Militarization of Cyberspace

Jaquan Odom

CYSE/POLS 526

Russell A. Korb

December 30th, 2025

Militarization of Cyberspace

Cyberspace has now evolved into a domain to where states compete and constantly try to maintain an advantage. Through the development of cyberspace, many states have begun to use their digital resources to spy on their rivals and to carry out attacks against countries or emerging powers that they view as a threat. Cyberspace has also become a part of our daily lives beyond government and military use. People rely on digital applications and devices for basic communication, work, and many other basic services. The cars we drive are digital or have digital appliances within them, we use our cell phones to communicate with people at all times of the day, and even when it comes to our jobs, many of our daily operations rely heavly of digtial products to get through a regular work day. Since government, economic, and military activities all depend on networks, cyberspace has taken on more characteristics of a military power. nowadays digital systems influence national security in ways that are comparable to the well known military powers, such as land, air, sea, and space. Researchers have stated that no information system is ever completely secure and that attacks are inevitable/bound to happen because of the increasingly evolving threat environments. What militarization means is that it is the process of developing and deploying military resources within a domain. Then, when you apply this to the idea of cyberspace, it refers to the involvement of governments and armed

forces shaping the digital environment. The modern threat actors, which includes avanced persisatnt threats, use long term and strategic methods that would resemble organized military operations.in the context of cyberspace, this militarization involves the development in offensive operations, specialized units and the development of digital tools that would function as weapons. While cyberspace was once originally a space for civilians, the rise of state sponsered operations, the national cyber commands, and the increasing growth of digital capabilities show signs of a shift toward militarization.

Militarization is the process of organizing, equipping, and deploying military capabilities within a specific domain. When it comes to militarizaion it is not a single action it is a process, and this is where governments build institutions, create strategies, train forces, and the development of both offensive and defensive tools. There are several reasons why behind a domain that has become militarized and the reasons are gaining an advantage over their rivals, creating a deterrent for any potential threats, or trying to establish control or dominance. This is seen in the traditional military environments, land is secured by armies, the sea is secured by naval forces, the air by air forces, and space through satellites and missile defense. Then once a domain has become miltiarized it begins to shift from normal civilian use to serving a more national purpose. This is because militarization can happen in any area of importance for national power, and this means the same process can be applied to cyberspace

When the idea of militarization is applied to cyberspace, it describes the process of how governments have begun changing the overall digital environment to a more military way of thinking. This includes strategies and structure. Researchers have already said that there is an intensification of cyberspace militarization, meaning that states now already view the digital domain as strategically important for national power (Zhang et al., 2025). This shift in

cyberspace is very visible; you can see this by how advanced persistent threat groups operate that have politically driven motives, persistent timelines, covert operations, and sophisticated methodologies. This shows long-term state-directed campaigns compared to ordinary criminal behavior.(Zhang et al., 2025). The defense strategies have also become more militarized. There are zero-trust networks that use concepts that are similar to battlefield defense which includes denying movement within a network and disrupting the attack kill chain to prevent adversaries from advancing (Zhang et al., 2025).Cyber operations increasingly demonstrate sustained attack defense dynamics that can degrade mission effectiveness, particularly when cyber assets are integrated with physical systems (Zuo et al., 2023).. Scholars argue that cyberspace itself now functions as a battle space and contested area, this shows that states now treat this domain the same way they would treat any of the traditional areas of conflict such as land, sea, air, and space (Kallberg & Cook, 2017). With all this information put together, the development of cyberspace would suggest that the digital realm is no longer simply an information network but is also a strategic domain which is continuously shaped by military logic.

In the cyberspace domain, not all hostile activity would be classified into the same group and are classified as cybercrime, cyber espionage and cyberwar. The differences between the three are that cybercrime is usually motivated by financial gain and the attacks are carried out by a single individual or by a small group for profit. Cyber espionage is usually driven by state actors focuses around long term information gathering. This type of behavior can be seen with advanced persistent threats and as mentioned before these groups usually operate politically driven motives, persistent timelines, covert operations, and sophisticated methodologies. This shows that objectives are sponsored by government objectives instead of just criminal gain (Zhang et al., 2025). Lastly cyberwar, cyberwar is more than just long term gathering of information; scholars describe cyberspace as a battle space and contested area and they argue

that cyber capabilities has become a viable strategic option for confronting adversarial societies (Kallberg & Cook 2017). Essentially, what that means is that the actions of cyberway is similar to traditional warfare. This would include disruptung crictcal infrascture, weakening enemy capabilities, or preparing cyberspace for future conflict. When you understand the differences between cybercrime, cyber espionage, and cyberwar, you understand the importance of militarization because when you shift between these topics, the cyberspace domain would resemble a domain of armed conflict instead of a space for crime and information gathering alone.

Even though there are cyber technologies that function as a militarized power, cyberspace is still used by civilains and it is a part of our everyday lives. There are still civilian systems, which are the power grids, everyday communications, everyday transports, and even industrial systems. These are also Cyber-physical systems that support both civilian activity and military missions (Zuo et al., 2023). Research on advanced persistent threats further shows that industrial and manufacturing systems are frequent targets of long-term cyber intrusions, demonstrating how militarized cyber activity can directly affect civilian economic infrastructure (Wu et al., 2020). Even though these systems are used by civilians, they are still used and deeply connected to military operations (Zuo et al., 2023). Since these operations are used for civilians and armed forces, any tool that is used to attack or defend our systems is technically dual use. Advanced persistent threats, which were originally developed for espionage or military operation,s usually affect civilian networks, and this proves that cyber tools go hand in hand on both sides, used for military and theirs a civilan side (Zhang et al., 2025). Researchers have also said that advanced persistent threats regularly damage government and business networks alike, showing how civilian infrastructure is pulled into state-level conflicts (Zhang et al., 2025). Dual technology really blurs the lines when it comes between cilivian cyberspace and military

strategy, which shows that cyberspace is shifting towards a militarized domain. Scholars even describe this trend as a deepening militarization of the global cyberspace, highlighting how the dual-use nature of technology is accelerating this shift (Zhang et al., 2025). Scholars even describe this trend as a deepening militarization of the global cyberspace, highlighting how the dual-use nature of technology is accelerating this shift

In the beginning, cyber threats were viewed as just isolated criminal acts; these acts are usually motivated by financial gain or individual motives. There has been research that shows that cyber activity has been turning into something far more strategic. In present day cyber operations, they take the form of advanced persistent threats, and the characteristics of these attacks consist of long term access, covert behaviour and politically motivated objectives instead of any short term goals (Zhang et al., 2025). These type of cyber operations require a lot of planning, resources, and coordination, and all of this would show or suggest that the attacks are state sponsored instead of regular cybercrime. As cyber capabilities get better, cyberspace begins to define itself as a contested battlespace in which states pursue national interests using cyber tools as instruments of power (Kallberg & Cook, 2017). This shift can also be proven because there is research that actively show that cyber intrusions can directly affect physical combat operations by degrading military effectiveness and disrupting mission critical systems, linking cyber actions to real world military outcomes (Jang et al., 2023). Cyber conflict now follows an ongoing cycle of attack and defense, and both sides are continuously adapting their strategies, which eventually start to resemble to the traditional military campaigns instead of the usual criminal activities (Zuo et al., 2023). These developments show that there’s a clear transition from cybercrime toward state level cyber conflict, which shows early signs of cyberspace becoming militarized.

There have been incidents that has happened and they have demonstrated that cyber activity was no longer a crime or just a single isolated disruption, but instead it could be used as a strategic tool at the national level. One of these early events happened in 2007, and that was when estonia had experienced a large scale cyber attack which disrupted government services, financial institutions, and the public communication systems. Even though that the attacks didn't cause any direct damage, they did reveal how digital operations could interfere with the functions of an entire state. When events like this occur, people are able to look back at the incident and see that it shows characteristics of being an advanced persistent threat. Although the Estonia attacks predate formal APT classifications, later scholarship helps explain how such incidents resemble sustained, politically motivated cyber campaigns. These cyber operations are sustained, coordinated, and they are aimed at achieving political objectives instead of short term financial gain (Zhang et al., 2025). Another very important event would be the discovery of Stuxnet in 2010, which wasa highly sophisticated piece of malicious software that was designed to target industrial control systems.

A more significant escalation occurred with the discovery of Stuxnet in 2010, a highly sophisticated piece of malicious software designed to target industrial control systems. Unlike earlier cyber incidents, Stuxnet demonstrated the ability of cyber tools to cause physical damage, reinforcing research that shows cyber intrusions can directly affect real-world military and strategic operations (Jang et al., 2023). These early cases illustrate how cyber operations evolved beyond nuisance attacks or criminal behavior and began to align with strategic state interests, signaling an early phase of cyberspace functioning as a contested domain of conflict rather than merely a civilian communication space (Kallberg & Cook, 2017). One way that it can be said that cyberspace is starting to become more militarized is because states have formally integrated cyber capabilities into their military establishments. Instead of treating the cyberspace

operations as a temporary or an experimental tool, there have been many governments that have created permanent cyber commands that work alongside the traditional military branches. With cyberspace working alongside the military it just reflects how cyberspace is getting the recognition that it is now essential to national defense. Like the traditional branches. Since adding cyberspace within the military structure, states now demonstrate long term strategic commitment to operating in the digital domain instead of civilian led responses.

The cyber commands that are implemented in the military structure are structured around principles that are related to traditional military logic. They show centralized command, coordinated offensive and defensive missions, and long term planning instead of reactive incident response. What this approach does is that it suggest that states view cyber operations more as part of a broader military strategy instead of just technical or law enforcement activities. Even though cyberspace is different from conventional domains, the adoption of this military style command strcuture show that states are applying similar warfighting concepts to digital environments the concept of militarization of cyberspace is reinforced by the development of cyber weapons that have characteristics that are similar to conventional military arms. There are scholars who argue that malicious software can be now be evaluated as a weapon, which is based on the technical features instead of it solely being based on the intent behind the malicious software use. The technical features include precision targeting, scalability, and the ability to produce strategic or physical effects. When there is malware that is designed to disrupt critical systems or the goal to disrupt specific military objectives, it moves beyond the ordinary cybercrime, and it begins to start to function as a weapon with a digital arsenal (Reinhold & Reuter, 2022) Defensive approaches such as moving target defense further reflect this

militarized logic by emphasizing continual system adaptation to counter persistent attacks, mirroring strategic defensive behavior found in traditional military planning (Zhang et al., 2019).

Malicious software can be evaluated as a cyber weapon based on its technical features, including precision, scalability, and the ability to generate strategic or physical effects. Separate research on exploit governance shows that states often retain undisclosed vulnerabilities to preserve strategic advantage, reflecting arms-race dynamics driven by low interstate trust. Instead of sharing weaknesses to improve overall security, governments may retain them for future use. This type of behavior is really similar to traditional arms races, where states gather weapons as a form of deterrence. In cyberspace, this creates a risk because undisclosed vulnerabilities can be exploited against civilian infrastructure, and the same goes for military systems as well. Research on exploit management shows how that mistrust between states complicates efforts to limit cyber arsenals and encourages continued militarization (Reinhold et al., 2023) State sponsered cyber operations also show that the militarization of cyberspace occurs through their scale, persistence, and strategic intent. This is different from regular cybercrime because cybercrime is usually driven by a short term goal like financial gain, state led operations usually look for a long term goal or access to networks so that they can gather information for future use. These state led operations have persistent timelines, covert techniques and politically motivated objectives, which are more related to military campaigns instead of criminal activity (Zhang et al., 2025). The modern cyber operations also show that digital actions can produce real world consequences. There is research that shows that cyber intrusions can directly affect systems that are in the real worl,d and the effects could cause the system to be degraded. Cyber intrusions can

degrade the military effectiveness by disrupting mission critical assets. When cyber attacks interfere with combat operations or critical infrastructure, this blurs the lines between digital conflict and traditional warfare. The connection between cyber activity and the physical impact that it causes only strengthens the argument that cyberspace now functions as a contested battlefield instead of just an information network (Jang et al., 2023)

One major challenge for international law in cyberspace is that traditional legal frameworks were designed for physical conflict and do not go well with digital operations. Cyber conflict lacks clear territorial boundaries and occurs in an environment characterized by anonymity and rapid, machine speed interactions. Since cyber operations usually do not show immediate physical damage, legal concepts like proportionality and attribution become hard to apply consistently. With this mismatch it creates uncertainty about how international law should regulate state behavior in cyberspace and weakens the ability of legal norms to constrain emerging cyber conflicts (Kalberg & Cook, 2017). Another major challenge for international law in cyberspace is the problem of attribution. When cyber operations are executed, they are usually carried out in such a way that the identity of the attacker is unknown. This makes it difficult to determine the responsibility of the executed attack. Because of this, it weakens the anonymity, weakens the accountability and the effectiveness of legal or diplomatic responses. Kallberg and Cook (2017) explain that cyberspace lacks the features that allow traditional conflicts to be managed, which would include clear identification of the bad actor. Because of this, states might hesitate to respond to cyber incidents or might not get involved at all. Since there's a lack of trust between states, it undermines the development of effective international cyber norms. Governments are usually not willing to share vulnerability information or limit their

cyber capabilities because it makes them lose their strategic advantage. The research on exploit management shows that states benefit from retaining and stockpiling cyber exploits instead of working together on security measures. This type of behavior increases the risk for civilian and military infrastructure and makes arms control efforts hard to implement. Since there isnt any trust or transparency, the international norms struggle to constrain state behavior,r which reinforces the militarization of cyberspace (Reinhold et al., 2023).

One argument against the claim that cyberspace is being militarized is that cyber activity is more similar to espionage than warfare. The reasoning being that states also engage in intelligence collection and cyber operations, which often serve a similar purpose; sometimes, the intent is to gather information instead of causing destruction or disruption. Kallberg and Cook (2017) argue that cyber operations don't have all of the features of traditional warfare, this would include clear beginnings, endings, and also battlefields that would be easily identifiable. Looking at cyber militarization from this perspective, it shows that cyber activity is really an extension of intelligence gathering instead of a new form of military conflict. Another argument to point out that's against cyber militarization is that states deliberately conduct cyber operations below the threshold of armed conflict to avoid escalation. Cyber actions are usually used to disrupt, watch, or signal without having to cause the military to retaliate. With this type of restraint, it would suggest that cyberspace functions can't be characterized as warfare or can't be said that cyberspace is militarized. Scholars have said that speed and ambiguity of cyber operations make it complicated for strategic contro,l which would cause states to avoid conflict but still be in pursuit of their national interest (Kallberg & Cook, 2017). Even though these arguments are present, the continued development of military cyber institutions and capabilities shows that cyberspace will continue to be perceived as strategically significant. Even though

cyberspace does not fit the norms of traditional warfare, there are governments that still continue to invest in their cyber forces and doctrines as a precaution against future threats. With this tension still building up it shows that militarization of cyberspace does not need to resemble traditional warfare. Instead, this shows that states are putting forth effort to prepare for future conflict in an uncertain and evolving domain.

In this paper, it has examined whether cyberspace is at risk of being militarized by examining states' behavior, cyber capabilities, legal norms, and debates between presented scholars. From the research conducted it suggests that cyberspace can’t be fully confirmed as a traditional means of warfare and that cyberspace is treated as a strategic domain. With the creation of cyber commands, the development of cyber weapons, and the persistence of state sponsered attacks is showing that military logic in the digital environment will continue to grow. Also with the weaknesses in the international law and norms, especially dealing with attribution and trust, it limits the ability of legal frameworks to stop this trend from happening. The implementation of militarization in cyberspace are important for global security. Civilian infrastructure is still connected to military systems, which increases the risk of unintended harm during these cyber operations. Without effective arms controls, mechanisms and enforceable norms, it increases the uncertainty and instability. With cyber capabilities evolving, states will try to rely on deterrence and preparedness instead of legal restraints. The understanding of cyber militarization is important so future policies can be shaped, reduce escalation risk, and the protection of both national and international security.

Works Cited

Jang, J., Kim, K., Yoon, S., Lee, S., Ahn, M., & Shin, D. (2023).

Mission impact analysis by measuring the effect on physical combat operations associated with cyber asset damage. IEEE Access, 11, 45113–45130.
https://doi.org/10.1109/ACCESS.2023.3273612

Kallberg, J., & Cook, T. S. (2017).

The unfitness of traditional military thinking in cyber: Four cyber tenets that undermine conventional strategies. IEEE Access, 5, 8126–8135.

https://doi.org/10.1109/ACCESS.2017.2693260

Reinhold, T., & Reuter, C. (2022).

Toward a cyber weapons assessment model: Assessment of the technical features of malicious software. IEEE Transactions on Technology and Society, 3(3), 226–239.

https://doi.org/10.1109/TTS.2021.3131817

Reinhold, T., Kuehn, P., Günther, D., Schneider, T., & Reuter, C. (2023).

EXTRUST: Reducing exploit stockpiles with a privacy-preserving depletion system for inter-state relationships. IEEE Transactions on Technology and Society, 4(2), 158–170.

https://doi.org/10.1109/TTS.2023.3280356

Wu, J., Dong, M., Ota, K., Li, J., & Yang, W. (2020).

Sustainable secure management against APT attacks for intelligent embedded-enabled smart manufacturing. IEEE Transactions on Sustainable Computing, 5(3), 341–352.

https://doi.org/10.1109/TSUSC.2019.2913317

Zhang, H., Zheng, K., Wang, X., Luo, S., & Wu, B. (2019).

Efficient strategy selection for moving target defense under multiple attacks. IEEE Access, 7, 65982–65996.

https://doi.org/10.1109/ACCESS.2019.2918319

Zhang, J., Zheng, J., Shi, N., Ci, Z., Wang, Y., & Zhu, L. (2025).

Toward mitigating APT attacks with zero-trust networks access control model. IEEE Internet of Things Journal, 12(19), 41215–41232.

https://doi.org/10.1109/JIOT.2025.3592616

Zuo, J., Guo, Z., An, T., Xu, Z., & Lu, Y. (2023).

A security resilience metric framework based on the evolution of attack and defense scenarios. IEEE Internet of Things Journal, 10(19), 17007–17021.

https://doi.org/10.1109/JIOT.2023.3274205