

Is Cyberspace Being Militarized?

Terrance Boakye

CYSE 526

December 11, 2025

In 2007, Estonia was struck with a major cyberattack that shut down banks, media websites and government services. The attack spread quickly and resulted in chaos throughout the country. As a result, it showed to the world how digital networks could be employed as weapons. No bombs were dropped. No soldiers crossed borders. But the damage was real. Many people now view this attack as a turning point in global security. It made governments reconsider what war might look like in the digital age. Since then, many countries have become more aware of the vulnerability they have online. They have begun to take cyberspace into account as an arena where conflicts might start or grow.

Over time, cyberspace went from being a space for communication to being a space for competition. Nations now wish to defend it, as they defend their land, sea, air and space. According to some academics, cyberspace is the fifth domain of warfare (Reinhold, Pleil, & Reuter, 2023). This idea recalls the developing belief in the importance of online systems as much as in those physical. Countries now develop cyber units and invest in the tools to spy, disrupt or damage digital networks. These tools can cripple economies or disrupt everyday life. They can also be used to gather intelligence and provide support to military goals.

The distinction between war and peace is less distinct. Cyber operations have no warning. They might remain in hiding for extended periods of time. Some experts believe that the militarization of the cyber space is unavoidable due to the high level of technology dependency of societies (Dunn Cavelty, 2012). Others are concerned that by treating cyberspace as a battlefield it makes conflict more likely. They point out that there is a possibility that constant competition may have a detrimental effect on the relations between the states making co-operation more difficult (Mathur, 2025). Attacks on digital systems can also have civilian impacts as hospitals, energy networks and transportation systems are prone to attack.

The reasoning of militarization is important. It has implications for global security and diplomacy and international law. It also has its impacts on ordinary individuals around the world. As technology plays an increasingly central role in modern life, the role of cyberspace in conflict will continue to increase. This paper acquires analysis of how cyberspace is militarizing, the challenges that restrict the process, and what this trend implies towards global stability.

The militarization of cyberspace is relevant because digital networks support nearly every area of modern life. They are used by government to store records and run important services. Businesses use them to transfer money and goods. They are used in care of the patients by the hospitals. Transportation systems use them to control the roads, ports, or airports. The impact of these systems being hit during a conflict is that the harm infects far beyond the intended victim. A single attack in a power grid or financial system may impact millions of people. This brings up very serious issues about safety and stability in the digital age.

Cyberspace has no distinct boundaries. Countries are interlinked through the global networks. In one attack, it can move from system to system and impact those states that were never involved in a conflict. This causes diplomacy to be more complicated. It is often impossible to prove who has executed a cyberattack. Nations may blame each other. Tensions rise. Cooperation becomes harder. International law was developed for physical warfare, not invisible attacks conducted by code. The rules of sovereignty, proportionality and self-defense do not fit easily to cyber operations (Sandvik, 2012). This gap results in confusion and disagreement over how states should behave online.

Cyberspace is also a blend of civilian and military systems. A single network could be used by a government agency and/or a private company. A willingness to attack a military target could also have an effect on hospitals or schools if they are relying on the same system (Dunn Cavelty,

2012). This makes cyber conflict unpredictable and hazardous. It raises moral questions about whether cyber weapons can ever be used responsibly. With the development of cyber units and digital weapons in the countries, the chances of accidental damage increase. These factors make it important to study whether cyberspace is becoming militarized and what that means to the peace in the world.

This paper employs literature-based approach. It is based on peer-reviewed sources in the fields of cybersecurity, international relations, and security studies. These sources contribute to the explanation of the understanding of states with regard to cyberspace and the ways they use it for military purposes. The paper does not gather novel data. Instead, it looks at arguments from experts and real-world cases discussed in the academic research. This technique is useful to relate theory to practice. It also helps to reveal where the experts agree and where they disagree.

The paper focuses on three areas. First, it examines evidence that points to cyber space being militarized. Second, it surveys counter arguments which caution against declaring cyberspace a military domain too soon. Third, there is an analysis of the consequences of militarization and the impact these changes have upon global security. This structure enables the paper to acquire a balanced and clear understanding of the issue.

Cyberspace is an Internet system of digital networks worldwide. It includes computers, servers, communication cables, satellites and software. It supports nearly all aspects of the modern society. Militarization is the process of turning what was once civilian space into a space that is incorporated into military planning or strategy. When the fight comes in cyberspace, nations start to view digital networks as a means of defense and offense. They begin to prepare for the attacks in this space. They also develop methods of striking back, in assault.

Cyberwarfare is the concept of using cyber tools in the time of an armed conflict. Cyber operations involve offensive and defensive operations undertaken by states in peacetime or crisis. While Cybersecurity is the principle of protection, stability, and resilience. These terms overlap with one another but have different purposes. Cybersecurity has the goal of protecting systems. Cyber operations are meant to serve strategic objectives. Cyberwarfare is a practice of fighting using digitised force in war. Militarization is the linking concept between these three concepts because the states consider the cyberspace as a place where security, conflict and competition blend together.

Scholars such as Dunn Cavelty and Sandvik help to explain this change. Dunn Cavelty (2012) argues that militarization is not merely the building of weapons. It is also how leaders speak about cyberspace. When states refer to cyberspace as a battlefield, this influences public fear and shapes policy. Sandvik (2012) adds that militarization puts international law at risk. Cyberspace has no borders. It is a mix of civilian and military systems. This makes it difficult to operate the laws of war. These scholars demonstrate that cyberspace is as much a result of politics, ideas and debates over the law as it is a result of technology.

Many states have formed offensive hacking teams. These teams can spy, disrupt or damage networks. Offensive tools enable states to cripple their enemies before firing a shot. Egloff (2023), it exists now cyber tools belonging to state violence. They provide countries with new means of projecting their power. The US created U.S. Cyber Command to oversee its cyber mission. China's People's Liberation Army Unit 61398 is a notorious hacker that is known for running large cyber espionage campaigns. Russia's GRU has employed cyber tools in its attacks on foreign governments and infrastructure.

Cyber weapons tend to be dual-use in nature. A protection tool for the system can also be altered into a weapon with slight modifications (Reinhold, Pleil, & Reuter, 2023). This makes arms control hard to handle. It is not always clear whether a given tool is for defense or attack. The expansion of offensive capabilities indicates a change in the way states think about conflict. They now view cyberspace as a place where the battles can be started long before any physical fight.

Many countries are now developing cyber operations as part of their defense plans. Dunn Cavelty (2012) writes that this changed when nations started to perceive cyberspace as a threatened space. Military agencies took over the digital security. NATO has in 2016 recognized cyberspace as a domain of operations. This means that cyberattacks on members could create a collective response.

The United States has a strategy called "persistent engagement." It is focused on constant action to shape the digital environment. Russia deploys cyber to be part of information warfare. China incorporates the cyber operations in the informatized warfare. These doctrines indicate that cyberspace is now a part of military planning. This integration goes even deeper in terms of militarization.

There are several instances where cyber operations have aided in supporting military objectives. Stuxnet was used to damage the Iranian nuclear equipment. Russia used cyberattacks during its invasion of Ukraine to disrupt networks and spread confusion. China continues the cyber probing around Taiwan. The Texas National Security Review (2024) describes how cyber effects can impact systems, shape decisions or determine public opinion. These cases illustrate that there are real conflicts with cyber tools. They assist states in preparations, weakening of enemies and gaining advantage.

It is difficult to know who was behind a cyberattack. Hackers have the ability to conceal their identities behind false paths or foreign networks. A state may be suspicious of another country but may not always be able to prove it. Without proof, states are unable to act with military force. This leaves cyberspace in a gray area between war and peace. Attribution also influences deterrence. Attackers can be daring if the offender believes he or she will not be caught.

International law finds it difficult to address cyber conflict. Sandvik (2012) explains that the existing rules were developed for physical war. Cyberattacks may interrupt the functioning of systems without causing physical damage. It is not clear when such attacks constitute armed attacks. The Tallinn Manual does try to tell states what to do, but there has been debate. Reinhold and Reuter (2022) suggest that there are new risks introduced by AI. AI tools are capable of acting quickly as compared with humans. They are able to make mistakes or do harm without specific intent. This leaves the legal situation open.

Mathur (2025) states that the digital space across the world is controlled by private companies. They own data centers, cloud networks and communication tools. States depend on them for cybersecurity. Criminal Groups are also involved. They can mount assaults that resemble state actions. This medley of players makes cyberspace very difficult to control. It prevents a complete militarization as the states do not completely own or control the domain.

As states are building cyber weapons, a digital arms race is growing. Nations race for superior tools. This increases tension. One cyberattack could turn into a larger war. Foulon (2024) describes the way cyber competition influences world politics even at a level lower than war. It undermines trust and makes diplomacy more difficult.

Cyberattacks can leak over into civilian systems. Hospitals, schools and energy grids may be affected. This causes real harm. The WannaCry attack in 2017 handicapped medical care. AI

weapons also create ethical issues. They can make decisions without any human control and take split-second judgments that harm people (Reinhold & Reuter, 2022).

The world needs clearer rules for cyber conflict. Arms control agreements could provide limits. Nations need assurance-building measures like shared communication channels and joint exercises. Private companies must also be involved as they control key networks. Cooperation is required for a stable digital world.

Another mechanism that can help understand the militarization of cyberspace is to examine the response to it in different regions. Not all of the states look at cyberspace in the same manner. Some countries view it as being primarily a security threat. Others see it as an opportunity to get a say. These different perspectives have implications for the speedup of militarization and the form that cooperation takes around the world.

In Europe many of the states are defence and protection rather than offense. This is because in Europe there are strong laws concerning privacy and human rights. These values have had an impact on the way that governments think about digital power. The European Union has established networks for reporting cyber incidents and exchanging threats. It also stimulates countries to reinforce their defence. However, Europe is split on offensive cyber capabilities. Some are supported by the states, while other states are concerned of the negative consequences of using offensive tools that can escalate the conflict. This debate slows down militarization in the region. It also indicates how values can contribute to influencing the way states perceive digital conflict.

In Asia, the picture is very different. The region has accelerated technological development and an increase in the competition between the major powers. China invests considerable money in cyber capabilities. It links cyber tools to national strategy and economic objectives. Japan has

more of focus on the defense but started increasing the focus on its cyber units. South Korea regards cyber threats as a significant challenge because of its enmity with North Korea. North Korea itself uses cyber operations to fund and global politics. These different approaches generate tension in the region. They also make the process of militarization faster since states need to react to each other.

It is important to note that in the Middle East, cyber operations are tied to political and military conflicts in progress. States such as Iran, Israel and Saudi Arabia have built up formidable cyber capabilities. They use them for intelligence, defence and regional competition. For instance, Iran has employed cyber tools as a way to react to economic pressure and political threats. Israel has evolved great digital defenses because of security. These actions start a cycle in which each state takes action to protect itself while at the same time escalating tension (Reuter, 2023). The region is witness to the rapid growth in militarization when conflicts are already present.

Developing nations are another challenge. Many do not have strong cyber defenses. They are exposed to attacks by criminals or powerful states. Some depend on foreign companies in order to safeguard their networks. Others are trained and supported by larger nations. This dependence has implications on their capacity to navigate the militarization of cyberspace. It also raises concerns about digital inequality. Wealthy countries are able to invest in cyber armies. Poorer countries find it difficult to secure basic services. This gap is impacting global stability because states which are weaker are often attacked.

Another issue is that of international organizations. Groups such as the United Nations try to establish rules for cyberspace. They encourage the states to act responsibly. They also support a dialogue in order to avoid misunderstandings. But progress is slow. States have disagreements as to what constitutes acceptable behavior. Some want tight restrictions on cyber weapons. Others

desire freedom to develop their own tools. These disagreements illustrate that militarization does not expand in the same way in all cases. It is influenced by politics, culture and regional tensions.

Many scholars say that we need more education and knowledge of cyberspace (Reuter, 2023). People depend on digital systems in their daily life. Yet many are unaware of the workings of cyber conflicts. This ignorance is what makes societies vulnerable. It also makes it difficult to talk about laws and policies. Also, if more people understood how cyberattacks operate, nations could better choose whether or not to militarize. This may diminish the fear and make more balanced decisions possible.

Overall, global responses demonstrate that militarization is not a simple process. In some areas, it moves fast and in some areas, it moves slowly. It is dependent on security threats, political objectives, economic circumstances and cultural values. These differences make it difficult for cooperation but they also demonstrate too where there is scope for progress. Understanding these regional perspectives is important for understanding why cyberspace is militarized in uneven ways.

The United States has the term "persistent engagement" to shape cyberspace. It acts early to stop threats. It is not sitting and waiting for attack, rather active. This affords the powers that be in the U.S. a better hand on the digital environment. China follows the informatized warfare. It combines the elements of cyber operations with the elements of intelligence and political goals. Russia combines cyber tool and information warfare. These doctrines have competition with one another. Each drives the others to improvement. This competition is reinforcing militarization (Reinhold, Pleil, & Reuter, 2023).

The proof is that cyberspace is being militarized. States develop cyber weapons, establish cyber units, and choose to write doctrines declaring cyberspace a domain of conflict. This process includes technology, strategy, and discourse. Leaders disclose talking about cyberspace in military

terms. They make plans for attacks and invest in digital capabilities. But militarization is not totalitarian. Attribution issues, legal vacancies and the role of private actors constrain the extent to which states are allowed to go. Cyberspace is an open and disputed space.

The world needs cooperation in managing these challenges. Cyber norms can serve as expectations. Arms control can ease the escalation. Transparency has the ability to build trust. Private companies should be included as they have control over important parts of the digital world. The fate of cyberspace rests on whether countries reach for restraint. As cyberspace becomes the next phase of power competition, humankind is faced with a choice. It can perpetually wage war the digital world and substitute in endless conflict. Or it can save cyberspace as a shared security space of trust and responsibility.

References

- Dunn Cavelty, M. (2012). The militarisation of cyberspace: Why less may be better. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.), 2012 4th International Conference on Cyber Conflict (CYCON 2012) (pp. 141–153). NATO CCD COE Publications. https://ccdcoe.org/uploads/2012/01/2_6_Dunn-Cavelty_TheMilitarisationOfCyberspace.pdf
- Egloff, F. J. (2023). The better angels of our digital nature? Offensive cyber capabilities and state violence. *European Journal of International Security*, 8(3), 256–276. <https://doi.org/10.1017/eis.2023.13>
- Foulon, M. (2024). The evolution of cyber conflict studies. *International Affairs*, 100(6), 2317–2334. <https://doi.org/10.1093/ia/iia070>
- Mathur, R. (2025). Techno-capitalism and weaponization of cyberspace. *Global Studies Quarterly*, 5(2), ksaf031. <https://doi.org/10.1093/isagsq/ksaf031>
- Reinhold, T., Pleil, H., & Reuter, C. (2023). Challenges for cyber arms control: A qualitative expert interview study. *Zeitschrift für Außen- und Sicherheitspolitik*, 16(3), 289–310. <https://doi.org/10.1007/s12399-023-00960-w>
- Reinhold, T., & Reuter, C. (2022). Cyber weapons and artificial intelligence: Impact, influence, and the challenges for arms control. In M. Brehm (Ed.), *Armament, arms control and artificial intelligence: The Janus-faced nature of machine learning in the military realm* (pp. 15–34). Springer. https://doi.org/10.1007/978-3-031-11043-6_1
- Sandvik, K. B. (2012). Towards a militarization of cyberspace—Cyberwar as an issue of international law. PRIO Paper. Peace Research Institute Oslo. <https://www.prio.org/publications/7262>

Texas National Security Review. (2024). Cyber effects in warfare: Categorizing the where, what, and why. Texas National Security Review, 7(2). <https://tnsr.org/2024/08/cyber-effects-in-warfare-categorizing-the-where-what-and-why>