Old Dominion University

CYSE 426 Cyber War

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Project Paper

Jacob Cagle

**Introduction**

Over the past 20 years technology has advanced at an unprecedented rate. So much so that the world we knew before has changed and the way in which we operate in the world has also changed. Technology as a whole has rapidly advanced when we compare it to the world just 10 years ago. The main contributor to the world’s rapid change is the internet. The internet was just being introduced in the 90’s, and today the internet is integrated into everything that we do. The rate at which we rely on the internet now compared to 20 years ago is astonishing. We use the internet to communicate, buy/sell items, and even how some people create their identity. Needless to say the internet quickly grew into something that we as humans rely on. As we rely on technology more of our information is being put on the internet for the world to see. Thus cyberspace has emerged into a place where people and countries can benefit socially and economically. Conversely, as cyberspace is being relied upon more, this has turned it into a new area of competition and conflict throughout the world. The same devices/technology that are being used for global communication are the same devices that can be used for surveillance and ways for countries to have a strategic advantage over other countries. This shift in the cyber domain has led to the question: Is cyberspace at risk of being militarized? The growing initiative of cyber focused doctrines throughout the world’s militaries tends to suggest that maybe cyberspace is turning into a new area of warfare. We have also seen an increased number of state sponsored cyber hacking groups and even the use of cyberattacks on governmental elections. Throughout this paper I will talk about how cyberspace has evolved from being a mainly communicative platform into a new potential area of warfare. Throughout this I will also look at the risks and consequences that come up when talking about the militarization of cyberspace.

**The Beginning of Cyber Operations in Military Strategy**

Over the past couple of years cyber warfare has been a growing topic among militaries. Nation’s across the world have realized how important the cyber domain is to the future of our growing world. Countries began to see how much our everyday world utilizes the cyber domain and our dependence on it. In the 2000’s when the dependance on the internet emerged, so did a new threat. This new threat could not be defended by missiles or aircraft but by cybersecurity. Many forms of the world’s digital infrastructure were vulnerable to cyber attacks. This included financial businesses to hospitals. These systems with sensitive information were vulnerable and now accessible via the cyber domain. Any and all information that was on the internet was now accessible and obtainable by anyone who wanted it. For governments and militaries around the world this was both a threat and an opportunity to gain information/intelligence.

This opportunity was initially seen as a means of surveillance and intel. This encouraged many countries/states to invest into capabilities that would gather intelligence to support war efforts/offer advantages. Some of these investments from countries would go towards cyber capabilities that would illegally go into foreign networks and gather sensitive information that had little risk due to the attacks being non-attributable. These attacks were very disruptive to the targets and provided little risk to the attacker. This was quickly realized by militaries across the world and this innovation quickly forced militaries to adapt and include cyber operations into their strategic planning. Some attacks that occurred in the early 2000’s into the early 2010’s encouraged militaries to implement cyber operations into their strategy and further develop doctrine to combat future cyber threats. For example, in 2007 Estonia fell under one of the first major cyber attacks that showcased what kind of damage could be done through cyberspace without a single kinetic effect. In April of that year, Estonia was attacked using specific cyber attacks like Denial of Service which temporarily shut down systems within the Estonian government. This attack targeted a lot of non essential systems like e-mails and public domains. However, this attack also targeted essential services like banking and sensitive records. The cause of this attack was due to a political situation involving a monument. In another example, a cyberespionage group called the GhostNet, used servers to gain access to classified documents from governments and private organizations from over 100 countries. These attacks and the motive behind them showed the world how dangerous cyberspace can be if not defended properly. Following these attacks, and the example of what can be done was set, countries quickly committed to funding their cyber infrastructure. Funding this infrastructure consisted of building up the defensive infrastructure that could protect against cyber attacks such as the one against Estonia in 2007. Furthermore, these attacks also showed countries/militaries what could be done when it comes to offensive cyber operations. Thus nations pushed to fund their offensive cyber operations and this opened up the capability of cyber operations in the future.

Some of the major militaries in the world began directly involving cyberspace into their military planning and incorporating cyber operations into their military doctrine. For example, in 2009 the United States established the U.S. Cyber Command which signaled to the world that cyberspace was being taken seriously and is being included in military strategy on a large scale. Similarly, both Russia and China made a push to directly involve cyber operations into their broader militarily strategy and doctrine. This opened up a future of conflict in cyberspace between major military powers. Countries around the world began to implement cyber operations into their military's strategy/doctrine in response to a potential threat and new generation of warfare.

**Cyber Militarization amongst the three global powers**

As previously stated, due to the previous attacks and utilization of cyber attacks the U.S., China, and Russia all invested in developing their cyber operations for defensive and offensive cyber operations. However, they all differ in how they incorporated the use of cyberspace into their military strategy. These countries have viewed how they should use cyberspace in their militaires differently based on how they view cyberspace as a threat and how their military operates. Looking at some of the differences between countries and how these countries incorporated cyberspace into their militaries will help determine how cyberspace is inching closer to become a militarized domain.

The United States incorporates cyberspace into their military by building up their defensive cyber operations more than anything. In one of my previous papers I talk about the United States and how they execute and look at cyberspace as a means of military strategy. I talked about Shadow Warfare from the book, “Shadow Warfare” by Van Wie Davis. In this book Shadow Warfare refers to a level of conflict that operates below the line of traditional warfare that prioritizes conducting military operations without developing a response from adversaries. This shadow warfare explains cyberwarfare as, “ continuous and strives to be unseen, making a state of war permanent.” ( Davis, p.xi) A lot of how the United States operates in cyberspace revolves around Shadow Warfare. For example, as stated in my previous paper, the United States looks to incorporate Shadow Warfare into their cyber strategy by making a potential attack too costly for an adversary to go forth with such an action. The United States overall strategy revolves around protection of national security and their power globally. As previously stated, this is all outlined in the United States military U.S. Cyber Command that was introduced following the attack on Estonia in 2007.

China’s strategy when it comes to militarizing cyberspace comes from their knowledge of past events and what can happen if they fall behind their adversaries in cyberspace. They realize that they need to develop their cyber capabilities to keep up with their adversaries and they view cyberspace as more of a weapon in comparison to the United States. China is much more focused on offensive cyber operations in comparison to the United States. To quote my paper and more specifically Van Wie Davis in “Shadow Warfare”, “ the ability to disrupt the command and control systems of an adversary’s military, the ability to fend off international malware and withstand DDoS attacks, and a capability to impose similar cyberattacks on others.” ( Davis. p.85) These three main points are how China operates in cyberspace. These three main points are how China views cyberspace and as we can see from them, China takes a more offensive approach to cyberspace. While China has changed their approach to militarizing cyberspace over the course of the past 10 years, they are more focused on developing their offensive cyber operations.

Russia’s cyber strategy revolves around, “the destruction of command and control centers combined with an electromagnetic attack on information and telecommunications systems; the acquisition of intelligence; disruption of computer systems; and disinformation.” (Davis, p.52) Later stated in “Shadow Warfare” by Van Wie Davis Russia’s doctrine is based around, “establishing full state control over the domestic cyberspace, overcoming the international “discrimination” of the Russian media, and growing concerns that Russia is lagging behind other key players in the domain of information technology and cybersecurity.” ( Davis, p.53) Continuing to reference my previous paper on Russia and their doctrine in cyberwarfare, we can see that Russia uses tactics in cyberwarfare like disinformation. They also focus on increasing their control over the cyber domain in order to ensure that they secure their countries national security as well.

As we see when comparing these three countries, they all have different ways in which they want to militarize cyberspace. This indicates that cyberspace is/has become a method of warfare and a militarized tool of power for nation’s and their militaries. In today’s military we see that cyber operations are included in military strategy and are accounted for when militaries are going into war planning. Thus our question of, Is cyberspace at risk of being militarized?, is answered as we look at current events. Powerful countries are coming out with various implementations into already existing strategies that push the boundary of offensive cyber operations. With the speed in which the cyber domain is growing, the innovation in how cyberspace will be militarized will be pushed as well.

**Risks and Consequences of Militarization of Cyberspace**

As we’ve talked about previously cyberspace is being integrated into military strategies at an unprecedented rate. Some risks and consequences can come with this. These risks and consequences could change the way we fight wars, how we secure information on the internet, and could affect the civilian population within countries. Compared to traditional warfare, cyberwarfare can spill out into the civilian world much quicker and far beyond traditional warfare in some ways. When countries use offensive and defensive cyber operations, countries can be oblivious to the impact of cyberwarfare because you mainly don’t see that kinetic effect. This can take the human element out of warfare which can make cyberwarfare much more dangerous when it comes to economic infrastructure. As mentioned previously, there can be an increased chance of unintended instability on a target. This can be due to the nature of cyberattacks and how they are difficult to attribute to a specific attacker. A nation that has been attacked by another country using cyberwarfare may find it much harder to find a country responsible for the attack. This can lead to other issues like false assumptions which could escalate actions to more kinetic means like missiles and aircraft.

Another risk that comes with cyberwarfare is the blurred line between military and civilian targets. The militarization of cyberspace sometimes ignores the distinction between the two especially when we consider that some military and civilian infrastructure are sometimes run on the same network. Meaning that when a country is targeting a military installation, they are also targeting a civilian one at the same time. For example, during the NotPetya attack, the target was intended for Ukraine, but instead this cyberattack spread across different nation’s. This cyberattack has unintended consequences that spread into the civilian infrastructure that ended up affecting innocent people. This shows us that any cyberattack can spread and the civilian infrastructure is not safe from military based cyberattacks.

Additionally, cyberwarfare lacks norms as countries have not agreed to a standard of conflict like in comparison to the Geneva Convention in traditional warfare. This leaves cyberwarfare in a space where there's much more ambiguity in what can be done by private actors and militaries. Based on non attribution, any private actor hired by a country/military can effectively act in whatever way they want. Without a global agreement cyberspace remains a domain in which anything can happen. For example, some countries work on one time use vulnerabilities in which they stockpile to use in a time of need. Going back to the concept of Shadow Warfare, this war is a war that is constant and never ends. Meaning that without a norm or agreements, countries will continue to build up on weapons in times of “peace” in order to use them when the time comes. This is a big risk that we take now without a signed agreement, especially when we consider the rate at which cyberspace is innovating. The establishment of international norms is needed within cyberspace to ensure that there is a future where our digital infrastructure remains somewhat constant.

Furthermore, when we don’t have an established norm within cyberspace, we can innovate within cyberwarfare. We can refer to the war between Ukraine and Russia. The innovation of cyberwarfare can be seen when Russia utilizes the combination of traditional warfare with cyberwarfare. Russia is utilizing tactics of information warfare to further innovate the war within Ukraine. They are using disinformation in combination with political tactics that have made it hard for Ukraine to defend. Like mentioned earlier, Russia is attacking military installations within Ukraine that are simultaneously affecting their civilian infrastructure that includes hospitals and banks. This war is an example of what can happen when we lack international norms within cyberspace. Eventually cyberwar could develop into something more dangerous that could directly destroy things on a kinetic level on a wider scale. As we’ve seen with the Stuxnet attack, this was already accomplished, but can this be done on a wider scale? These are the questions that have to be asked when we are looking at the risks and consequences of cyber operations when we have no regulation on what can and what cannot be done.

**Conclusion**

In conclusion, to answer the question of, Is cyberspace at risk of being militarized? I would answer yes, and as we can see throughout what we research and gathered throughout the paper, this question is already being answered in real time. When we look at events like Stuxnet, the attack on Estonia, and the NotPetya attack we can see that the rate at which cyberspace is being militarized has been increasing. In combination with the risks and consequences that were discussed, we can conclude that with no norms within cyberspace, anything can effectively happen. What norm is there in place that talks about cyberspace and how it can’t be militarized? There is none, which leads me to think that with the rapid growth of innovative ideas and technology, there is a risk of cyberspace becoming militarized in the future.

**Works Cited:**

Olszewski, B. (2016). Militarization of cyber space and multidimensionality of security. *Zeszyty Naukowe/Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. T. Kościuszki*.

Alberto N. Gomez, M. (n.d.). Arming Cyberspace: the militarization of a virtual domain. *Global Security and Intelligence Studies - Volume 1, Number 2 - Spring 2016*. <https://www.researchgate.net/publication/307438579_Militarization_of_Cyber_Space_and_Multidimensionality_of_Security>

Ottis, R. & Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. (n.d.). *Analysis of the 2007 Cyber Attacks Against Estonia From the Information Warfare Perspective*. https://ccdcoe.org/uploads/2018/10/Ottis2008\_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Patacsil, P. K. (2021). *The Design and Evolution of the United States Cyber Command* (Order No. 28492464). Available from ProQuest Dissertations & Theses Global. (2572618935). <http://proxy.lib.odu.edu/login?url=https://www.proquest.com/dissertations-theses/design-evolution-united-states-cyber-command/docview/2572618935/se-2>

Van Wie Davis, E. (2021). *Shadow Warfare*. <https://doi.org/10.5771/9781538149683>

Krasznay, C. (2020). Case study: The notpetya campaign. *Információés kiberbiztonság*, 485-499.

[Case-Study-The-NotPetya-Campaign.pdf](https://www.researchgate.net/profile/Csaba-Krasznay/publication/353072644_Case_Study_The_NotPetya_Campaign/links/60e6bbe00fbf460db8ee783d/Case-Study-The-NotPetya-Campaign.pdf)

*Book Analysis 3*. (n.d.). Retrieved April 6, 2025, from <https://docs.google.com/document/d/164AcHYjYowfdsleEqrGLodhkWsdIAZMy104eIF7ptWQ/edit?tab=t.0>

Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2025). *Cyber Operations during the Russo-Ukrainian War*. <https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war>

Kramer, A. E. (2023, September 26). *Disinformation is a weapon regularly deployed in Russia’s war in Ukraine.* The New York Times. Retrieved April 6, 2025, from <https://www.nytimes.com/2023/09/26/world/europe/ukraine-russia-war-disinformation.html>

Jamieson, Kathleen Hall, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know* (New York, 2020; online edn, Oxford Academic, 18 Feb. 2021), <https://doi-org.proxy.lib.odu.edu/10.1093/oso/9780190058838.001.0001>, accessed 25 Mar. 2025.