ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.3364437

INTERNATIONAL JOURNAL OF RESEARCH – GRANTHAALAYAH
A knowledge Repository

Science

CYBER POWER

Akinwale M. Oteniya [1], Matthew N. O. Sadiku [1], Sarhan M. Musa [1]
[1] Roy G. Perry College of Engineering Prairie View A&M University, Prairie View, TX 77446

Abstract

Cyber capabilities are becoming more and more important in modern warfare. Strategists and decision-makers increasingly regard cyberspace as an indispensable weapon to achieve national objectives that can supplement the need for land, sea, air and space power. The concept of cyber power has received much attention in the U.S and around the world. This paper provides a short introduction to cyber power.

Keywords: Cyber Power; Cyber Dominance; Cyber Capabilities; Cyber Threat; Cyber Self-Defense; Cyber Attack.

Cite This Article: Akinwale M. Oteniya, Matthew N. O. Sadiku, and Sarhan M. Musa. (2019). "CYBER POWER." *International Journal of Research - Granthaalayah*, 7(7), 340-342. https://doi.org/10.5281/zenodo.3364437.

1. Introduction

Cyberspace refers to the environment characterized by the use of computer networks, wireless networks, tactical data links, and any other networks (which use electromagnetic spectrum) through which information is shared. It is all about connectivity—globally interconnected networks. It is new and a volatile manmade environment which is subject to more rapid technological changes than other domains (land, sea, and air). As a domain, it should be treated no differently than the conventional warfighting domains [1]. Controlling cyberspace is crucial for effective operations across all strategic and operational domains. It is difficult if not impossible to wage a modern war without employing cyber capabilities.

Due to its physical infrastructure of networked computers, cables, and satellites, the geographic setting has no relevance to the political use of cyber power. Although no nation can exclusively dominate the cyber domain, nations worth noting are the U.S, China, Russia in that order, followed in distance by Iran, North Korea and other nations [2]. These countries spent Billions of dollars in cyber power and defense. This offensive capability directly translates to cyber power, which is now an essential component of modern warfare [3]. Cyber threat which could be defined as the ability to inflict damage, misinformation, unauthorized control and other dangerous actions on networks, systems and data communication. Typically, these are done through the use of networked computers. Cyberattack are threats such as computer viruses, DoS (Denial of Service)

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.3364437

attacks, Data compromise in form of breaches and malware attacks. Cyber self-defense means taking proactive measures to protect or countermeasure to react to an attack. This could also be a presumed attack against an offender that has already attacked. The U.S DoD is maintaining a deterrent posture to persuade potential aggressors that their objective in attacking will be denied and that any attack on U.S territory, people critical infrastructure (including cyberspace) or forces could result in an overwhelming response [4]. With the launching of USCYBERCOM which involves the US Navy, army, US Marine Corps and air force, this is largest cyber-defense organization in the world formed to respond to cyber threats.

2. Operation of Power

In the international arena, the concept of power is greatly contested and no definition is accepted by all. Power depends upon context, and it can mean different things to different people. Simply put, power is the ability individuals and objects have to act. It indicates differences in our abilities. It also can be regarded as the ability to make someone do something even if it is against their will. It is sometimes understood as a possession [5]. One's ability to control, be it on the sea, of air, or cyberspace, is always a measure of the power one possesses. Cyber or information power is hard to categorize. However, Barnett and Duvall distinguish four types of power [6]:

- Compulsory, epitomizing 'power as relations of interaction of direct control by one actor over another.' This involves the ability of A to get B to do what B otherwise would not have done.
- Institutional, considering 'the control actors exercise indirectly over others through diffuse relations of interaction.' In such a scenario, A does not exercise power directly over B, but A could be dominant.
- Structural, expressing 'the constitution of subjects' capacities in direct structural relation to one another.' It is 'the supreme exercise of power to prevent actors from arising within societies or structures.
- Productive, entailing the 'socially diffuse production of subjectivity in systems of meaning and signification.' It is concerned with the social processes and the systems of knowledge through which meaning is produced.

3. Applications of Cyber Power

The cyberspace serves as a potent conduit through which cyber power can be conveyed.

As a concept of military doctrine, cyber power has become a vital element of hostile action between nations. All forms of power are generally hard to measure, and cyber power is no exception. Cyber power drastically affects other domains from war to commerce [7]. Treating cyberspace as an essential war fighting domain enables the capabilities of each of the armed forces (Army, Navy, and Air Force) to be better trained and managed.

A nation's cyber power has three dimensions: (1) coordination of operational and policy aspects across governmental structures, (2) coherency of strategic policy through international alliances and legal frameworks, and (3) cooperation of non-state cyber actors [8]. The U.S. Cyber Command was established to protect and defend DoD (Department of Defense) networks against cyber attacks and to develop offensive cyber capabilities. With the establishment of the Cyber Command,

ISSN- 2350-0530(O), ISSN- 2394-3629(P)
DOI: 10.5281/zenodo.3364437

national security strategy can be effectively implemented and the United States can express national values and protect national interests [9].

A major concern is the ends for which cyber capabilities or cyber power may be used. Cyber power is not created simply to exist, but rather to support some critical strategic objectives. Cyber war can result as an exercise of cyber power between nations. With the advancement in technology and the era of connected systems, it is worth noting that a compromise in private or public sector has huge impact the on nation being attacked. Vulnerabilities include power, telecommunications, financial, education, health, government, censors bureau, electoral board, research, military, private industries, public utilities etc. all these and many more are vulnerable to attack and can be used weaken a nation into surrendering to do her attacker's bidding.

The United Nations prohibits nations from using force against another nations except for self-defense or actions sanctioned by the Security Council. NATO (North Atlantic Treaty Organization) has made substantial progress in defining what a cyber defense posture should be, addressing issues of what constitutes defense, response, and deterrence. Under the Obama administration, the U.S treated cybersecurity as an important security challenge [10].

4. Conclusion

Cyberspace is the newest domain for fighting war. The cyber domain allows the military to develop the cyber power needed in the event of a cyber war. Most powerful states cannot dominate this domain as they can dominate sea and air. Cyber power would entail conveying power in or through cyberspace. Its main goal is to command cyber capabilities.

References

[1] J. M. Elbaum, "Cyber power in the 21st century," *Master's Thesis*, Wright-Patterson Air Force Base, Ohio, December 2008.
[2] D. R. Coats, "Statement for the Record," *Worldwide Threat Assessment of The U.S intelligence Community*, January 2019.
[3] J. Chen and A. Dinerman, "On Cyber Dominance in Modern Warfare," *European Conference on Cyber Warfare and Security*, July 2016.
[4] D. H. Rumsfeld, "Quadrennial Defense Review Report" *Washington, D.C. Department of Defense*, February 2006, pp.25.
[5] T. Jordan, *Cyberpower: The Culture and Politics of Cyberspace and the Internet*. London, UK: Routledge, 1999.
[6] J. van Haaster, "Assessing cyber power," *8th International Conference on Cyber Conflict*, 2016.
[7] J. S. Nye, "Cyber power," *Harvard Kennedy School, Belfer Center for Science and International Affairs*, May 2010.
[8] A. Klimburg, "Mobilising cyber power," *Survival*, vol. 53, no. 1, 2011, pp. 41-60.
[9] M. D. Young, "National cyber doctrine: the missing link in the application of American cyber power," *Journal of National Security Law & Policy*, vol. 4, 2010, pp. 173-196.
[10] J. Hunker, "Cyber war and cyber power issues for NATO doctrine," NATO Defense College, *Research Paper No. 62*, November 2010.

*Corresponding author.
E-mail address: tennymatt@ gmail.com/ sadiku@ ieee.org/ smmusa@ pvamu.edu