eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 03, Issue 05, May 2024

Destructible Domain: Is Cyberwarfare a new domain of warfare?

Mr. Aamir Khan[1] , Dr. Rajesh Kumar[2]
[1]Research scholar Department of Political Science, PPN College, Kanpur, India.
[2]Professor Department of Political Science, PPN College, Kanpur, India.

Received: 15 May 2024 Accepted & Reviewed: 25 May 2024, Published : 31 May 2024

Abstract

This article makes a counterintuitive argument that cyberwarfare is not a new domain of warfare. It has been unnecessarily hyped. The analysis of the past 20 years shows that there have hardly been any successful cyber-attacks and even supposedly successful cyber-attacks have had extremely limited success. This article argues that cyberweapons can be an irritant and can supplement other domains of warfare but cannot be considered a domain on their own or a separate domain of warfare. The so-called cyberwarfare suffers from a Prediction Paradox which means since it has already been predicted earlier hence its probability of creating havoc declines automatically as states become well-prepared for such an attack. Even if attacks take place, there are highly likely chances that they will be less catastrophic than predicted. The cost-benefit analysis of cyberwarfare from the state's standpoint also makes it an improbable choice, given the skill and money involved in developing a cyberweapon. In terms of cost-benefit analysis, cyberweapons are ineffective, and if ineffective, they cannot form a fifth domain of warfare. On the hand, the theory of deterrence is being used as a measure to deal with cyberattacks. There are two types of deterrence i.e., deterrence by punishment and deterrence by denial. However, this paper supports deterrence by denial as a viable policy measure to deal with cyberattacks. Deterrence by denial is an approach that emphasizes improving cybersecurity and resilience to make it harder for attackers to successfully breach systems, steal data, or disrupt operations. As far as cyberattacks are concerned, deterrence by denial is the best strategy.

Keywords Cyberwarfare, Cyberweapons, Cyberattacks, Prediction Paradox, Domains of Warfare, Deterrence by Denial

Introduction

The growing intensity of cyberspace creates an illusion that this is the new normal and whatever big will happen, will happen in this domain. The pervasiveness of the internet in our life raises the obvious question of whether we are living in a cyber-driven world with cyber-led attacks. There is increasing emphasis on declaring cyberspace as the new domain of warfare and that future wars will be cyber wars. However, a thorough and critical understanding of the cyber world dispels the idea that cyberwarfare is the new domain of warfare. There is considerable disagreement about whether cyber warfare represents a new area of warfare or merely a new tool within current fields of warfare. While arguing that cyberwarfare is not a domain Michael P. Kreuzer explained that the operating environment can be divided into two major types: layers of warfare and domains of warfare. Layers of warfare are defined as operating environment media that allow military operations to be performed and operational effects to be realised across all domains of conflict. A domain of warfare is described as a physical sphere of the operating environment that requires specialised doctrines, organisations, and equipment for armed forces to successfully control and exploit in the execution of military operations. In its typology, cyberspace is not the space domain, but rather a multi-domain operational construct, more akin to special operations or intelligence operations. These constructs are function-centric,

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 03, Issue 05, May 2024

frequently dealing with difficulties relevant to modern combat but not usually in the conventional military context (Kreuzer, 2021).

A cybersecurity analyst and specialist, Carr (2012) defines cyberwarfare as "the art and science of battling without fighting, of beating an opponent without spilling their blood". According to the definition, the goal is to accomplish victory with no bloodshed. This is in itself a contradiction if something is defined as warfare but involves no violence. The three classical principles of Clausewitz whose theory is still relevant to understand the concept of war, state that, initially the opponent's military forces must be destroyed. Second, the country must then be occupied. Finally, the enemy's will must be crushed (Lindell, 2009). There is no cyber-attack that fits all three conditions if the use of force in war is violent, instrumental, and political. Furthermore, very few cyber-attacks in history have met only one of these conditions (Rid, 2012). The comprehensive analysis of cyber-attacks made so far in this article vindicates the argument.

This article analyses the cyber world from two aspects. The first is the Prediction Paradox and the second is cost-benefit analysis. In the end, this article will suggest a strategy of deterrence by denial, which is already being used by various countries, enough to deal with future cyber-attacks.

After establishing that cyberwarfare is not a new domain of warfare, this paper argues due to Prediction Paradox a successful cyber-attack is highly unlikely because targets already anticipate such attacks and prepare themselves.

Prediction Paradox

Cyberwarfare as a domain of warfare has been unnecessarily hyped. The analysis of the last 20 years reveals that there have been few successful cyber-attacks, and those that have been deemed successful have had extremely limited success. The basic reason behind this is that various states have been so well prepared that their firewalls protect them from any targeted attacks. At the very best cyber-attacks can only be described as a minor nuisance. One reason behind this may be the Prediction Paradox. The Prediction Paradox is a concept in philosophy and logic that suggests that the act of predicting an event can undermine the likelihood of that event occurring. This is because the prediction itself can change the circumstances surrounding the event, making it less likely to occur as predicted (Rescher, 1998). The paradox arises because predictions can affect the behavior of individuals and groups, making it difficult to accurately predict the outcome of an event.

For example, if a weather forecaster forecasts a strong storm tomorrow, people may take precautions such as remaining home or storing up on supplies. Yet, if enough people take these precautions, the storm may occur, or it may be less catastrophic than predicted.

In case of cyberwarfare, consider a scenario in which a cybersecurity analyst predicts that a specific sort of assault is likely to occur based on prior attack patterns and intelligence. The analyst takes steps to prevent the assault, such as adding extra security measures or enhancing surveillance. The Prediction Paradox can make it difficult for attackers to anticipate defensive behaviour and change their tactics accordingly. If an attacker predicts that a target's security protections would be weak and launches a relatively basic attack, but the target has upgraded their defences in anticipation of the attack, the attacker may be compelled to abandon the attempt or employ more advanced methods. This can be difficult for attackers because they may lack the resources or ability to respond rapidly to changing circumstances.

The cyberwars were predicted when cyberspace itself was not that pervasive. In the article “Cyberwar is Coming!’ According to RAND Corporation's Arquilla and Ronfeldt (1993) cyberwar may be to the twenty-

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 03, Issue 05, May 2024

first century what blitzkrieg was to the nineteenth. As a result, states have prepared so well that their firewalls shield them from any targeted attacks. The Y2K crisis is a prime example of the Prediction Paradox. In 1993, a magazine called 'Computerworld' first mentioned the Y2K or millennium bug. The magazine published a story titled "Doomsday 2000" (Javaid, 2020). When the year 2000 approached, computer programmers realised that the number 00 may be interpreted by computers as 1900 rather than 2000. Tasks planned on a daily or yearly basis might be harmed or faulty. Yet, nothing globally crashed on December 31, 1999 (Y2K Bug, n.d.). Another example of the Prediction Paradox is threats to national holidays. Due to threats from several anti-state and terrorist organisations, national holidays are normally guarded very closely. As a result, the national security system is so well prepared for probable attacks that attacks on holidays rarely takes place.

Hence, the Prediction Paradox played a significant role in confining cyberspace a supplement to the other four domains of warfare rather than a domain in its own right.

Although the Prediction Paradox renders a successful cyber-attack extremely unlikely, cost benefit analysis suggests that an attacker may be dissuaded by the notion that a successful cyber-attack may be prohibitively expensive in comparison to the extremely high cost involved.

Cost-benefit analysis

The most important aspect of any weapon is its efficiency. How much it costs to manufacture and the kind of destruction it can unleash is the ultimate test of a weapon. The sophistication and the money involved in making a cyberweapon are millions of dollars. Yet, in terms of cost-benefit analysis, cyberweapons are ineffective, and if ineffective, they cannot form a fifth domain of warfare. The cost-benefit analysis of cyber-attacks can suggest that such attacks are often inefficient and not worth the effort.

These cyber-attacks can be effective in certain circumstances, the costs and risks involved often make them an inefficient weapon. There are many examples of cyberweapons being ineffective and less lethal compared to other domains of warfare. The 2008 Russia-Georgia war is perhaps the most frequently cited example of cyber operations being employed in concert with more traditional military means. In that case, the Russian land and air campaign was preceded by cyber-attacks on the digital networks of Georgian government ministries and military units, causing confusion and reducing their ability to communicate, and arguably providing a significant military advantage to the advancing Russian offensive (Burton, 2015). Prima facie, the cyber strikes were not violent in and of themselves, but they significantly improved the capability and ability to advance Russian forces to launch a violent military advance.

Another example is the Stuxnet which was dubbed the “Hiroshima of Cyber War” (Gross, 2011). The 'Stuxnet' virus, developed and implemented by the US and Israel and detected in the networks of an Iranian nuclear power station in 2010, was, according to analysts, a complex operation that took many years to build, cost up to $300 million, and likely required a human operative (Domingo, 2015). The incident, which was designed to halt Iran's nuclear enrichment, destroyed one-fifth of the facility's centrifuges. Yet, the rate of enrichment increased during this episode, demonstrating the limited influence of even the most sophisticated cyber operation.

Similar conclusions can be derived from the December 2015 Ukrainian power grid breach, which resulted in a blackout for nearly 230,000 people in Western Ukraine. To prevent responses to the disruptions, Russian hackers disabled power supplies and launched a telephone denial of service attack against customer support call centres. The logistics and months of planning needed in this operation were rated "extremely complex". The attack's impact on the target was also clearly limited, as power was immediately restored thanks to a

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 03, Issue 05, May 2024

human override device. These high-profile cases demonstrate that cyber operations are neither inexpensive nor simple to execute in order to achieve strategic triumph (Zetter, 2016).

In recent times, around 6,000 attempts were made to hack into the Indian Council of Medical Research's system (ICMR). The site was hosted at National Informatics Centre (NIC) Data Centre. The NIC was notified of a cyber-attack by email and has stated that the attack was averted. The website could not be hacked due to the installation of an upgraded firewall and additional security measures. The ICMR has discovered the website in the order and systems were running just fine (Bhardwaj, 2022). Despite cases of attacks on hospitals, schools, local governments, or ransomware, they can be avoided. But, given that the state is the dominant actor, it does not stand up against the might of the state. In most cases, the compromised system is quickly restored which again questions the efficacy or lethality of cyberweapons but it will not be declared as a new warfare domain in the near future.

Prediction Paradox and Cost-benefit analysis prove the unviability of cyber-attacks, even the cyber-attacks which are likely to be successful can be handled by strategy of deterrence by denial. This paper proposes deterrence by denial as a perfect strategy for handling cyber-attacks.

Deterrence by Denial

Deterrence is the practice of discouraging or restraining someone in world politics, usually a nation-state—from taking unwanted actions. Deterrence works when the target believes that the costs and hazards of a military attack outweigh the expected benefit (Mazarr, 2018). The traditional literature identifies two basic approaches to deterrence: deterrence by punishment and deterrence by denial. Deterrence by denial techniques aim to dissuade an action by making it impossible or unlikely to achieve, depriving a potential aggressor confidence in achieving its goals. Deterrence through punishment, on the other hand, warns of severe consequences in the event of an attack, such as nuclear escalation or heavy economic penalties. The focus of punishment deterrence is not the direct defence of the contested commitment, but rather threats of broader punishment that would raise the cost of an assault (Borghard & Lonergan, 2021). In the case of cyberspace, the use of deterrence by punishment is not a viable option. The most important reason is its viability, as proved previously in numerous situations, that the level of skill and cost involved, as well as the governments' readiness, make this tactic of limited utility. The deterrence by punishment includes by "conducting strategic cyber-attacks (within-domain), or through kinetic non- cyber means, which may include conventional or nuclear military force (cross-domain) (Borghard & Lonergan, 2021)." However, it is difficult to determine if the absence of opponent strategic cyber-attacks is due to effective punishment or to other, unrelated variables.

Examples of ransomware attacks against civilian critical infrastructure, such as pipeline attacks (Siberian Pipeline Explosion 1982), attacks on Georgian private and public websites and recent ICMR websites, have resulted in very small, short-term service outages. As a result, deterrence through punishment based simply on offensive cyber operations is unlikely to be effective since cyberwarfare is insufficient to induce an unacceptable level of fear and agony in an adversary.

Thus, deterrence by punishment is not a viable option in the context of cyberspace. The difficulty of attribution, risk of escalation, challenge of determining proportionality, and potential for unintended consequences make this strategy impractical and potentially dangerous.

Deterrence by denial is a concept that involves making it difficult for an adversary to achieve its objectives through cyberattacks. It is an approach that emphasizes improving cybersecurity and resilience to make it harder for attackers to successfully breach systems, steal data, or disrupt operations. Deterrence by denial is a

eISSN 2583-6986
IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 03, Issue 05, May 2024

pragmatic strategy to deal with cyber-attacks. This approach emphasizes the importance of preventing attacks from succeeding in the first place, rather than relying solely on the threat of retaliation to deter attackers.

Deterrence by denial in cyberspace is strategy in cyberspace on which states can reply upon. The US Department of Defense (DoD) employs a deterrence by denial tactic. This technique was evident in the Pentagon's 2015 cyber strategy, and even the 2018 DoD Cyber Strategy, which established the concept of "defend forward," has components of the defensive form of deterrence by denial (DoD Cyber Strategy and Cyber Posture Review, 2018). The Defense Department's doctrine defines defend forward as "disrupt or halt harmful cyber activity at its source, even behaviour that does not rise to the level of armed conflict."

On the other hand, the Hunt Forward Operations (HFOs) are solely defensive cyber operations carried out by the United States Cyber Command (USCYBERCOM) at the request of partner states. The strategy of “Malware inoculation” is also an effective way to secure the cyberspace with public private collaboration. Sharing the information in public domain about adversary malware can aid in the "inoculation" of domestic networks by allowing network defenders to patch vulnerabilities that the malware exploits and create signatures that alert defenders to the presence of the malware in their environment. Malware inoculation limits the attack surface of possible US targets, making it more difficult for enemies to fulfil their goals (Borghard & Lonergan, 2020). For example, the U.S. Military Publishes North Korean and Russian Malware. The Cyberspace Solarium Commission suggests that the United States speed up current malware inoculation efforts. This would provide additional opportunity for the commercial sector to establish response strategies and safeguard their systems.

The Cyberspace Solarium Commission’s March 2020 report articulates how actions by US military cyber forces that could be defined as offensive at the operational level—gaining access to and manoeuvring within and across non-US cyberspace—are nonetheless meant to serve defensive strategic objectives—enhancing the US's defence and resilience in cyberspace (Cyberspace Solarium Commission, 2020).

However, these defensive approaches to deterrence by denial are not clear about what constitutes an optimal posture for a deterrent defense versus actual defenses. "Organizations should adopt what we in the cybersecurity industry call an 'assumption of breach' approach, where defenders operate on the basis that an adversary has already gained access to their sensitive networks," Dmitri Alperovitch said in Congressional testimony in February 2021, reflecting on the SolarWinds hack (Homeland Cybersecurity, 2021.).

Borghard and Lonergan (2020) while analysing the applicability of deterrence principle in cyber space stated that the best prospects for cyber deterrence center on a more offensive deterrence by denial approach. They also highlighted that the analogy to conventional deterrence rather than nuclear deterrence is significant. In the latter situation, the use of force implies that deterrence was ineffective. Yet, for conventional deterrence, actually carrying out operations could serve as a deterrent rather than signalling their failure. The goal is to make adversary military operations more expensive by focusing on their offensive capabilities and strategy rather than solely on defence. The Counter-cyber operations may directly increase the costs of adversary offensive cyber operations by halting nascent operations, reducing adversary attack capabilities, or denying adversary attack infrastructure access. Furthermore, counter-cyber operations may have secondary and tertiary repercussions, making it more difficult for adversaries to execute offensive strategies.

Hence, deterrence by denial involves improving cybersecurity and resilience to make it harder for attackers to achieve their objectives. By implementing strong cybersecurity measures, regular monitoring and assessment,

incident response plans, collaboration and information sharing, and effective deterrence strategies, organizations can improve their cybersecurity defenses and reduce the risk of successful cyber-attacks.

Conclusion

The cyberworld is the present and the future, the purpose is not to belittle it or indicate that it is less important on the contrary it is becoming an important part of lives and it is now far more essential and will only become more so in the future. However, Cyberworld is undoubtedly an important field of knowledge different from others, but by this logic, any military speciality may be termed a domain in some manner. Cyberwarfare is certainly a new way to conduct warfare, it is not a completely new domain of warfare. The use of technology in traditional warfare, the existence of cyber-attacks outside of warfare, the blurring lines between traditional and cyberwarfare, and the adaptation of military doctrine to include cyber all suggest that cyber warfare is an extension of traditional warfare, rather than a completely new domain. On the other hand, in most of the cases, the system affected gets restored in a while, so defense is a better option for such incidents. It can fall under the category of security while being ineligible for designation as a new domain of warfare.

References-

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, 12(2), 141–165. https://doi.org/10.1080/01495939308402915

Bhardwaj, S. (2022, Dec 6). Around 6000 attempts made to hack ICMR server on Nov 30; website safe after attacks prevented. *Asian News Agency*. https://www.aninews.in/news/national/general-news/around-6000-attempts-made-to-hack-icmr-server-on-nov-30-website-safe-after-attacks-prevented20221206195227/

Burton, J. (2015, May 13). Cyber warfare – a new strategic reality. *National Library of New Zealand*. https://natlib.govt.nz/blog/posts/cyber-warfare-a-new-strategic-reality

Borghard, E. D., & Lonergan, S. W. (2020 April 22). U.S. Cyber Command's Malware Inoculation: Linking Offense and Defense in Cyberspace. *Council on Foreign Relations*. https://www.cfr.org/blog/us-cyber-commands-malware-inoculation-linking-offense-and-defense-cyberspace

Borghard, E. D., & Lonergan, S. W. (2021). Deterrence by denial in cyberspace. *Journal of Strategic Studies*, 1–36. https://doi.org/10.1080/01402390.2021.1944856

Carr, J. (2012). Inside cyber warfare 2e: Mapping the Cyber Underworld (2nd ed). *O'Reilly*.

Cyberspace Solarium Commission. (2020, March 11). March 2020 CSC Report. *Office of the Secretary of Homeland Security*. https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report/

Domingo, F. C. (2015). Cyber War Versus Cyber Realities: Cyber Conflict in the International System by Brandon Valeriano and Ryan C. Maness: New York, NY: Oxford University Press, 2015, 288 pages. ISBN: 9780190204792. *Journal of Information Technology & Politics*, 12(4), 399–401. https://doi.org/10.1080/19331681.2015.1101039

Gross, M, J. (2011, Mar 6). A Declaration of Cyber-War. *Vanity Fair*. https://www.vanityfair.com/news/2011/03/stuxnet-201104

Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience. (2023, March 24). https://www.congress.gov/event/117th-congress/house-event/LC65989/text

Kreuzer, M, P. (2021, July 8). Cyberspace is an Analogy, Not a Domain: Rethinking Domains and Layers of Warfare for the Information Age. *The Strategy Bridge*. https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age

Lindell, J. (2009, November 26). Clausewitz: War, Peace and Politics. *E-International Relations*. https://www.e-ir.info/2009/11/26/clausewitz-war-peace-and-politics/

Mazarr, M. (2018). Understanding Deterrence. *RAND Corporation*. https://doi.org/10.7249/PE295

National Institute of Standards and Technology. (2018). *DoD Cyber Strategy and Cyber Posture Review*. Department of Defense United States of America. https://dodcio.defense.gov/Portals/0/Documents/Library/CyberStrategyFactsheet2018.pdf

Rescher, N. (1998). Predicting the future: An introduction to the theory of forecasting. *State University of New York Press*.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Javaid, A. (2020, May 15). What was the Y2K bug and how it helped India's IT sector? *Jagran Josh*. https://www.jagranjosh.com/general-knowledge/y2k-bug-1589540224-1

Y2K bug. (n.d.). *National Geographic*. https://education.nationalgeographic.org/resource/Y2K-bug

Zetter, K. (2016, Mar 6). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *Wired*. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/