



Is Cyberspace at Risk of Being "Militarized"?

CYSE 426

Kevin Maxey

July 19, 2024

Is Cyberspace at Risk of Being "Militarized"?

Cyberspace, a networked digital domain, has become an indispensable component of modern civilization. It has exerted influence over various aspects of human activity, such as communication, trade, entertainment, and governance, which exemplifies its influence. However, as the significance of cyberspace continues to grow, there has been a corresponding increase in the number of concerns surrounding the possibility that it could be weaponized into a military asset. An investigation into the factors that lead to the possibility of cyberspace being militarized is demonstrated in this essay. In it, historical instances, present tendencies, and the possibly catastrophic effects on global security and governance that could result from the militarization of cyberspace are analyzed. Cyberspace is essential to global communications because it enables us to connect with others, manage critical infrastructure such as energy and financial systems, and store crucial information. On the other hand, due to the vastness of cyberspace, some malicious individuals attempt to commit unlawful acts, such as stealing personal information or disrupting essential services.

The historical context of cyberspace and militarization refers to the background and circumstances surrounding the development and use of digital networks and their integration into military operations. The idea of militarizing emerging domains has precedent. Throughout history, the emergence of new technological frontiers has frequently been followed by their subsequent militarization. An example is the rapid advancement of aviation technology during the early 20th century, which promptly resulted in the establishment of air forces and aircraft integration into military campaigns. In a similar vein, the nuclear era commenced with the swift militarization of scientific advancements, resulting in the creation of nuclear stockpiles and the development of the deterrence doctrine. "Historical Context of Cyberspace and Militarization: This book provides a comprehensive overview of the evolution of cyberspace and its growing significance as a national security concern. The authors discuss various cyber doctrines and the establishment of cyber units, offering context for understanding current trends in cyber militarization" Clarke, R. A., & Knake, R. K. (2010).

Cyberspace, in numerous respects, adheres to this historical pattern. The Internet was created as a tool for academic and government research, but it rapidly grew into a worldwide communication network. In the early 21st century, there was a growing acknowledgment of

cyberspace as a vital infrastructure crucial for national security, economic stability, and the functioning of society. As a result of this recognition, it has become inevitable to consider it as a domain for military operations.

The Present Condition of Cybersecurity and Cyber Warfare

The present state of cybersecurity and cyber warfare underscores the growing emphasis on cyberspace as a crucial military domain. Nation-states have acknowledged the potential of cyber capabilities to accomplish strategic goals without relying on traditional military forces. As a result, cyber doctrines have been developed, and specialized cyber units have been formed within military organizations.

Multiple nations have formulated cyber doctrines that delineate their strategies for ensuring security in cyberspace and conducting military operations. For example, the United States established the Cyber Command, a centralized command structure for cyber operations. Additionally, the country has released documents like the "DoD Cyber Strategy" to guide its activities in the digital realm. Likewise, nations like Russia and China have incorporated cyber operations into their military tactics, recognizing cyberspace as a vital battleground for attaining strategic dominance.

Cyber-attacks and Activities Sponsored by the Governments

The growing occurrence and complexity of cyber-attacks highlight the increasing militarization of cyberspace. Government-backed cyber campaigns have aimed explicitly at critical infrastructure, governmental establishments, and private businesses, frequently resulting in notable geopolitical consequences. Prominent instances comprise the Stuxnet worm, which specifically aimed at Iran's nuclear facilities and the sequence of cyber assaults ascribed to Russian agents during the 2016 U.S. presidential election. These occurrences illustrate how cyber operations can effectively accomplish strategic goals, such as disrupting vital infrastructure or exerting influence over political processes, without relying on conventional military force.

The process of transforming cyberspace into a military domain includes the practice of cyber espionage. Nation-states have been increasingly engaging in cyber espionage to achieve strategic benefits. These benefits include stealing intellectual property, acquiring sensitive information, and undermining adversaries' capabilities. The alleged theft of classified defense information by

Chinese hackers, including the blueprints for the F-35 fighter jet, is an example of the direct impact of cyber espionage on the military's capabilities and the nation's security. Significant implications for global security, governance, and the nature of warfare are associated with the process of equipping and deploying military forces in cyberspace. As nation-states increasingly view cyberspace as a domain for military operations, several significant concerns have emerged.

One of the most essential concerns that arises from the militarization of cyberspace is the possibility of escalation in the situation. Considering the inherent characteristics of cyber operations, it is possible for there to be ambiguity and difficulties in determining attribution, which can lead to misunderstandings and incorrect calculations. Inadvertently leading to a more extensive military confrontation is the possibility that a cyberattack could have. The concept of cyber deterrence, analogous to nuclear deterrence, is complex and requires a definitive definition. Since cyber activities are secret and can be quickly disputed, defining explicit standards and limits for retaliatory actions in cyberspace is challenging. "One of the primary concerns with the militarization of cyberspace is the risk of escalation. By their nature, cyber operations can be ambiguous and difficult to attribute, leading to misunderstandings and miscalculations. An unintended consequence of a cyber-attack could be a broader military conflict. Like nuclear deterrence, cyber deterrence is also complex and less well-defined. Establishing clear norms and thresholds for cyber responses is challenging, given the covert and often deniable nature of cyber operations" Rid, T. (2013).

Rid's contention that cyber warfare may not manifest conventionally offers a crucial viewpoint on the character of cyber conflicts. This perspective aids in shaping the discourse in this paragraph concerning the uncertain and intricate nature of cyber operations and their capacity for escalation.

Legal and Ethical Factors to be Considered

Incorporating military capabilities into cyberspace raises significant legal and ethical issues. The existing body of international law, which includes the rules that govern armed conflict, does not adequately account for the unique challenges cyber operations pose. It is necessary to thoroughly investigate several factors, including national independence, the distinction between non-military and military objectives, and the appropriate scale of cyber countermeasures. Furthermore, it is of the utmost importance to take into consideration the ethical repercussions of cyber warfare,

which include the potential for unintended harm to be inflicted upon non-combatants and the possibility of the disruption of civilian infrastructure. Acknowledging and addressing these concerns within the realm of digital technology is necessary to encourage responsible behavior.

Cyberspace is naturally interconnected, with civilian and military networks frequently intertwined. If military forces are equipped and deployed in cyberspace, civilian infrastructure may be damaged unintentionally. Attacks that target essential infrastructure, such as power grids, financial systems, and healthcare facilities, can potentially have significant repercussions for society. Ensuring that these systems are both long-lasting and protected is of the utmost importance to lessen the potential risks associated with cyber warfare.

Global Standards and Collaboration

It takes a substantial amount of effort to tackle the difficulties posed by cyber militarization; fostering global collaboration and creating standards and structures that govern responsible conduct by nations in the digital realm is essential. The United Nations Group of Governmental Experts (UNGGE) on Developments in Information and Telecommunications in the Context of International Security has tried establishing norms and confidence-building measures. Nevertheless, reaching a consensus on these matters proves challenging due to different states' interests and capabilities. "Mitigating the Risks of Cyber Militarization: The handbook includes discussions on international norms and cooperation, providing context for the importance of diplomatic efforts and frameworks like the UNGGE. Insights from this reference help inform the debate on the need for international agreements and norms to govern state behavior in cyberspace" Weiss, T. G., & Daws, S. (Eds.). (2018).

Case Studies and Examples

Examining specific case studies and examples of cyber operations with military significance is a valuable approach to better understanding the risks and implications of cyberspace militarization.

The topic of discussion is Stuxnet and its impact on Industrial Control Systems: The Stuxnet worm, identified in 2010, is frequently referred to as the initial documented instance of a cyber weapon specifically engineered to inflict physical harm. Stuxnet, suspected to be a collaborative effort between the United States and Israel, specifically aimed at Iran's Natanz nuclear facility, with a specific focus on its industrial control systems. Stuxnet's interference with the functioning

of uranium enrichment centrifuges resulted in a significant delay to Iran's nuclear program. This case exemplifies the ability of cyber operations to accomplish strategic goals that have traditionally been tied to military force. "The Current State of Cybersecurity and Cyber Warfare: Lin's work provides insights into cyber doctrines and strategies, particularly those of the United States. The book includes discussions of specific cyber incidents, such as Stuxnet, which are used to illustrate the practical implications of cyber operations" Lin, H. (2012).

This conversation will focus on the cyberattacks that occurred in Estonia in 2007: In 2007, Estonia was the target of a series of coordinated cyber-attacks that targeted various government agencies, financial institutions, and newspapers and magazines. A disagreement surrounding the relocation of a war memorial from the Soviet era led to the attacks, which have been attributed to Russian actors. The conflict came up as a result of the relocation of the memorial. The incident brought to light the vulnerability of a society that relied significantly on digital technology for cyberattacks and the capability of cyber operations to be utilized as tools of statecraft and coercion among individuals.

The incident known as the 2014 Sony Pictures Hack: The 2014 cyber-attack on Sony Pictures Entertainment, ascribed to North Korean perpetrators, was a retaliatory response to the release of the film "The Interview," which portrayed the assassination of North Korea's leader. Sony experienced substantial data breaches, incurred financial losses, and suffered reputational damage due to the attack. This case exemplifies using cyber operations to attain political goals and influence cultural and economic spheres. "The Current State of Cybersecurity and Cyber Warfare: The authors provide empirical data on cyber conflicts, supporting the analysis of state-sponsored activities and cyber espionage. Valeriano and Maness discuss various cyber incidents, such as the 2014 Sony Pictures hack and the NotPetya attack, which are used to illustrate the broader trends in cyber operations" Valeriano, B., & Maness, R. C. (2015). The NotPetya ransomware attack: The 2017 NotPetya ransomware attack, attributed to Russian state actors, specifically targeted Ukrainian infrastructure. However, it rapidly spread worldwide, resulting in extensive disruption and significant financial losses. The attack showcased the capacity of cyber operations to cause vast and unintentional repercussions, impacting military and civilian targets across numerous nations.

Addressing the Hazards of Cyber Militarization

The development of techniques capable of effectively decreasing the issues associated with the militarization of cyberspace is absolutely necessary to address the significant threats and implications. Improving the capacity to withstand and recover from cyberattacks is a priority. One of the most important ways to lessen the dangers linked with cyber militarization is to strengthen the resilience of vital infrastructure and systems. In order to accomplish this, stringent cybersecurity measures must be deployed, industry-leading network security practices must be incorporated, and investments must be made in technologies that can recognize and respond to cyber threats. When it comes to the construction of resilient cyber ecosystems, public-private partnerships and international collaboration are vital components. It establishes international conventions and principles that mitigate the risks linked with the militarization of cyberspace, and it is essential to develop global rules and treaties that govern responsible behavior by governments in the digital sphere. The Tallinn Manual on the International Law Applicable to Cyber Warfare and the United Nations General Assembly (UNGGE) provide valuable frameworks for understanding how current international law might be applied to cyber operations. Despite this, considerable work must be done to achieve general agreement and compliance with these standards.

They are advocating for the enhancement of openness and trust-building initiatives. Transparency and confidence-building measures (CBMs) can mitigate the likelihood of escalation and misjudgment in cyberspace. These measures may encompass information-sharing agreements, collaborative cyber exercises, and creating communication channels between nations to tackle cyber incidents. CBMs, or Confidence-Building Measures, can enhance the stability and security of cyberspace by promoting trust and cooperation.

Legal and Policy Frameworks

Establishing extensive legal and policy frameworks at national and international levels is crucial to effectively tackling the difficulties associated with cyber militarization. These frameworks should delineate the duties and obligations of various parties involved, establish unambiguous directives for utilizing cyber capabilities, and guarantee responsibility for actions taken in cyberspace. Policymakers must also consider the ethical ramifications of cyber operations and try to find a balance between security concerns and the safeguarding of human rights and civil liberties.

Cyber diplomacy is an essential instrument for tackling the issues arising from the militarization of cyberspace. Diplomatic endeavors can foster global agreement on crucial matters, facilitate intergovernmental dialogue, and advance the establishment of standards and accords. Investing in cyber diplomacy entails enhancing the knowledge and skills of diplomats and policymakers to comprehend and tackle the intricacies of cybersecurity in the digital realm.

Conclusion

There is a growing risk that cyberspace may become military, which presents a significant challenge that is constantly evolving and has far-reaching implications for the governance and security of the entire planet. Cyber operations are becoming increasingly likely to result in more significant conflicts as nation-states become more conscious of the strategic significance of cyber capabilities. The adoption of a comprehensive strategy that includes the building of cyber resilience, the establishment of global norms and agreements, the promotion of transparency and the implementation of steps to build confidence, the creation of legal and policy frameworks, and the allocation of resources to cyber diplomacy is required to reduce this risk.

By implementing these measures, the international community can work toward achieving a safer and more stable online environment, one in which the potential dangers of militarization and conflict do not overshadow the benefits of digital interconnectivity. To successfully navigate the complex landscape of cyber security and protect the integrity of this essential domain, the future of cyberspace is dependent on the concerted efforts of states, companies, and individuals working together. By implementing these measures, we can ensure that cyberspace not only remains secure but also becomes an influential stimulus for positive change and innovation in our society.

References

- Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. Ecco.
- Lin, H. (2012). *Cyber conflict and national security*. The Cato Institute.
- Rid, T. (2013). *Cyber War Will Not Take Place*. Oxford University Press.
- Valeriano, B., & Maness, R. C. (2015). *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press.
- Weiss, T. G., & Daws, S. (Eds.). (2018). *The Oxford Handbook on the United Nations*. Oxford University Press.