persuasion, 5 ed., Los Angeles, London, New Delhi, Singapore, Washington DC: Library of Congress Cataloging-in-Publication Data, 2012, p. 7.

[6] S. Frenkel, M. Scott and N. Perlroth, "The New York Times: Cyberattack Hits Ukraine Then Spreads Internationally," 27 06 2017. [Online]. Available: https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html. [Accessed 17 05 2020].

[7] J. Wang and C. Wu, "Analysis of Cyberterrorism and Online Social Media," in Proceedings of the 2019 4th International Conference on Modern Management, Education Technology and Social Science (MMETSS 2019), China, 2019.

[8] P. W. Singer and A. Friedman, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW®",, New York: Oxford University Press, 2014.

[9] S. W. Brenner, ""At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare," Northwestern University, School of Law, Illinois, 2007.

[10] A. Parlakkılıç, "Cyber Terrorism Through Social Media: A Categorical Based Preventive Approach," Department of Management Information Systems, Ufuk University, Turkey, 2018.

[11] A. Marwan, "Cyber Attacks and Terrorism: A Twenty-First Century Conundrum," Springer Science+Business Media, Dordrecht, Netherlands, 2016.

[12] Robinson, Michael, et al. "Developing cyber peacekeeping: Observation, monitoring and reporting." Government Information Quarterly 36.2 (2019): 276-293.

[13] Ayres, Nicholas, and Leandros A. Maglaras. "Cyberterrorism targeting the general public through social media." *Security and Communication Networks* 9.15 (2016): 2864-2875.

[14] Cook, Allan, et al. "Attribution of cyber-attacks on industrial control systems." *EAI Endorsed Trans. Indust. Netw. & Intellig. Syst.* 3.7 (2016): e3.

[15] Drivas, G., Chatzopoulou, A., Maglaras, L., Lambrinoudakis, C., Cook, A., & Janicke, H. A NIS Directive compliant Cybersecurity Maturity Assessment Framework. *arXiv preprint arXiv:2004.10411*. (2020)

Global Foundation for Cyber Studies and Research (GFCYBER) is an independent, nonprofit and non-partisan think tank, which conducts studies and research and provides consultation on cyberspace challenges and issues from the intersecting dimensions of policy and technology for the betterment of a globally-connected world. The foundation works on the philosophy that together we can secure the cyberspace!

Contact Us:

5614 Connecticut Avenue, N.W., No. 209,
Washington, D.C. 20015, USA.

www www.gfcyber.org
✉ info@gfcyber.org
@gfcyber