Marcus Sowers

Professor Karahan

CYSE 495 - Project Paper

12/6/21

Is Cyberspace at Risk of Being "Militarized"?

Within the last 20 years, the cyberspace has continuously grown and expanded leaving the cyberworld completely up for grabs. With this being the case, governments around the world must adapt to the new age so they can keep their country and people safe and secured. In this day and era, war has been an on-going and common issue around the world whether it's over land, resources, funds, etc. Internet militarization has already been a tactic and carried out as the process of using the Internet and the cyberworld in order to ensure state and national security, while also keeping their information and people protected from all potential cyber threats. With every country still trying to fully understand how conflict and potential attacks in the cyber realm could shape international relations, each are very determined to be the first to the new cyber advancement. In this project paper it will discuss into detail about why the cyberspace is at risk of being militarized by examining few and analyzing a few topics. These topics will go over what exactly the cyberspace is, create an understanding of cyber attacks and warfare, and discuss the cost and potential gain if militarized.

Cyber Space

For one to fully understand and agree if cyberspace is at risk of becoming militarized, one must understand what the cyberspace is. The cyberspace is basically the virtual computer world, allowing everyone within this space to have access to communication and information through computer networks. Every country can have access to this world, making it very concerning on if it would be used with positive intentions or used as an advantage to execute threats and attacks. One of the scholarly journals used for this project paper stated that the "incentives for moderation are built into its cooperatively constructed infrastructure, and these incentives grow stronger as more economic and administrative functionality moves online" (Duncan B. Hollis). This basically states that as technology continue to improve and advance, conflicts would also increase because of the unlocked capabilities the cyberworld provides.

Earlier in this course, the question "do you think cyberspaces should be seen as a domain of operations like land, sea, air and space" was asked. This is a great question to take into consideration because even though the cyberspace is not physically a domain on this Earth, it may need to be considered an area of domain because of the potential power a country can gain if used properly. This large computer network connecting every computer from all around the world is great for reliable communication and information transactions but is at major risk of being militarized if used properly. Within the cyber world, countries are beginning to take advantage of opportunities to execute data breaches and attacks. This is extremely concerning making the possibility of a militarized cyberspace and cyber-attacks more likely to happen.

Cyber Attacks

Ever since the first computer systems have been built there has always been a potential risk of misuse from military operatives. In April 1967, a computer scientist named Willis Ware delivered a conference paper called 'Security and Privacy in Computer Systems', that highlighted "the dangers of resource-shared computing, especially for military and defense systems, arguing that deliberate attempts to penetrate such computer systems must be anticipated" (William Marrin). This gives great reasoning why there will always be a risk of potential attacks and possible misuse of militarized cyberspace. The conference paper focused directly "on the threat of 'deliberate penetration', including 'active in filtration' of systems and 'passive subversion' tapping communication lines" (William Marrin). Different militaries across the world could execute these acts of cyberattacks creating an opportunity to upgrade their military power.

With the possibility of a militarized cyberspace and cyber-attacks more likely to happen, it is time to discuss what exactly a cyber attack is. A cyber-attack is an attempt by someone to damage or destroy a computer network and system. This can easily be carried out by a country for an act of potential gain of military power, which is why this is such a strong subject to discuss. If certain countries believe there could be a potential military benefit from a cyberattack through the cyberspace, it will most likely be carried out regardless of moral standards. Therefore, all countries most stay educated on cybersecurity programs and the cyberspace, in order to keep their country and confidential information secured. Even though there is chance war in the cyberspace may never occur, there is also a chance "cyber-attacks will play a part in ongoing policy conflicts and threaten to burst out of the ether and into the world of bombs and bullets" (Peter Campbell). A militarized cyberspace is very concerning because with the global militaries, most show pride in being the "strongest" in power. A countries military could believe executing these attacks could lead to more power but could actually be an "an intermediate step in conflict escalation leading to limited or major wars" (Peter Campbell).

Cyber Warfare

With a better understanding of what the cyberspace is, one can now dip into what would or could happen with the potential of a militarized cyberspace. If the cyberspace was the become militarized, it is safe to say this would spark up potential cyberwarfare within the technology. According to Richard A. Clarke, “Cyberwarfare is the unauthorized penetration by, on behalf of, or in support of, a government into another nation’s computer or network. Or any other activity affecting a computer system, in which the purpose is to add, alter or falsify data, or cause the disruption of or damage to a computer, or network device, or the objects a computer system controls” (William Merrin). In other words, cyberwarfare is the use of cyber technology to attack and disrupt computer and information systems for strategic or military purposes. As technology has begun increasing and becoming more reliable over the years, military interest across the world has also increased.

A scholarly source analyzed for this paper made it easy to understand that military interest in cyberwar has always been increasing. This was understood when it stated that on June 9th, 1997, the USA had launched a cyberwar exercise called Eligible Receiver, tasking an “NSA ‘red team’ to infiltrate DoD networks using only commercially available technologies. Intrusion turned out to be ‘absurdly easy’. The two-week test was over within four days, as the NSA team penetrated the entire defense establishment network, leaving markers to demonstrate their access and even interfering with communications: ‘They intercepted and altered communications, sent false emails, deleted files and reformatted hard-drives’. Eligible Receiver was another proof-of-concept of both the possibilities of penetration and of actual disruption and damage” (William Marrin). This well executed cyberwar exercise the research stated gives a full understanding of the potential loss and gain for using the cyberspace as military grounds for advantages and help.

Potential Gain

Everyone knows there is great gain through the cyberworld when the right information or data is stolen or disrupted. Humans always tend not to do the morally right thing when their own goals or desires intervene. Studies have proven that "the complexity of cognitive work associated with human-technological interaction with multiple interdependent, interconnected and networked environments is compounded, as these human and technological agents consequently bring their own assets and goals (e.g., informational, social, physical, cyber) into the operating and decision-making space" (Øyvind Jøsok). This basically states that even though there are rules and guidelines to follow, a certain individual might not tend to follow them for personal benefits. The same could be said about a country or states benefit, leaving a gap of error of where the line would be crossed for this potential cyber gain.

As any military guideline soldiers and officers most follow strict military protocol, especially when it comes to planning for cyberattacks. These protocols may only be approved when it has been checked and reviewed by the chain of command. If a country decides to use the cyberspace as an advantage of force, this could very well be believable. It is found that "cyber-attacks with material effects, such as damage or destruction of property, or injury or death to human beings, are considered the easy cases for the use of force analysis" (Samuli Haataia). A countries military power could significantly increase if the cyberattacks are successful, creating a tough ethical decision for any personnel in charge. The specific personnel in charge would then have to take into consideration where the certain attack is located, its benefits and costs, and the potential risk must be assessed. Some people may believe that there is too much concern and time consumption about the approval of these policies. By the time everything is passed off and approved by upper officials, it is most likely already past the best and most efficient way to operate.

Conclusion

In conclusion, this paper went into great depth and detail about why the cyberspace at risk of being militarized. In this paper, it stated and analyzed what exactly the cyberspace is, created an understanding of what exactly a cyber-attacks and warfare is, and it discussed the cost and potential gain if militarized. When all this is understood and truly taken into consideration, there is always a question of what a militarized and war environment cyberspace would look like. Two authors who wrote one of the works cited journals, Duncan B Hollis and Jens David Ohlin, believe that a militarized cyberspace would "be where states would take on a greater (but not exclusive) role in governing all aspects of the technical architecture and infrastructure" (Duncan B Hollis). This is a great quote because if states were to take on a greater role in governing all aspects of the technical architecture and infrastructure, it helps focus that each government role would have to have equivalent power making the urge for higher power that much higher. With the research information stated, the question shouldn't be if the cyberspace is at risk, but exactly how much risk and when will it surpass a point where everyone must take on more responsibility of the cyberspace?

Works Cited

Campbell, Peter. "Generals in Cyberspace: Military Insights for Defending Cyberspace." Orbis (Philadelphia) 62.2 (2018): 262-77. Web.

Haataja, Samuli. Cyber Attacks and International Law on the Use of Force [e-book] the Turn to Information Ethics (2019). Web.

Hollis, Duncan B, and Jens David Ohlin. "What If Cyberspace Were for Fighting?" Ethics & International Affairs 32.4 (2018): 441-56. Web.

Jøsok, Øyvind, Benjamin J Knox, Kirsi Helkala, Ricardo G Lugo, Stefan Sütterlin, and Paul Ward. "Exploring the Hybrid Space." Foundations of Augmented Cognition: Neuroergonomics and Operational Neuroscience (2016): 178-88. Web.

Merrin, William. Digital War. 1st ed. Milton: Routledge, 2018. Web.