Is Cyberspace at Risk of Being “Militarized”?

Joey Navarrete

Old Dominion University

Saltuk Karahan

CYSE 426: Cyber War

11/23/2022

Is Cyberspace at Risk of Being “Militarized”?

Introduction

In the modern world of technology, there has become a prominent growth in cyberspace. Cyberspace has allowed us to make some tremendous strides not only in the technological world, but as well in our personal lives, along with the greater society overall. But, before we talk about the wonders of cyberspace, we must first find out what exactly cyberspace is and what its origins are.

Starting with the prefix of the word “cyber-“ , we know that that term has a rather strong connection to the computer and networking world. The main term that comes to mind when discussing the term “cyber” is cybersecurity. Cybersecurity is a vast world of computer networking that ensures the security and protection of computer systems and networks from a plethora of things, primarily including theft, cyber attacks, and unauthorized access of said computer systems and networks. There are still a countless amount of things in the world of cyber that we do not know about yet, and as we find more stuff, we begin to question how large the cyber world actually is. That is where the suffix “-space” comes in to play. As we have still only theoretically scratched the surface of the cyber world, that makes it one extremely large place that we know very little about. For a comparison, another vast environment that we know little to none about is outer space. It appears that the suffix “-space” in cyberspace was derived from actual outer space, which makes sense because of the significantly large size of both are something that we do not have complete clearance on. More specifically, cyberspace can be defined as “a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and

controllers.” (National Institute of Standards and Technology, 2012). The term cyberspace was first coined by American-Canadian author William Gibson in 1982, but did not gain relevance until his 1984 book “Neuromancer”. In cyberspace, a variety of things can be done, including the sharing of information, the connection of new perspectives and ideas, the playing of games, and the interaction of people.

Answering the Question

With all that cyberspace brings to the table, there have become growing concerns that cyberspace will soon undergo the major risk of being militarized. Unfortunately, while this question is currently being asked, it appears that it just might be too late to ask that question. In recent years, with the inevitable evolution of technology, many nations around the world are already turning their direction towards implementing cyberspace in their militaries. In an article from Frederick Douzet and Aude Gery, they believe that cyberspace has already been at risk of being militarized starting around some time in the late 2000s. Moreso, they asserted that many nations around the world have already considered using cyberspace as a new military domain. “The representation of cyberspace as a new military domain emerged during the 2010s, the last step in the territorialization of cyberspace by states in reaction to the multiplication of the strategic surprises they had faced there since the late 2000s.” (Douzet & Gery, 2021). While cyberspace can most certainly be grouped in with the other four domains of land, sea, air, and space, cyberspace is still nothing like the other ones. It was found that “cyberspace is constructed by man and constantly under construction. It changes from moment to moment. Military interest in cyberspace is dominated by the use of networks for friendly and adversary operations” (Welch). Since we technically have

control over cyberspace and is man-made, that makes it completely different from the rest of the other four domains. This militarization of cyberspace has led to the tremendous growth of cyber warfare. Cyber warfare can be defined as nations implementing cyberspace in attempt to cause damage to another country, whether that damage be a country’s security and computer systems, or the personal data of its citizens. Cyber warfare is also something that has become more common in the last few decades, as revolutionary technology has allowed us to do things that we had never imagined before. Prior to the end of the 2000s, cyberspace served the primary purpose of stopping users from preventing many types of cyber crimes. Ever since then, nations in power have turned to using cyberspace for political and military purposes. But why did this change happen so suddenly? The most obvious answer for this is society’s dependency on modern technology. Technology is one of the largest factors in everyone’s lives, so it is not a surprise that both the governments and militaries of the world rely on technology as well. To find a better idea of why cyberspace has become militarized and used for offensive purposes, we must first learn about the origins of cyberspace and how its militarization began.

Origins of Cyberspace Militarization

As stated earlier, the term “cyberspace” first came from author William Gibson in 1982, but did not become known worldwide until 1984. In his novel “Neuromancer”, Gibson described cyberspace as “a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by being taught mathematical concepts… A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the

non-space of the mind, clusters and constellations of data” (TechTerms.com). Cyber attacks have been occurring since well before the 21st century, but at that time, it was not done for political or militaristic purposes. The first instance of cyberspace being weaponized for either political or militaristic purposes was first discovered in 2010, that being the Stuxnet worm. The Stuxnet worm was first discovered in June of 2010, and is considered to be responsible for an extreme amount of damage to the nuclear program of Iran at a facility in the city of Natanz, Iran (Gomez, 2016). However, the first instance of cyberspace being weaponized for military purposes, Stuxnet was first developed in 2005. Along with the conflict in the air, sea, land, and space, cyberspace was finally recognized as a military domain in 2004 by the Joint Chiefs of Staff. Although the Stuxnet worm of 2010 has been the first instance where the government of a state implemented cyberspace to attack another state, there is no clear-cut evidence of that being the case. “It may never be possible to know for certain who gave the order to program Stuxnet, who actually did it, and what the intent behind it was. However, this is strangely irrelevant: The only thing that does not matter in this instance is what states make of it – because it is their actions and reactions that create political reality” (Cavelty, 2012). It took some time to figure out who exactly created the Stuxnet, but it was later found that both the United States and Israel were involved in doing so. “Under the leadership of the US National Security Agency (NSA), the joint operation was tasked with developing a virus or other form of malware that didn’t just infect computers, but could actually damage physical infrastructure too” (Buxton, 2022). The general belief among the public and those in power was that cyberspace had nothing to do with offensive cyber operations (OCOs) (Gomez, 2016). However, that opinion quickly changed with the discovery of the 2010 Stuxnet worm.

Countermeasures To Be Taken Against Militarization of Cyberspace?

We also know that it is too late to consider the militarization of cyberspace as a risk, as it has already been implemented worldwide for nearly the last two decades. With the militarization of cyberspace already taking place not too long ago, the general public and governments alike are most likely wondering what measures can be taken place to prevent their nations from becoming the victims of OCOs. The simplest answer is that there are no new measures that can be taken. However, if a nation could do something to prevent OCOs from happening to them, that thing would be cyber deterrence. First off, deterrence can be defined as “the prevention of action by either the existence of a credible threat of unacceptable counteraction and/or the belief that the cost of action outweighs the perceived benefits” (McKenzie, 2017). To get the bigger picture about cyber deterrence, we need to look at how a certain nation approaches this situation.

The United States is one of the most prominent and powerful nations when it comes to their cyber operations. The United States does not have the clearest deterrence declaration when it comes to their cyber operations. The US National Security Strategy (NSS) also does not have the strongest declaration when it comes to how it is worded. In their deterrence declaration they say that “we will deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks by . . . investing in people in technology . . . [and] strengthening partnerships” (McKenzie, 2017). To add on, the NSS only adds a little more to that, saying that they will “strengthen our international partnerships on . . . the development of norms for acceptable conduct in cyberspace . . . [and] laws concerning cybercrime” (McKenzie, 2017). They say that they are looking to deter any possible attacks against the U.S., but they do not bring up any kind of

punishment for those who attempt to attack the country. The US has another policy for cyberspace with the International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. In this document, it says the goal of the US for the future of cyberspace is to “work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, [the United States] will build and sustain an environment in which *norms of responsible behavior* guide states’ actions, sustain partnerships, and support the rule of law in cyberspace.” (McKenzie, 2017). There is one more document that has information on the US’s plans on cyber deterrence, which is the 2011 Department of Defense Strategy for Operating in Cyber Space. There are three specific instances where they will activate cyber deterrence:

1. Theft or exploitation of data
2. Disruption or denial of access services that affects the availability of networks, information, or network-enabled resources
3. Destructive action including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems. (McKenzie, 2017)

Should We Consider Lessening the Militarization of Cyberspace?

With the evolution of modern technology along with the intensifying of cyber conflicts worldwide, I believe that some things should be taken into consideration about militarizing cyberspace. Also, along with all the cyber attacks and threats that occur in a non-governmental/militaristic way and all the economic and societal harm that they

cause, this question should be brought up: Are we doing too much? Along with the measures that are taken by countries in attempt to deter militarized cyberspace from opposing nations, could there be a way to deter the use of militarized cyberspace as a whole? There is an extremely high amount of risk that can go into militarizing cyberspace. When dealing with the risk “as with militarization, there is currently no quantitative state-level measure for risk in cyberspace” (Gomez, 2016). When a cyber attack occurs to a large company or business, the damages that are done could be majorly destructive, and could take years, even decades to recover from. If that same kind of damage is done to large national governments, and there is little to no protection of that that government, the damages could be considered “earth-shattering.” Going back to the incident of the Stuxnet worm in 2010, the damages done in that speak for itself. “Therefore, Stuxnet is probably the most expensive malware ever found. In addition, it behaves differently from the normal criminal-type malware: it does not steal information and it does not herd infected computers into so-called botnets to launch further attacks from” (Cavelty, 2012). While there are many risks of militarizing cyberspace, there also comes with that some unwanted side effects. For example, if cyberspace was militarized, there could be the possibility of the military and government gaining access to the critical infrastructure of opposing nations, which in turn could lead to devastating damage worldwide of said critical infrastructure. With all that being said, I believe that any country that plans on/already has militarized cyberspace should consider the long term effects of using cyberspace as a weapon. There is no reason to cause such unnecessary damage to those who do not deserve it.

Conclusion

Is Cyberspace at Risk of Being “Militarized”?

Although cyberspace has already been militarized in the last decade, there are still great risks and dangers that could happen if this progresses any further. Cyberspace brings great potential to the modern world of technology. However, with the way that cyberspace could possibly be utilized by the military and the government, the cyber world could potentially face some devastating damages. It is no surprise that cyberspace became another domain for the military as soon as it did. Governments all around the world have already caused damages with the other four domains of sea, land, air, and space, so it is expected that cyberspace will be damaged as well. For example, the 2010 Stuxnet worm is proof damage can be done in this fifth domain, especially the economic damage that was caused by it. As for the defensive side, there are measures that can be taken to defend a state against an opposing country that militarizes cyberspace. For example, the United States has guidelines in place for if something like that were to happen. These countermeasures that can be taken are known as cyber deterrence. The United States has plenty of great guidelines that can help combat these situations, but there are also some guidelines that do not really give us any kind of clarification on what will be done to those who try to cause a cyber attack against the US. As for measures that can be taken to completely get rid of militarized cyberspace, it is a little less manageable. The main solution for this is to lessen the militarized cyberspace that already exists. This seems to be one of the only ways to prevent the growth of conflict between opposing nations. In the near future, one could hope that nations realize that militarizing cyberspace can cause unnecessary harm to not only opposing nations, but also to their own citizens.

References

Buxton, Oliver (2022). *Stuxnet: What Is It & How Does It Work?* Avast, https://www.avast.com/c-stuxnet

Cavelty, Myriam D. (2012). *The Militarisation of Cyberspace: Why Less May Be Better*, Swiss Federal Institute of Technology Center for Security Studies, https://ccdcoe.org/uploads/2012/01/2_6_Dunn-Cavelty_TheMilitarisationOfCyberspace.pdf

Cyberspace. TechTerms.com, https://techterms.com/definition/cyberspace

Guide for Conducting Risk Assessments, National Institute of Standards and Technology, U.S. Department of Commerce, appendix B, page B-3, September 2012, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Douzet, Frederick & Gery, Aude. *Cyberspace is used, first and foremost, to wage wars: proliferation, security and stability in cyberspace*, Journal of Cyber Policy, pg. 96-113, June 9, 2021, https://www.tandfonline.com/doi/pdf/10.1080/23738871.2021.1937253?needAccess=true

Gomez, Miguel, Alberto N. (2016) *Arming Cyberspace: The Militarization of a Virtual Domain, Global Security and Intelligence Studies*: Vol. 1: No 2, Article 5, https://www.ibei.org/arming-cyberspace-the-militarization-of-a-virtual-domain_54871.pdf

Is Cyberspace at Risk of Being “Militarized”?

McKenzie, Timothy M. (2017). *Is Cyber Deterrence Possible?* Air University, https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF

Welch, Larry D. *Cyberspace – The Fifth Operational Domain*, Institute for Defense Analyses (IDA) https://www.ida.org/-/media/feature/publications/2/20/2011-cyberspace---the-fifth-operational-domain/2011-cyberspace---the-fifth-operational-domain.ashx#:~:text=That%20is%2C%20cyberspace%20is%20a,sea%2C%20air%2C%20and%20space.