SITJOURNAL
Security Intelligence Terrorism Journal

*Security Intelligence Terrorism Journal (SITJ), Vol. 02 No. 01 (2025), pp. 48-55*
*Research Article*
**doi:** https://doi.org/10.70710/sitj.v2i1.31

# Cyber Warfare And Its Place In Modern Geopolitics And War

Idden Aryasatya[1,a,*], Eko Daryanto[2,b]

[1,2]National Defense Studies, University of Indonesia, Indonesia
[a]iddenaryasatya010@gmail.com; [b]eko.daryanto151@gmail.com
*Corresponding author

**Article Info**
Received: 23-Dec-2024
Revised: 29-Jan-2025
Accepted: 30-Jan-2025

**Keywords**
Cyber Security; Cyber Security; Development; Technology

**Abstract**
There are now major cybersecurity concerns as a result of how fast technology has changed geopolitics. Attacks against a nation's communication, infrastructure, and economy through cyber espionage, sabotage, disinformation, and DDoS attacks undermine national stability. The high level of digital integration in industrialized nations makes them easy targets, while the lack of resources and digital knowledge makes underdeveloped nations vulnerable. There has to be international collaboration on cybersecurity rules and ethics because of this chasm. While cutting-edge innovation like AI strengthens defenses, it also introduces new dangers and raises new ethical questions. This study delves into the consequences of cyberwarfare. It highlights the importance of strong cybersecurity measures, online education, and global cooperation to safeguard nations and their inhabitants against ever-changing cyber dangers.

## 1. Introduction

Concerning the contemporary issues within the geopolitical field, it is safe to assume that modern technology has developed too quickly for a number of states. This could be seen by viewing the integrity of the state when discussing cybersecurity issues; it is not to say, however, that smaller or less developed states could not combat this in any way. Some states lean towards technological-based progression within the confines of state security as time went on; this could be followed through if one focuses on the industrial revolution. By now, the technology we have and utilized is part of the 4th coming of the industrial revolution (Muller, 2015).

Cities with a larger and more complex infrastructure usually prioritize things related to smart cities. It turns out, however, that relying heavily on these technological wonders has some side effects, one of which is the tendency to push forward agendas or policies that would favor a state's economy or, in a bleak sense, it would be in the interest of large companies and conglomerates. Using self-driving cars, automated industries, e-banking, and e-commerce may seem like a big step forward. Still, with such integration, the newly added idea sometimes lacks proper policies, laws, or even ethics. The probable cause of cyberattacks is when a target becomes too lenient or instead becomes fully integrated to such an extent that dangers and threats from cyberspace or real life may have affected it (Clim, 2022).

Due to the immense growth of technology, states may now face less conventional issues. Cybersecurity nowadays is not just about protecting individuals, companies, or institutions; it has now escalated to war tactics and/or espionage. Known now as cyber warfare would now endanger the national security of a state if it were to be directed towards a country with less than suitable conditions for cybersecurity; these attacks may come directly from states in an act of aggression or could be from a group of individuals threatening both public safety and national security (Digmelashvili, 2023). These threats would now be in the form of

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0)

cyberspace or, in more straightforward terms, the Internet. The vast utilization of cyberspace by numerous users would lead to a dependency on technology, a technology that has been a part of everyday life in the modern era. The technology itself, though deemed helpful to society, would need some regulations if it meant being safe from it. Implementing simple digital literacy as public knowledge in schools would significantly reduce the number of attacks occurring for people. Hence, as a result of overuse of technology could potentially lead to issues within real life; in extreme cases, the incapacitation of an institution within a state would be a determining point for some countries to take into account how serious cybersecurity really is (Peter, 2023). This paper aims to analyze the impact of cyber warfare on national security, explore its implications on geopolitics, and recommend measures for enhancing cybersecurity as the new technology develops; contingency plans for such tools should, at the very least, be supervised thoroughly.

## 2. Discussion

## 2.1. Cyber Warfare Applications

The applications of cyber technology in warfare have some implications which would concern national security as a whole. Since there are many applications of such issues, it is worth noting that some countries are less susceptible to these concerns as some developed countries have yet to integrate their technology into the masses, whilst most commonly developed countries have their technological advancements be part of everyday society. However, most developing countries do have technology dependencies on par with developed countries, just less secure and sometimes less digitally literate (Popoola, 2024). Some key applications in cyber warfare are as follows:

- Targeting a key infrastructure of the state is within the realms of possibility, as it has the potential to temporarily incapacitate a state which would cripple power grids, water supply, transportation, and telecommunication. The attacks themselves would then generate chaos within the masses and could also affect military operations as civil unrest erupts into possible riots or strikes (Imperva, n.d.). The most clear-cut example is the downed power grid in Ukraine, which was suspected to be orchestrated by Russian actors; the event caused thousands to lose electricity and caused significant momentary damage (Pollard, 2024).

- Espionage in contemporary issues is usually correlated with technological factors; the use of technology for humans runs the risk of being spied on. What some espionage or covert missions target is information, preferably those that are state-sensitive, which cover military, political, or economic information regarding the state. Though it resulted in near to no damage, it would have long-term effects internally and externally for the state; since the act of spying itself is staying hidden, the mistrust or distrust would then possibly lead to a larger chain of events which may endanger the state (Gillis, 2023).

- Sabotage is a standard action in warfare; the main idea is to turn off key parts of the military infrastructure somehow to gain an advantage over an opponent. Whilst sabotaging in cybersecurity could seem less apparent at first, it could result in a much larger problem. Primarily, the sabotage itself targets key points such as communication, databases, weapons, and targeting controls, along with systems within the military that could be breached. These alterations could be the determining factor of a conflict or a battle, as they may hinder the operation of a state's military (Slonopas, 2024).

- Another form of sabotage that is also used in cyber warfare is targeted towards the state's economy. Economic sabotage is utilized to disrupt the economic flow of a state by targeting the economic infrastructure, such as the financial systems of a state, stock markets, and digital banking infrastructures, which in turn would lead to economic instability. This would sufficiently cripple economic operations, with transactions being disrupted, accounts being hacked, and, most commonly, stealing assets from banking clients or shareholders. Thus, the sabotage itself would lead to a number of issues within its populace. Still, historically, it could lead to public distrust and the economic collapse of a nation (Slonopas, 2024).

- Though more traditional in terms of its utilization in warfare, cyber misinformation or cyber propaganda is used extensively to a target audience. It most likely targets a general group to alter

their viewpoints and influence them to adhere to specific information. This type of action could be considered overt, as it relies on discrete planning and intentionally manipulating the public. It is the most similar to conventional methods, as traditional propaganda is used in the same way, and in some cases, to destabilize political systems by spreading manipulative information (Kravchenko, 2024).

- A more direct approach to cyber warfare is Distributed Denial of Service Attacks (DDoS) attacks. These attacks would prove to be concerning as they disrupt government systems, telecommunication, and military operations. As the attacks are more apparent, it is used as a method to throw the state into disarray, with public trust being lowered, mainly attributed to the government's incompetency concerning digital protection. It also has the potential to paralyze government operations, which could lead to a shutdown of government-based websites as DDoS attacks become more prevalent in cyber warfare. However, defenses against such types of attacks have been improved to at least nullify the effects but not the risks (de Neira, 2023).

- A relatively new form of cyber warfare as direct as Ddos attacks are cyber weapons, these new technological weapons of combat that allow the attack to affect physical structures. One of these tools was initially developed by the United States and Israel in 2010 and was used to attack Iran's nuclear infrastructure without using any traditional weapons. The creation of the tool shows the forward advancement of cyber warfare. As time went on, the combat of cyberspace has crossed its boundaries into the physical world. Hence proves that cybersecurity is just as crucial to be developed in a nation as its military presence upholds national security (Mushkhanov, 2023).

- In lieu of current geopolitical struggles, some developed countries have advanced their cyber technology in its use for warfare, as mentioned earlier. It is now, however, being used in tandem with conventional warfare. As stipulations of warfare became more stringent towards technological advancements, wars could now be initiated through cyberspace. The development of EMPs suggests that, at some point, war has become a battleground of mixed tactics that, as of now, require far more resources than before. It shows that military actions alone do not fare well in a physical sense where terrain or location does not seem favorable. Hence, the newly adopted idea of war has cyber technology included in its structure. Per se, wars can be engaged by sabotaging, propaganda, and espionage not just in a conventional path, but a far more contemporary aspect using cybers warfare as seen in real life (Mumford, 2023).

- Though warfare as of now varies greatly depending on the national interest, the appearance of cyberspace and cybersecurity can profoundly disrupt state operations. By the time modern war has become far more complex, as the adoption of technological improvements has created a way to provide means of attacking, it is only natural that the development of countermeasures and counteroffensive tactics becomes more prevalent. As the use of cyber threats, real-time monitoring, and Artificial Intelligence (AI) become more apparent, the harmful effects of cyber-attacks may become more lenient as technology develops (Obi, 2024).

- In other cases related to cyber warfare, its use may also provide a side effect that proves fruitful in some regard. Instilling fear in the public will significantly improve the rate of success that cyber warfare provides; as in similar cases in conventional warfare, the use of military-grade cyber attacks could affect the public disposition regarding the state while also creating unease. The far-reaching consequences of warfare have always created lasting effects; the impact of hybrid campaigns is subsequent to its more traditional counterpart since war has always generally been an issue that affects physiology as well. The proper usage of fear can be conducted in the simplest of ways by creating false alarms that keep the populace and the state on edge. As mentioned before, the use of propaganda and its relative ease of use could create a dispersion of national security. Hence, the process would create panic and destabilize the target; no matter the form, warfare has always included the physiological aspect of it, shellshock or fear-mongering as examples in history (Bardin, 2024).

## 2.2. Ethics In Cyber Warfare

As mentioned above, these examples are the base of cyber warfare, its usage may prove to be unfamiliar to some states, especially developing states with low GDP per se. However, the concern itself is as genuine as traditional warfare; though some states have less integration than others, it is safe to state that as years pass by, even smaller or micronations will adopt these technological advances. These facts can easily be traced to how some smaller countries' infrastructure has yet to support typical digital applications and have inequalities within them (Khan, 2024). The lack of resources in a country also significantly contributes to the well-being of cybersecurity as "Developing countries often lack the financial means to invest in the infrastructure, manpower, and technology needed for effective regulation." Thereby reducing the development of their technological department as a whole (Kayode, 2023). It is also worth mentioning that since less developed countries tend to ally with other states for safety, they rely heavily on their cooperation to sustain a form of technological growth that could potentially be fleeting if not harnessed correctly (Bartlett, 2024).

However, while the technology itself develops at a rapid pace, some ethical concerns are less heard of since the idea of such a novel thing is yet to be practiced in ideal circumstances. Using technology in warfare has not been a new idea; the usage of radars, transmitters, and telephone lines has been etched into history. Thus, one can genuinely ask where one draws the line to put in place regulations akin to the Geneva Convention for cyber warfare. Although not technically adapted to warfare regulations, some concerns have been raised about this to some degree (Wilson, 2023). Some ethical concerns are as follows:

- Collateral damage has been part of many wars; some may even try to attack said collateral, such as monuments or historical sites. However, collateral is in of itself an event that one did not factor in when calculating the plan. Civilian deaths can be emphasized as collateral, but other parts such as hospitals, schools, libraries, research institutions, and transportation hubs in cities could also be a part of that. In other terms, these are prime targets for cyber attacks. Since civilians usually rely heavily on public services in their everyday lives, disrupting what civilians use would also disrupt the government as well. In some extreme cases, the military may be sent out to put out the metaphorical fire. Things such as power grids are what power today's lives and nations, but because both the state and the people use them; it makes it an easy target if one is trying to hamper or cripple a state. To some extent, some of these damages are collateral and are not meant to cause civilian harm. However, due to the range of motion that cyber warfare includes in its attacks could not be specified, it is far easier to deem that collateral as accidents (Cremer, 2024).

- Attributing rights and wrongs are a staple part of any conflict. To justify war per se, one must have Casus Belli, and for any reasonable efforts to spark a war, the wrongs are then placed on the aggressor. It is, however, rather complicated to conclude one's wrongdoings when it is nearly impossible to trace them in the first place. Though it is possible in some instances to figure out the perpetrators, the reasoning and evidence itself must be solid. As quoted by Kravchenko (2024), "States and organizations may launch information operations to present evidence or make accusations against the adversary, such as disseminating information about the cyberattack disclosing methods and perpetrators". Finding proper evidence is then tricky since it may unnecessarily escalate tensions further and may potentially violate laws put into place for warfare itself (Lonergan, 2023).

- In war, there have always been cases of accidental deaths or collateral as it's been covered before; cyber warfare, at the very least, tends not to create deaths of innocent bystanders. However, those bystanders can be indiscriminately harmed when executing a cyber attack (Neil, 2009). While the operation of cyber attacks itself sometimes deems non-combatants a necessary casualty, the damage itself will always linger on the innocents; leaking private data or disrupting essential and possibly life-threatening services –such as executing a blackout– could end up resulting in potential non-lethal harm or could result in life-altering changes or death (Shandler, 2023).

- The lack of regulations or policies relating to cyber warfare and its usage has yet to be universally regulated. Hence, the issue is that even in warfare, it could be considered a newly adopted tactic, that is, when discussing conflict usage. On the other hand, the dilemma still stands as there is malicious use of this technology since there are no proper laws put into place that restrict or

prohibit specific actions. The rise of AI or the utility of specific cyber warfare technology, though it has been discussed in the international community, still lacks the proper regulations (Buçaj, 2025).

- Regarding issues of psychological harm that have been briefly discussed, it is essential to understand that when conducting cyber warfare, the target of any attacks may result in trauma or psychological damage for civilians. Bystanders in war should be treated as non-combatants according to the Geneva Convention, however, since cyber warfare is a new form of combat, it is difficult to differentiate the proportionate damage it could deal to civilians (Shandler, 2023). Conversely, damage done to civilians is not only calculated through psychological effects but could enter the realm of economic endangerment. This could happen due to crossfires within cyber warfare, and justification of such actions is commonly disregarded as yet again collateral damage. But, at some point, the line between incapacitating the state's government and accidentally harming non-combatants that result in economic instability or distress should be revised if concerns of ethics are prevalent (Atrews, 2020).

- Lastly, due to the entanglement of both civilian and military applications of cyber tools, it is difficult to tell apart the boundaries of combat and non-combatant in war. It should be noted that since cyber warfare has ties to international affairs and has probable issues in geopolitics, such as the silent war in Pakistan and India, the main target of attacks could hardly be precise, and it could be sourced from both the government or civilian that launch cyber attacks (Taddeo, 2022).

## 2.3. Development of Cyber Warfare And Cybersecurity

Since warfare has evolved beyond what would usually be conducted on the physical ground, the coming of cyber warfare takes a toll on security policies set up by states and security communities in the international world. While innovation is a large part of developing an adequate defense, the bridge between politics and war has to add cyber technology to its midst now. State and international politicking will change strategies and ideas in the future, along with national security either having it implemented or, at the very least, having a way to mitigate cyber-attacks. It is important to note that by now, power dynamics do not only concern military power; the power dynamics itself would change entirely as hard power implements cyber tools to its arsenal (Haddad, 2024).

The notion that technology may surpass the boundaries of man has been held near in many media and literature, and the concept of robotics or AI has made waves in recent years as well. Yet now, it is capable of assisting humanity by simplifying tasks and automating processes. Still, in the realm of cybersecurity, this complicates the matter as the ideas of novelty AI have entered the baseline of state and organizational defenses. AI, in this sense, is simply bots that follow a set of commands in its simplified state; however, in a more complex manner, AI could learn and adapt to certain conditions, being more sophisticated as time passes (Raska, 2023). Cyberattacks using these new technologies are still a new concept, but these attacks have far more creativity than before. Attacks on the state are usually a mix of both discrete and direct attacks, which, as mentioned before, target state infrastructure to an extent. While attacks on individuals are technically discrete if one has low digital literacy, since phishing, malware injection, DDoS attacks, DNS tunneling, etc, are seen as one that infects a device or non-physically harms the user rather than using attacks that per se overload a device and make it explode (Al-Hawamleh, 2023).

Cyber tools themselves have adapted to be much more user-friendly and easy to use for deployment; this can change how cyberattacks work in an overall setting. As the capability of the technology improves, the better and more flexible it is to be utilized by institutions or the military (Rahman, 2023). However, the ambiguity of a traditional and a newly digitized battlefield will prove to –at the very least– challenging to sort out as regulations and possible speculations of cyber tool usage become more apparent; warfare then has to accommodate laws and conducts concerning cyber warfare (Mumford, 2023).

## 2.4. Cybersecurity Potential Damage Of Cyber Warfare

Integration of a novel type of technological development is commonly seen as an evolving procedure. Cybersecurity itself has some issues integrating due to the lack of funding for some states or even readily available specialists who could operate cyber tools and their technology in the state. However, roughly 91% of cyber leaders have been surveyed concerning the ever-growing change in cybersecurity infrastructure.

They pointed out that a cybersecurity event that concerns geopolitical instability may rear its head sooner than expected (World Economic Forum, 2023). Since the parameters for cyber attacks are more commonly associated with individuals working by their lonesome, the cyber attacks directed towards the government have risen from 40.000 cases in February of 2023 to 100.000 recorded cases in the same year around August of 2023 (Statista, 2023).

Considering developed states have more leeway on the budget for cybersecurity, it also makes them prone to more attacks since the resources and data they store are worth their weight enough to launch attacks or initiate espionage. The issue of whether developed states fare better than developing ones has been made clear and can usually be attributed to the economy and the state's coffers. However, large states, Australia, for example, have had 11% of the incidents that occurred affecting the state's infrastructure and have targeted their public sectors. These include power, water, gas, hospitals, schools, and public transport (Reuters, 2024).

Currently, most governments in the world with high development in technology would invest millions in their cybersecurity sector. Furthermore, organizations have increased funding in their cybersecurity to the wall against malicious attacks and threats; organizations are stated to have spent $176 billion in 2023 and could surpass $200 billion in 2024 for cybersecurity investment. These investments are a natural reaction to the threats present in cyberspace and improper or lacking cybersecurity structure, as cybercrime itself is projected to have cost the global economy approximately $9.5 trillion in 2024 (Mclean, 2024). On the contrary, due to the rapid adoption of AI, it has been developed and swiftly integrated into cyber tools to both use offensively and defensively. Yet, due to the widespread use of this technology, nearly every associated individual who knows the utilization of cyber tools has the potential to launch attacks, and a state or organization's defense is only as good as one's budget (Pratt, 2023). Hence, it is imperative that cybersecurity, state or otherwise, must be developed thoroughly so as not to leave any cracks in one's defenses. As discussed beforehand, the idea of growing threats that could fundamentally change how one operates an organization or a state is now far more feasible than ever before.

## 3. Conclusion

Thanks to the rapid development of technology, hacking, and cyberwarfare have become very common. This has completely changed how politics works, as it gets worse for countries when they depend more on technology for things like transportation, infrastructure, and economic safety. Spying, hacking, sharing hoaxes, and direct attacks like DDoS are all forms of cyber warfare. Cyberattacks on Ukraine's power grid are one way that both state and non-state actors can cause disruption and incapacitate countries.

Cyber threats can still happen in wealthy countries, even if they have an assortment of modern technology. In fact, they are easy to target since they depend on computer systems. They are more likely to be breached, though, because they do not have as many ways to keep their computers safe, and their defenses are not as strong as they would hope they would be. The difference between the two shows that an actor needs a global plan to make attacks and defenses stronger, with rules and morals like those that govern real war. When new technologies, AI, are now commonly used in security, they make things possible whilst also providing a way of attack. These tools can make defenses better, but they also make these issues less safe and raise moral questions when conducting operations of cyber warfare. Strong protection is more critical than ever as the number of global conflicts grows, and digital safety is not just the responsibility of state actors; it's a task that everyone should learn from.

This paper touches on contemporary subjects which are yet to be normalized in military expenses. The appearance of such wonders would bring many new technological marvels. However, a caveat in its place would settle in warfare. This paper would not be possible without the availability of today's informational technology, such as the internet, that provides substantial data for this paper. Hence, it is recommended that this paper should be followed in the future with new information, regulations, laws, and policies, as this paper could only bring so much before it starts to appear repetitive.

## References

Al-Hawamleh, A. M. (2023). Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures. Momentum, 3(14), 15.

Atrews, R. (2020). Cyberwarfare: Threats, security, attacks, and impact. Journal of Information Warfare, 19(4), 17 – 28. Retrieved from https://www.jstor.org/stable/27033642

Bardin, J. S. (2024). Cyber warfare. In Computer and Information Security Handbook (pp. 1345 – 1380). Morgan Kaufmann.

Bartlett, B. (2024). Why do states engage in cybersecurity capacity-building assistance? Evidence from Japan. The Pacific Review, 37(3), 475 – 503.

Buçaj, E., & Idrizaj, K. (2025). The need for cybercrime regulation on a global scale by international law and cyber convention. Multidisciplinary Reviews, 8(1), 2025024 – 2025024.

Clim, A., Toma, A., Zota, R. D., & Constantinescu, R. (2022). The need for cybersecurity in the industrial revolution and smart cities. Sensors, 23(1), 120.

Cremer, F., Sheehan, B., Mullins, M., Fortmann, M., Ryan, B. J., & Materne, S. (2024). On the insurability of cyber warfare: An investigation into the German cyber insurance market. Computers & Security, 123, 103886.

de Neira, A. B., Kantarci, B., & Nogueira, M. (2023). Distributed denial of service attack prediction: Challenges, open issues and opportunities. Computer Networks, 222, 109553.

Digmelashvili, T. (2023). The impact of cyberwarfare on national security. Future Human Image, (19), 12 – 19.

Haddad, C., Vorlí ček, D., & Klimburg-Witjes, N. (2024). The security-innovation nexus in (geo-)political imagination. Geopolitics, 29(3), 741 – 764.

Kayode-Ajala, O. (2023). Establishing cyber resilience in developing countries: An exploratory investigation into institutional, legal, financial, and social challenges. International Journal of Sustainable Infrastructure for Cities and Societies, 8(9), 1–10.

Khan, N. F., Ikram, N., & Saleem, S. (2024). Effects of socioeconomic and digital inequalities on cybersecurity in a developing country. Security Journal, 37(2), 214 – 244.

Kravchenko, O., Veklych, V., Krykhivskyi, M., & Madryha, T. (2024). Cybersecurity in the face of information warfare and cyberattacks. Multidisciplinary Science Journal, 6.

Lonergan, E. D., Smith, M. W., & Mueller, G. B. (2023, May). Evaluating assumptions about the role of cyberspace in warfighting: Evidence from Ukraine. In 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon) (pp. 85 – 102). IEEE.

McLean, M. (2024). 2024 must-know cyberattack statistics and trends. Retrieved from https://www.embroker.com/blog/cyber-attack-statistics/

Muller, L. P. (2015). Cybersecurity capacity building in developing countries: Challenges and opportunities.

Musakhanov, D. (2023). The international consequences of cyber warfare: A study of the Stuxnet case. Acta of Turin Polytechnic University in Tashkent, 13(3), 47 – 50.

Mumford, A., & Carlucci, P. (2023). Hybrid warfare: The continuation of ambiguity by other means. European Journal of International Security, 8(2), 192 – 206.

Obi, O. C., Akagha, O. V., Dawodu, S. O., Anyanwu, A. C., Onwusinkwue, S., & Ahmad, I. A. I. (2024). Comprehensive review on cybersecurity: Modern threats and advanced defense strategies. Computer Science & IT Research Journal, 5(2), 293 – 310.

Peter, A., & Ohakpougwu, U. (2023, May). Origins of cyberwarfare: How the internet got weaponized. In European Conference on Social Media (Vol. 10, No. 1, pp. 364 – 372).

Pollard, M. (2024). A case study of Russian cyber-attacks on the Ukrainian power grid: Implications and best practices for the United States. Pepperdine Policy Review, 16(1), 1.

Popoola, O. A., Akinsanya, M. O., Nzeako, G., Chukwurah, E. G., & Okeke, C. D. (2024). Exploring theoretical constructs of cybersecurity awareness and training programs: Comparative analysis of African and US initiatives. International Journal of Applied Research in Social Sciences, 6(5), 819–827.

Rahman, M. H., Wuest, T., & Shafae, M. (2023). Manufacturing cybersecurity threat attributes and countermeasures: Review, meta-taxonomy, and use cases of cyberattack taxonomies. Journal of Manufacturing Systems, 68, 196 – 208.

Raska, M., & Bitzinger, R. A. (2023). Introduction: The AI wave in defence innovation. In The AI Wave in Defence Innovation (pp. 1 – 11). Routledge.

Rowe, N. C. (n.d.). The ethics of cyberweapons in warfare. Retrieved from https://faculty.nps.edu/ncrowe/ethics_of_cyberweapons_09.htm

Shandler, R., Gross, M. L., & Canetti, D. (2023). Cyberwarfare and democracy: Emerging risks and protective measures. Journal of Cybersecurity Studies, 5(3), 245 – 267.