Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume12, Issue 5, July 2021: 3231-3236

Research Article

A Critical Study On Major Issues And Implications Of Cyber Warfare

Dr. K. Sita Manikyam* Devi Varaprasad Romala**

Abstract

The digital age has given rise to a new type of threat: cyberwar. "Cyberwar" denotes the use or targeting of computers, the internet of things (IOTs), and network-based systems in the context of warfare. Since information technology and the internet have evolved to the point where they are major components of national power, state militaries have been developing cyber weapons for use in national security preparation. An alarming number of states are engaging in cyber espionage, reconnaissance, or cyber-attacks, or both. There is considerable debate over whether such campaigns can be called "wars." Due to a lack of detailed knowledge in cybersecurity, those who are already in the industry have a difficult time meeting the cyberwarfare challenge. Despite several cyberattacks, the world has failed to keep up with the evolving threats of modern warfare. This research paper aims to examine the legal context of cyber warfare, i.e., the legislation that applies to cyber warfare, as well as case studies of cyber warfare events from around the world. It also focuses on issues like the use of force and the challenge of electronic warfare governance. This paper concludes with observations and recommendations for the future of cyber warfare.

Keywords: Cyber Warfare, Deterrence, Cyber Warfare Law, Automated Weapons, Use of Force.

1. Introduction

Cyber-warfare is a new weapon in today's internet-centric world. To many, cyberwarfare represents the fifth battlespace—a new type of warfare that needs to be defined further (Salasin J 2001). It solicits the question of how far existing international laws can be extended to the cyber domain. Applying pre-existing legal rules, concepts, and terminology to new technology may present challenges. preparing for electronic warfare has been a key issue in many countries' development. Besides, non-state actors have also benefited from the interdependence of cyberspace, causing considerable damage (Sigholm J 2013). They show that maintaining order and security is getting more difficult with each passing day in Estonia and Georgia, and Georgia is further proof of that fact (Georgia - defense & national security.2014). Also, it is important to build new regulations and improve the legal system.

* Correspondence : Rdvprasad.lawrs@andhraunivesrity.edu.in , Dr BR Ambedkar College of Law, Andhra University, Andhra University South Campus, Andhra University, Visakhapatnam, Andhra Pradesh 530003

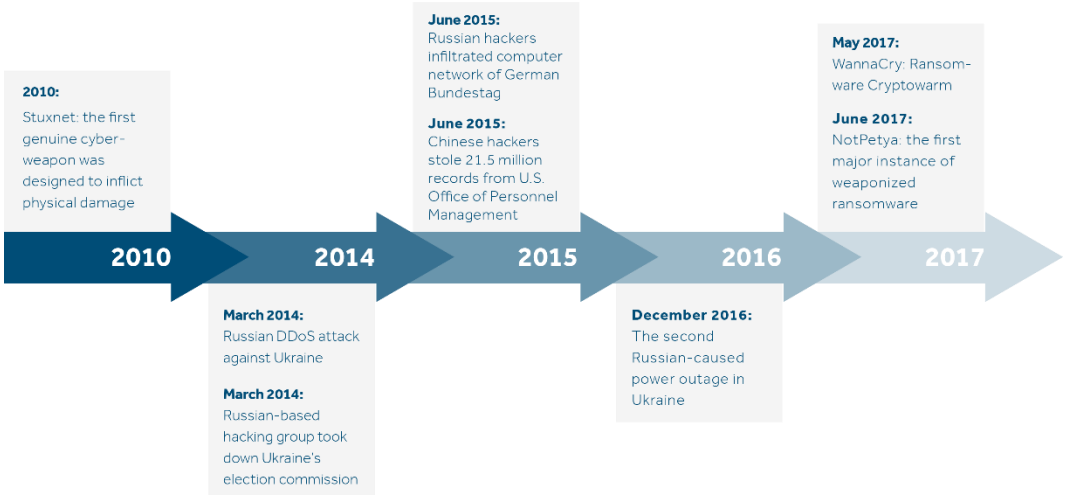
1.1 Virtual Battlefield

Lethal warfare has found its broadest application since the invention of the aeroplane (Pavelec S M 2017). It has broadened the scope of possible military action to include organizations that have traditionally not served as military defence contractors. A cyber warfare strategy is inexpensive for the aggressor but expensive for the defender. The number of countries involved in cyber-security projects increased to 114 in 2012, with 46 being "formal ready" and the rest on the way

(Rivera J 2017). More developed countries, led by the United States, have developed cyber warfare policies and strategies. The United States is critical to multilateral arms control and disarmament. Everything it does in cyberspace has the potential to have an impact on global armaments. Awareness in cyberspace is the foundation of good control. Some states are now employing a covert strategy in cyber warfare. This eliminates the need to follow rules of engagement.16 of the world's top 15 nations are developing military and cyber-offensive and defensive capabilities (Smeets M 2018). Cyber-attacks and cyber-warfare have become weapons of modern warfare.

2. A Short Glimpse of Cyber-warfare

More than 95 % of the US defence department machines released between 2012 and 2017 were found to have "mission-critical" type vulnerabilities, thereby making the United States progressively vulnerable to cyber-warfare attacks (Guide to Vulnerability Analysis for Computer Networks and Systems, 2018). The Following are a few examples.



2.1 Stuxnet (2010).

This was the first actual cyberweapon created with the intent of causing actual harm. It is estimated that it destroyed nearly one-fifth of Iran's nuclear centrifuges (Poroshyn R 2014).

2.2 2014, DDoS attack by Russia against Ukraine:

Russia for the second time has been accused of coordinating military and cyber activity in the Ukraine conflict. Russian-armed insurgents seized hold of Crimea just before a DDoS assault 32 times higher than that of the previous largest known attack on the internet (6. words of Warcraft: Manufacturing dissent in Russia and Ukraine. 2019).

2.3 2014, Russia vs. election commission of Ukrainian:

A Russian-based hacking group was able to compromise both Ukraine's backup system and the commission itself on the eve of the presidential elections in Ukraine. The attack on election night was an attempt to destabilize Ukraine and aid the pro-Russian campaign (Tatyana Ivzhenko. 2018).

2.4 2015, Russia vs. parliament of Germany:

The Federal Office of Information Security in Germany discovered that hackers had hacked into the Bundestag’s network Germany’s domestic intelligence service, later concluded that the attack

was done by Russia to investigate the operations of the Bundestag, NATO, and other German institutions (Usacheva M 2019).

2.5 2015, China vs. Personnel Management Office United States:

The accounts of 21.5 million federal personnel and applicants were stolen from the U.S. Office of Personnel Management. The perpetrator, according to US intelligence agencies, was the People's Republic of China (Cybersecurity resource centre Cybersecurity incidents 2021).

2.6 2016, power outage in Ukraine caused by Russia:

Russian hackers are thought to have deliberately put in a power provider's system for six months formerly shutting down the power supply. The power supply outage cost roughly one-fifth of the electricity consumption that night. This outbreak occurred a nearly single year after a cyber-attack in December 2015 that knocked out power supply to Two Lakh Twenty-Five Thousand people in western Ukraine (Kagarlitsky B (2019).

2.7 2017, The Famous WannaCry:

It is estimated that this attack affected over two lakh computers in more than 150 countries. WannaCry virus was a ransomware crypto worm that targeted Microsoft Windows computers. (One year after WannaCry Assessing the aftermath 2018).

2.8 2017, The latest Not Petya Ransomware:

This is the first time we've seen a weaponized ransomware event. The malware was designed to look like ransomware, but it was designed to damage files. While the attack began in Ukraine, it quickly spread around the world. The extent of the damage caused by this attack is still unknown, but it is estimated to be more than USD 10 billion. Cyberwarfare is increasingly targeting systems such as transportation, healthcare, utilities, and other critical industries (Harrison Dinniss, H. 2012).

3. Cyber War's Major Issues, Implications and Problems

Cyber-attacks are a form of conflict, but they also pose some challenges due to their inherent ambiguity. The majority of these involve the use of force. The issues stem from a variety of sources, including current laws governing cyber-attacks. The Issue of Governance of Cyber Warfare.

3.1 The Legal Frame Work For Cyber Attacks and Use of Force

Cyberwarfare is defined as a deliberate action that threatens, influences, disrupts, deceives, or damages computer systems and networks, as well as the data and/or messages that run through these systems. it is incorrect to label every negative event as a "war or cyberattack in cyberspace." War is the use of force to cause damage, destruction, or the governments or other organizations. A computer-based attack is likely to inflict harm or destruction. An act of war can be used for political gain or against national security. Force necessitates the use of physical or legal violence or the threat of legal violence. If there is no aggression, it is not an assault. If there is no danger of aggression, it is not the use of force.

What legal framework exists to govern cyber-attacks? Wars are regulated by international agreements such as the Geneva Conventions, Humanitarian Law, and customary practices (The Geneva conventions and enforcement of international Humanitarian Law 2019). The United Nations Charter, which was written to remove the word "war" from the vocabulary of states.

Article 2(4), of the United Nations Charter, requires countries to refrain from using armed force against another country's provincial integrity or radical independence (Attack on Iraq - SecCo debate - Verbatim record - question of Palestine, 1981). Because of the frequent references to provincial integrity and radical independence, it is understood that these rules apply to all uses of force, not just those that are "otherwise permitted by the Charter." The UN Charter provides two justifications for using force:

(a) force authorized by the UN Security Council, and
(b) when a state acts in self-defence.

Article 51 states that nothing in the Charter will “affect the inalienable right of individual or collective self-defence if an armed conflict occurs (Kucinich D 2020). ” Cyberwarfare is not expressly addressed in International Humanitarian Law, but it doesn't mean that the rules of international law do not apply to these. Self-defence necessitates the use of force. The application of UN Charter Article 51 would be invoked only in the event of a large-scale attack on infrastructure that resulted in significant physical or human losses. However, for many uses of force, an armed response is required. A nation can be attacked by cyber force, but it cannot respond with armed force because the magnitude of the force used does not correspond to an armed attack. As a result, there is an urgent need to resolve the right to self-defence, as well as rules of engagement regarding the use of private networks for disruption.
As a general rule, if it is not prohibited, it is permissible. The International humanitarian law does not explicitly address particular methods; however, the principles of international humanitarian law can be used to limit them. As a state initiates a belligerent action, the use of force is governed by the fundamental rules of the Hague and Geneva. These principles can be upheld in cyberwar because of military need, distinction, proportionality, perfidy, and unnecessary misery.

3.2 The Problem of Governance.

In several nations, both the procedures for launching a cyber-attack and for detecting it are still not up to date. It has only recently been accepted as a legislative choice for policymakers, and there are few precedents to be identified (Shackelford S. J 2020). By their very existence, equipment and services required for such operations are less evident than military, security, or law enforcement. As a result, they are unable to be categorized. The weapons' initial purpose is to incapacitate or injure rather than damage. Their occupations are so many and varied that they do not confine themselves to simple surveillance or clandestine operation. Furthermore, guns are further protected by confidentiality. A cyberattack capability can be acquired for a relatively limited amount of money as opposed to a traditional weapons program. The perceived value of cyber-attacks by decision-makers is usually going unrecognized. For the most part, a protocol for notifying both the executive and legislative branches seems to be nominal or non-existent. Around the same time, neither the government nor the general public had devised a plan for dealing with cyber threats. Again, a critical component of the system is Parliament's absence from the decision-making process on cyber-attacks (Calder A 2020). As a result, there is a governance problem that must be addressed.

4. Conclusion and Way Forward.

Because of ICT's significant impact on contemporary society, cyber-attacks pose a new degree of danger to national and economic security. Data generation, storage, processing, and transmission

capacities are all growing, and cloud computing is boosting personal computers and infrastructure and resulted in an unresolved problem in both the public and private sectors.

Many cyber activities, for the most part, do not meet the standards of "use of force or act of war as commonly defined by international law." By adhering to their formality, the noble class minimized ambiguity and applied to everything that could be calculated in terms of value. One of the key arguments is the threat faced by access to electronic weapons in several conflicts, ranging from simplistic one-on-one conflicts to wars between small parties to major world powers capable adversaries capable of deploying mass destruction in cyberspace.

The use of cyber threat capabilities by national policymakers expands the range of options available to national and other nations. Unintentional or unwanted effects of their use will occur from time to time.

Countries that depend heavily on ubiquitous ICT for both military and civilian functions are therefore highly vulnerable to global disruption. The number of Internet infrastructure targets is increasing rather than decreasing. Since an offensive and defensive approach to information security is necessary, there is potential to study and apply arms safety concepts in this area (including options for confidence and security-building measures). The goal would be to make certain
Furthermore, humanitarian law applies in the cybersphere.

Despite the questions surrounding the military use of cyberwar, it is unlikely the battle will be waged only in the cyber realm. Cyber capabilities would probably play a significant role in a future conflict between nations. Continue with the specific strategy is advantageous in the short term but risky in the long term.

A number of the known questions, ambiguities, and challenges will remain unsolved before further research and development in the area of cyberwar yields results. In the meantime, war games, simulations, simulations, and defensive drills, maybe, might provide useful information about cybersecurity There may be a collaboration with partners to better explain questions, and make it less difficult for adversaries to misinterpret one another.

References

1. Salasin, J. (2001). Architectures for network-centric warfare. *Battlespace Digitization and Network-Centric Warfare*. doi:10.1117/12.438303.
2. Sigholm, J. (2013). Non-state actors in cyberspace operations. *Journal of Military Studies, 4*(1), 1-37. doi:10.1515/jms-2016-0184.
3. Georgia - defense & national security.(2014). (n.d.). *Foreign Law Guide*. doi:10.1163/2213-2996_flg_com_079032h.
4. Pavelec, S. M. (2017). The future of war and warfare. *War and Warfare since 1945,* 152-157. doi:10.4324/9781315175478-9
5. Rivera, J. (2017). Cyber security via formal methods: A framework for implementing formal methods. *2017 International Conference on Cyber Conflict (CyCon U.S.)*. doi:10.1109/cyconus.2017.8167500

6. Smeets, M. (2018). Integrating offensive cyber capabilities: Meaning, dilemmas, and assessment. *Defence Studies, 18*(4), 395-410. doi:10.1080/14702436.2018.1508349
7. Guide to Vulnerability Analysis for Computer Networks and Systems: An Artificial Intelligence Approach. (2018). Germany: Springer International Publishing.
8. Poroshyn, R. (2014). Stuxnet: The true story of hunt and evolution. United States.
9. 6. words of Warcraft: Manufacturing dissent in Russia and Ukraine. (2019). *Plots against Russia*, 202-236. doi:10.7591/9781501716362-009.
10. Tatyana Ivzhenko. (2018). UKRAINE demands Russia be punished for HOLDING election IN CRIMEA. *Current Digest of the Russian Press, The, 70*(012), 15-15. doi:10.21557/dsp.50922183.
11. Usacheva, M. (2019). The NATO Information Office activities in Russia in the context of realpolitik. *Threats to Euro-Atlantic Security*, 85-95. doi:10.1007/978-3-030-19730-8_6
12. Cybersecurity resource center Cybersecurity incidents. (n.d.). Retrieved March 24, 2021, from https://www.opm.gov/cybersecurity/cybersecurity-incidents/
13. Kagarlitsky, B. (2019). Ukraine and Russia: Two states, one crisis. *Russia, Ukraine and Contemporary Imperialism*, 25-45. doi:10.4324/9781315205625-2
14. One year AFTER WANNACRY: Assessing the aftermath. (2018). *Network Security, 2018*(5), 1-2. doi:10.1016/s1353-4858(18)30037-0
15. Harrison Dinniss, H. (2012). Targeting and precautions in attack. *Cyberwarfare and the Laws of War*, 179-219. doi:10.1017/cbo9780511894527.008
16. The Geneva conventions and enforcement of international Humanitarian Law. (2019). *Revisiting the Geneva Conventions: 1949-2019*, 300-326. doi:10.1163/9789004375543_013
17. Attack on Iraq - SecCo debate - Verbatim record - question of Palestine. (1981). Retrieved March 24, 2021, from https://www.un.org/unispal/document/auto-insert-177595/
18. Kucinich, D. (2020). Privileged Resolution: Intent to Offer: Representative Kucinich Announced His Intention to Offer a Privileged Resolution. Czechia: Good Press.
19. Shackelford, S. J. (2020). *Governing new frontiers in the information age: Toward cyber peace*. Cambridge, United Kingdom: Cambridge University Press.
20. CALDER, A. (2020). The Cyber Security Handbook: Prepare for, respond to and recover from cyber attacks with the IT Governance Cyber Resilience Framework (CRF). Ely, Cambridgeshire, United Kingdom: IT Governance Publishing. doi:10.2307/j.ctv19shhms