South Asian Studies
A Research Journal of South Asian Studies
Vol. 38, No. 1, January – June, 2023, pp. 113 – 128

Cyber-Nuclear Weapons: Impact on the Modern Warfare Landscape

Shabana Fayyaz
Chairperson & Associate Professor, Defence and Strategic Studies Department
Quaid-i-Azam University, Islamabad, Pakistan.
Email: sfayyaz@qau.edu.pk

Baqir Malik
Assistant Professor, School of Politics and International Relations (SPIR), Quaid-i-Azam University, Islamabad, Pakistan.
Email: mbaqirmalik@gmail.com

Received: April 27, 2023

Published: June 23, 2023

ABSTRACT

The popular trends of information technologies have created a virtual world around the globe with the domain of cyberspace, which offers plenty of opportunities and challenges. In the last few years, several events have been described in terms of cyber warfare or the use of cyber weapons, leading to critical international security concerns. At the same time, there is little research on the definitions and power of what constitutes a cyber weapon and how it can be profiled. In the age of globalization and with the dynamic digital environment a new way of strategy and thinking is developing to introduce the new weapons, which has challenged the strategic environment around the globe and changing the concept of warfare in 21st century. The present article is to develop a preliminary hypothesis for to identifying the power of cyber weapon and how it relates with the nuclear weapon to examining the changing landscape of modern warfare. The comparative analysis of cyber weapons and nuclear weapons will help to understand the exact nature of cyber weapons with comparison of nuclear weapons to conclude which one is more preferable and dangerous in modern warfare techniques. The paper is divided into three sections. First part is brief introduction of genesis of cyber weapons, nature, evolution and its different types. The second part is comparison of cyber weapons to the nuclear weapons based on diverse characteristics (developing of weapons, security, arsenal, uses, target etc.). The third part is an analysis cyber weapon vis-a-vis nuclear weapon on the impact level. The paper conclude that the development of cyber-nuclear weapons has significantly altered the nature of contemporary warfare techniques. As technology continues to advance, the use of a cyber weapons has becomes increasingly likely, which could result in devastating consequences. It is important for nations to develop effective cybersecurity measures and maintain a strong nuclear deterrence strategy to prevent such scenarios from occurring.

Key Words: **Digital weapons, computer worms, High level languages, Feeding Material, SCADA, Nuclear Weapons.**

Introduction

The human mind is restless, and the progress in science is attributable to this trait. As part of this nature, humans have the need and struggle to fit in the universe by exploring the new opportunities to suit their needs in-universe. Cyberspace is one of these products that uses a platform for the life in the 21st century, resulting the interaction between technology and people for different services (Ryan, 2013). Five decades ago, no one can imagine that the cyberspace will bring revolution in our life. In 1969, the Department of Defense and Advance Research Project Agency established an experimental network for military purpose and then civilian use; within a few years this network evolved into an extensive network which we call internet (Kent, 2012). More than 4.57 billion users are now active on the internet, using different technologies to connect with one another, and cyberspace is the domain of this communication (Digital Population Worldwide, 2022). They use it for many reasons such as monetary transactions, vast robotized processes, monitoring the critical infrastructures, communication, and many other applications. As technology advances and our lives become increasingly dependent on it, we find ourselves trying to deal with technical concerns and problems that are affecting our society and our lives. Thomas Edison invented the lightbulb and it easy to see (visualize), hold it in your hand, and examine it from angle and what do you want. But the internet is unexamined entity and it is opposite, found everywhere but only we can see it in glimpses and that's why it is called the holy ghost (Piesing, 2014).

In terms of power and law, the domain of cyberspace is undefined at the international level. We can easily judge and quantify the power of conventional means and weapons such as biological, chemical, and nuclear weapons, but there is no international mechanism exist that could help to measures the cyber power index. That being said, policymakers face a difficult task when they are dealing with cyberspace and the utilization of cyber weapons. Today, no one can claim to be perfectly safe and secured from intruders (hackers or from cyber weapons) (Oakley, 2020). The term weapons are usually referring to the instruments of harms, which may be used to threaten or the reason for physical, or mental harm to the structure, system, or living things (Metzl, 2019). Cyber weapons are not exceptional from this universal concept. Various security experts, analysts, and technological professionals have discussed cyber weapons, and majority of them relate them with cyberwar, although there is no uniform definition exists for cyber weapons (Steele, 2000). There is a challenge settling upon a comprehensive, exact, and accurate definition of cyber weapons. The dual nature of cyber technologies makes defining cyber weapons more difficult. Based on the available literature, cyber weapons can be defined through two lenses that is, narrow, and a broad one. A narrow definition, a computer code that works with an information technology system aims to disrupt the system is known as a cyber-weapon. More considerably the cyber weapons are the combination of computer code and network technology

that manipulate, deny, degrade, destroy, and disrupt information and network system (Tom Uren, 2018).

The term "cyber weapons" was coined in the United States, and it is now widely used by policymakers and practitioners. The US Cyber Command team were tasked against specific adversaries including North Korea, Iran, and China to gain control of their digital network and the cyber weapons are the result of their research work in collaboration with the intelligence community (Halpern, 2019). The former Director of National Intelligence James Clapper, define cyber weapons; "a computer code that exploitable domain used by adversaries to conduct espionage, theft, extortion, and other criminal activities" (Clapper, 2016). United States security strategies have traditionally highlighted WMD threats from state actors and also acknowledge the danger associated with cyber weapons is real and credible (Trump, 2017). The Trump administration's 2017 National Security Strategy noted: "cyberattacks can harm large numbers of people and institutions" (Trump, 2017). The 2015 National Military Strategy specifically calls out particular concern with the proliferation of "cyber capabilities," referencing this concern in the same sentence as WMD (National Security Strategy, 2015). The 2014 Quadrennial Defense Review states the Department of Defense, "must be able to defend the Nation from an imminent, destructive cyberattack through cyber weapons on vital US interests" (Dale, 2014).

The military activities in cyberspace have increased during the last two decades, transforming it into a new strategic domain (Lessig, The Zone of Cyber Space, 1996). Current cyber politics around the globe indicates that all future conflicts directly or indirectly have cyber dimensions. Computer viruses, often known as cyber weapon, have become the most lethal weapon in the age of cyber technology .[1] As in the conventional power the nuclear weapons were used to measure the power similarly in the technological war the cyber weapons are at the center of this power. The development of cyber weapons is regarded as the birth of new strategic weapons in the twenty-first century in technological war. The strategic potential of cyberspace is dependent on the use of cyber weapons. The nature, consequence, and impact of cyber weapons are all extremely similar to those of nuclear weapons. However, the development and deployment of these weapons are more adaptable than nuclear weapons. The threat of cyber weapons is a well-accepted reality for practically all countries throughout the world.

In the lieu of the overleaf discussion, this research study explores the critical question regarding the capability and capacity of cyber weapons through a comparison of nuclear weapons. The paper is divided into three sections. The first part of the paper deals with the genesis of the cyber weapons: nature, evolution

[1] Business insider included 19 top dangerous weapons in 21st century and Stuxnet placed on 5th placed. According to experts the Stuxnet is the game changer of modern warefare and it was first reported state sponsored computer virus (cyberweapons). Retrieved from https://www.businessinsider.com/21st-century-game-changing-weapons-2015-5#iron-dome-111112

into various kinds. In the part two, comparison of the cyber weapons to the nuclear weapons based on diverse documented sources is discussed. The third part of the research study deals with the impact analysis of the nuclear weapons and cyber weapons on the enfolding nature of warfare. Finally, concluding part reflects the observations distilled from all the three parts of this scholarly analysis.

Part One: Genesis of the Cyber Weapons: Nature, Evolution and its various Kinds

We have witnessed the strength of nuclear weapons, especially after the use of nuclear weapons against Japan, and everyone is aware of the power of nuclear weapons. However, there is some skepticism about the effectiveness of cyber weapons. This section will emphasize the potency of cyber weapons. Is it possible to weaponize software and deploy it as a strategic weapon? To explore the answer to this question, we divide the debate into two different perspectives that help us to understand the potential of weaponized software. The first is the working mechanism and impact of cyber weapons, and the second compares the capability of cyber weapons with conventional weapons with three characteristics of both weapons that is offensive, defensive, and hybrid.

The invention of the computer virus in the mid-1980 changed the concept of using computer technology in various fields.[2] Although the first computer self-replicating virus, known as the 'Creeper System' was introduced in 1971, it was exclusively for research purpose. The 'Brain' was the first MS-DOS computer virus invented in 1986, while the 'Morris' virus was the first to spread extensively in 1988.[3]

These developments in the computer industry provided the technology a strategic dimension and created a new challenge for both state and non-state actors. In the early period of computer technology, the development of computer viruses was seen as a professional activity with many institutes regularly hosting tutorial classes on computer viruses (Stallings, 2012). It was considered a very tough and challenging task in the early '1990s, but the technology advancement and the availability of the internet have made it very easy.[4] According to AV-Test Institute, every day over 350000 malicious programs and unwanted applications

[2] Computer languages mean the codes which can computer easily understand. The binary language which consists of 0's and 1's is called the computer languages. It is also called the low level languages. It is very difficult to understand and then to write the script. It needs high professional skills and technical knowledge. as the technology developed these languages become very easy and in 1960 high level languages was introduced in computer industries. The high level languages consist of English languages and these are very easy to understand and to write the code. C, C++, FORTRAN, Java, Visual Basic, COBOL, Algol are some of these languages.

[3] The Creeper system virus was created by BBN Technology in the United States. The Brain virus was over rewrite the boot sector of floppy disk and prevent the computer from booting. The Morris was developed in Cornell University by Morris who wanted to know the size of internet. It Infected 15000 computer in 15 hours. For more details see, The A short history of computer Virus, Sentrian, https://www.sentrian.com.au/blog/a-short-history-of-computer-viruses

Fulghum, D. A. (2006). Redefining victory. Aviation Week and Space Technology, 1(26), 64

are examined. These are examined and classifies according to their groups, uses, activities, and characteristics.[5]

Cyber weapons are very powerful in term of their operational capabilities and network penetration speed. Stuxnet, Duqu, Flame virus, WannaCry, and NotPetya are some examples of these attacks, which spread rapidly over the globe (Baram, 2018). This is the reason cyber weapons are being developed, with the goal of making them more destructive and lethal than today. There are two main reasons behind this (Zeltser, 2004). First, cyber weapons are portable, and there is no need to launch from a base or need special arrangements to use them. Portable devices such as USB, CD, and Smart Disk are the main source to spread of these weapons. These devices are available at a very low price and accessible to the general public. Second, the internet makes it simple for users to download hacking tools easily.[6] Ray Kramer, Director of the National Institute of Standards and Technology (NIST) said, "One popular site has over 400,000 unique visitors per month downloading attacks and estimate that at least 30 computer attack tools per month are written and published on the internet" (Starr, 2009). These weapons can be new arms conflicting issues in global politics (Meyer, 2012).

The capability of traditional weapons can be classified into three broad categories: offensive, defensive, and hybrid. High-level programming is the primary source for developing cyber weapons (Mell, 1999). Although it is difficult to categorize cyber weapons into different forms, they are classified as offensive, defensive, or hybrid based on their functionality and penetrating speed. Offensive cyber weapons are used to harm the national critical infrastructures. These weapons, sometimes known as first strike weapons, represent the aggressive behavior of the users. The basic strategy of the use of offensive weapons is to breach the computer system and damage the state's important infrastructure via computer networks. For example, the WannaCry ransomware which is included in this category hit over 300,000 computers in 150 countries in May 2017 (Baram, 2018). The data-mining virus flame, ransomware duqu, and a computer worm dubbed Stuxnet all are included in offensive cyber weapons. Estonia was the first state who faced an offensive cyber weapons attack in 2007.

Defensive cyber weapons are commonly referred to as pro-reactive weapons. The purpose of using these weapons is to detection, prevention, and respond to any attacks. Encryption, firewalls, anti-viral software, and intrusion detection systems are further example of defensive cyber weapons (Denning, 2000). Hybrid weapons have both offensive and defensive capabilities. These weapons are used to protect the system as well as to target the infrastructures of enemies. There are few computer program (software) that can helpful to protect and strike back such as war dialers scanners, password crackers, key crackers, sniffers, and network

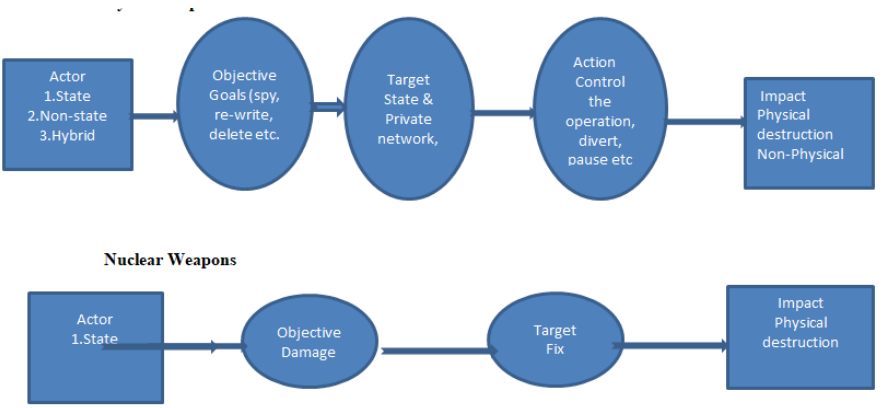
[5] Malware, AV-Test, see detail, https://www.av-test.org/en/statistics/malware/

[6] Typing "hacking tools" in Internet search engine yielded 42,012 hits in March 2006 and 1, 64,669 in Feb, 2014. NIST also examined 237 attack tools and found that 20% could remotely penetrate network elements and that 5% were effective against routers and firewalls.

administration, and monitoring tools. A brief introduction of these software is given her. The war dialers and vulnerability scanners can use with three different steps, (1), to find weaknesses in the system, (2), set targets for an attack, (3), trace the exact path for data transmission. Password crackers are considered a double edge of the sword. It is not only used to recover the passwords but also to trace the passwords of other networks[7]. Sniffers use to watch for possible intrusions.[8] A simple systematic working mechanism of both weapons are shown in following figure.

Explanatory Framework: Cyber Weapons & Nuclear Weapons

Cyber Weapons



Source: Authors Illustration.

Weapons

To compare cyber weapons to nuclear weapons, this section describes the nature of cyber weapons and nuclear weapons based on their defensive and offensive capabilities in various warfare scenario. Eight major differences between the two that is, Cyber weapons and Nuclear weapons are noted. These are the authority to the use of weapon, mechanism to prevent weapon, defense layer, stability-instability paradox, tangible and intangible condition, the situation of utilizations, capabilities, proliferation, and deployments. Also, some similarities of both weapons are discussed in detail (Ronefeldt, 2001).

[7] "WCCO News. (2000, February 17). Two Face Felony Charges in Software Thef.

[8] It also harvests usernames and passwords for subsequent exploitation. Network administration and monitoring tools can be used to administer one's own network or to take over a victim's computer and steal sensitive information from it. In some cases, it might be possible to distinguish dual-use weapons that are used mainly for defense from those that are also used to facilitate an attack. For example, a password sniffer designed solely to steal user names and passwords has no role in defense, where as a sniffer that is used for intrusion detection does. In that case, the password sniffer could be treated as an offensive weapon.

Comparing the differences between the two weapons, the first is the authority to launch weapons, the nuclear attacks need unique equipment and special orders, which are always in hierarchical order, to launch the nuclear bombs. In the United States, for example, the launch of a nuclear facility is dependent on the President's order to deploy nuclear weapons, which must be verified by the Secretary of Defense (Ford, 1985). This is known as the two-man rule or nuclear football. The sole power to employ nuclear weapons is that of the state, and the goal of launching a nuclear bomb is to produce huge physical destruction. In contrast to cyber weapons, it does not require any special arrangements to employ and can be used by both state and non-state actors. Its purposes are to disrupt the critical infrastructures and damage or steal data. There is no direct chance of physical damage from cyber weapons, as it occurs with nuclear weapons, yet they create more fear than nuclear weapons (Kemp, 2012).

Second, mechanisms to prevent weapon, once nuclear weapons are launched there is no mechanism to stop it. However, cyber weapons can be easily stopped at any stage and can easily hide for a specific period of time for further functioning. Furthermore, the antimissile system as a defense layer can be used to prevent and protect from nuclear attack. However, there is no mechanism exists against cyber weaponry. It is due to the flexible nature of the internet and its processing speed which cannot be measured by its intensity of penetration into the system and clueless nature. The anti-virus systems are maybe the one step to provide the defense layers, but it is not a perfect security system because anti-virus not functioning all time.

Third, the stability-instability paradox. The stability-instability paradox is an effective bridge to propose an idea to settle the conflict between two nuclear powers, because it is based on the deterrence theories and a valid framework for conflict in the modern world between two nuclear powers. The cyber weapon, unlike nuclear weapons, can generate its own version of stability- instability paradox[9]. The stability-instability paradox is very important for assessing offensive-defensive capability. This is easy to measure in terms of nuclear weapons, but it is almost impossible to measures in term of cyber weapons capacity because power is undefined in cyber space.

Fourth, the nature of weapons, cyber weapons exist in the category of invisible weapons, whereas nuclear weapons are visible weapons. This feature of the cyber weapons makes it bit superior over the nuclear weapons. To quote Sun

[9]Griffin, J. (2012). A cyber weapon is a weapon of mass destruction. TMCnet.com. Retrieved from http://www.tmcnet.com/topics/articles/2012/05/29/292267-flame-cyber-weapon-mass-destruction.htm. Scholars like Barretta and Rauchhaus describe it as, both states must (1) be locked in nuclear stalemate, (2) be contesting a contiguous territory, and (3) they must have employable conventional forces against each other, these all factors are undefined in cyber weapons. While Kapur, define it as, "the inverse relationship between the probability of nuclear and conventional military conflict", the cyber weapons are less chance of direct military conflicts between states and the intensity of conflicts can not be measures

Tzu, the military strategist: " best weapon is one that is invisible to adversaries and produce more disaster but do not show their existence" (Greers, 2001).

Fifth, utilization mechanism of the weapons, cyber weapons are used on daily basis and are not dependent on any particular situation. It is because cyber weapons can be used as a spy agent, stealing data, low escalations, changing the code, erase and delete the data. While nuclear weapons are used in extreme conflicting situations, a state can never use these weapons in times of peace, and even in times of war, it is a very rare chance that a state decides to use nuclear weapons. For example, the first nuclear weapons were used in 1945, and no nuclear weapons have been used against any state since. The use of nuclear weapons can also have a negative impact on country's image. For example, during the cold war, there were many occasions when nuclear weapons could have been used, but both the Soviet Union and the United States avoided using them. Even in a high tense situation, they were not in a position to use these weapons. Compare it to with the cyber weapons, every second, every hour, every day, cyber weapons use to achieve the strategic goals. The dependency on information technology and popular trends of cyber technology makes it possible. The use of nuclear weapons means the act of war, but the use of cyber weapons is not called a demonstration of war.

Sixth, weapons and state capability, only a few states (almost nine) have nuclear weapons and the capability to use these them. There is no report or evidence that non-state actors have nuclear weapons, they are attempting but have not yet acquired them, as per official and non- officials reports. It is almost impossible for the non-state actor to make nuclear bomb because of the lengthy-time process, resources, and special arrangements for the making the nuclear bombs, this can only do the state. However, in the case of cyber weapons, both state and non-state actors are developing and employing the cyber weapons to the same capacity.

Seventh, proliferation, there is clear mechanism and system (global proliferation treaties) to stop the development of nuclear weapons. For example, after the Soviet Union and the United States tested their nuclear weapons and three more states (China, United Kingdom, and France) joined the nuclear club, action was taken to stop the growing nuclear club, and these nuclear states introduced the nuclear ban treaty. The developing of a nuclear weapon was declared as an illegal and offensive act. However, a ban on the cyber weapon is almost impossible. It is because there is no need for a proper laboratory for the development of cyber weapons, as there is for the nuclear weapons.

Eighth, deployment or distance factor, there is a distinction between the deployment of cyber weapons and nuclear weapons. There is no need to deploy cyber weapons across the world to gain strategic advantages, as there is with nuclear weapons. Because cyber weapons may be launched from anywhere and the target is only one click away, distance is not an issue. Hackers, for example, can penetrate any computer network system and produce numerous distractions to their

adversary nations. These attacks are in the form of digital surveillance, cybercrimes, and economic warfare to an assault on its adversary basic framework (Schneier, Cyberweapons vs. Nuclear Weapons, 2016). However, the distance matter for the nuclear weapons and this is the reason the nuclear weapons are deploy on different location for the strategic purposes. For example, throughout the Cold War, both superpowers deploy nuclear weapons in different places to gain strategic edges and cover the missile range in case of war. There is always a possibility that nuclear weapons can be smuggled or stolen from the deployment point and the state may not know. Keeping all these points the cyber weapons are reversed in nature as compared with nuclear weapons.

While expressing the impact of cyber weapons some security experts and technology professionals believe that many similarities exist between both weapons (Lindsay, 2019). Some of these: first both weapons are the product of modern technology which has changed the concept of power on their inventions and in use. Second, both are using vast military applications and operations. Third, both have changed the concept of war and how the nations can fight the war and win the maximum strategic objectives. Fourth, cyber weapons and nuclear weapons are creating great fear and anxiety. Fifth, as states are busy developing more offensive cyber weapons than defensive weapons and similar trends were seen during the period of development of nuclear weapons. It means both weapons have advantages of offensive over defensive measures. Sixth, both weapons can provide and become the source to maintain stability and sureness of state security. Seventh, both weapons cause massive physical destruction and harm. Although nuclear weapons provided a clear picture of physical destruction when employed against Japan, there is still doubt about the cyber weapons.

The negative consequences of utilizing cyber weapons cannot be set aside. Technology is involved in every sector, including power grids, traffic control, defense sectors, water, and gas supplies, and many more. In 2007, cyber weapons were used against Estonia, and within a few minutes governmental infrastructure collapsed. This was the first large-scale incident reported against the state. The speaker of Estonian parliament observed the criticality of the situation : " When I look at a nuclear explosion and the explosion that happened in our country, I see the same things, as with the nuclear radiations, the cyber weapons can destroy a modern state without drawing blood, the only difference is that Japanese know their enemy and we are blind" (McGuinness, 2017).

Thus, at this point one can note, there is a clear difference and similarities across weapons, ranging from speed to usage and defense to assaults. It is possible to defend against nuclear weapons by taking some security measures, but it is very difficult to stop or prevent digital strikes completely, the antivirus software is unable to provide 100% shield against the cyber-attack. However, the rate at which digital strike could be executed, there is some need for robotized strategies in digital defense which reacts immediately to protect from such assaults. The computerized response may be the best way to protect against a digital strike, but it

should also keep in mind that it is unclear how viable such reactions could be fruitful. Despite this debilitation, it does give the idea that in terms of the pace of assault, digital weapons require not to take a secondary lounge to their nuclear partners.

Part Three: Analysis of Cyber Weapons and Nuclear Weapons on the nature of warfare

The intensity and reliability of weapons can be measured by their working mechanism, which includes the development of operating systems. There are main differences that are critical to be registered while comparing the strength of both weapons- Cyber weapons and Nuclear weapons respectively. These deal with the placement, making weapon, operating, feeding material, striking power, and environment, target, and direction (Cirenza, 2018). First, placement, nuclear weapons required proper placement with a perfect security system to protect from unauthorized people, and only a few top officials can have access to the nuclear stockpile (Kristensen, 2006). However, cyber weapons are not subject to these restrictions, and it can store in a portable device and carried with these devices or through a virtual medium such as emails and messenger. Second, making weapons, nuclear weapons require a fully equipped laboratory as well as a lengthy process that required huge funds. While the cyber weapons can be built in a simple computer lab with fewer resources in a relatively short period of time, there is also no need for proper equipment as in the case of nuclear weapons. Third, operate to weapons. The operation of nuclear weapons is based on a very complicated system that required certain parameters and circumstances. Cyber weapons, on the other hand, do not require any complicated mechanism to function. Anyone with little knowledge can use them, and there is also a less official restriction on the use of digital weapons because cyberwar is happening every day, and cyber weapons are a tool of this conflict (Greers, 2001). Fourth, feeding material. There are different types of nuclear weapons, which are classified depending on their fuel/material such as uranium, platinum, or some other radioactive material. The impacts of these nuclear weapons are depending on their substance they are used during the bomb process. Similarly, there appears to be various types of digital weapons, and their feed material dependent on the code and language used to develop. These digital weapons appear and transform an extensive variety of impacts on their rival's network. For example, that of the Supervisory Control and Data Acquisitions (SCADA) frameworks that control a large portion of the robotized or automated system regulating key processes in various parts of the chemical and nuclear industries can be easily targeted with the digital weapon (Schneier, Beyond Fear: Thinking Sensibly About Security in an Uncertain World., 2009).

Fifth, striking power and environment. Cyber weapons are created using different computer languages scripts, and the programming/coding of these languages provides an impression into the capabilities and purpose of the cyber

weapons. The coding is divided into different small parts called packets, and these packets further used to set the targets. For example, some digital codes are used to disrupt the network traffic, others to steal sensitive information and data, yet others to destroy the overall plant cooling or other monitoring systems, and so on. This is why cyber weapons are also called mission slaughter weapons (Weimann, 2011). Nuclear weapons give a different impression as compare to cyber weapons. Almost all nuclear weapons serve the similar goal and that is only the destructions. The intensity or power of the striking capacity may be different, but the result remains the same and that is only to bring the only destruction. No monitoring or spy mechanism exist in the coding of nuclear weapons (Poulsen, 2011).

Sixth, target and changing nature. The target of nuclear weapons cannot be changed easily, and deactivations of these weapons are also almost difficult. However, cyber weapons can detect and may divert their target. There are some software and anti-virus system installed in the network which helps to deactivate the cyber weapons and to protect the critical infrastructures from the physical and digital attacks. But nothing can provide full surety to stop the cyber weapons. It is because the nature and status of the cyber weapons can change easily according to circumstances and nuclear weapons are lacking from these characteristics. Moreover, the cyber weapons are invisible that it not only changed their target but also can easily be modified, rewrite and the power of threat can increase or decrease within a limited period (Geers, 2010).

Seventh, direction and distance. The direction is important to set the target. This is the most important factor and calculated when the weapons are developed in the laboratory. The direction can help to attack the target. Once the direction is set to nuclear weapons it is very hard to change the direction when it launches from the operating base or missile. However, the cyber weapons can easily reverse, and their target situated is continually changing in ways that hazard rendering them ineffectual or out of date. This proves that cyber weapons disastrous decimation may depend to a critical degree on a moderately stable target build, or in light of the capability to screen nearly changes in the base. By comparing these, nuclear weapons appear to be generally immune to changes in the target base. To conclude, the strategic cyber weapons have some arsenals challenge of target base while the nuclear weapons look free from this challenge.

At this juncture question arises: which weapon that is cyber or nuclear is more dangerous and lethal?

It's challenging to directly compare cyber and nuclear weapons since they provide different kinds of risks, but both are deadly and dangerous in their own ways. Critical infrastructure, such as power grids, transportation networks, and banking networks, can be affected by cyber weapons, leading to general chaos and devastation. Cyber attacks can potentially steal valuable data, including commercial secrets, military plans, and personal information, with serious security

and economic repercussions. Yet, nuclear weapons have the capacity to unleash unfathomable levels of devastation, with devastating long-term impacts on human life, the environment, and international security. The use of nuclear weapons might trigger a nuclear winter, which would cause a worldwide hunger and mass death.

However, the contemporary debate about cyber weapons and nuclear weapons indicates that nuclear weapons are liable to be more dependable than cyber weapons. This clear difference could be demonstrated regarding an attacker's readiness for a digital strike whose intention is to cause cataclysmic annihilation. Aside from being more dependable, nuclear weapons exact harm that is more intense and far less reversible than that of a digital attack even one that catastrophic harm (Barnes, 2008). Despite the utilization of nuclear weapons, it produces an electromagnetic pulse covering a large territory. The nuclear attack makes far more collateral damage such as human causalities, leftover radiation, and physical annihilation than any other conventional and cyber weapons. In this respect, cyber weapons may offer a sizeable point of interest over nuclear weapons, in that the digital attack to undiscovered a significant part of the harm created by the strike, and to do so quickly. Moreover, cyber weapons produce fewer casualties and destruction as compared to nuclear assault.

The impacts of a nuclear attack have all being connected to a significant degree with the number of nuclear weapons used, their target, and the power of destruction that depends on the material used in the nuclear weapons. But it is very important to note that even a single nuclear weapon could produce unlimited dreadful destruction, such as using an electromagnetic pulse (EMP) assault. If an EMP attack is properly executed, it has the potential to cause widespread devastation. In this way, the impacts of cyber weapons look a less capacity of disastrous as the number of nuclear weapons utilized, particularly if EMP attacks are marked down. To some degree this is since a single cyber weapon, a worm might be fit for reproducing itself and contaminating countless. For example, the Slammer worm had performed different activities and brought countless impacts on the network. Similarly, the Stuxnet worm may have begun to penetrate through a thumb drive and then spread one computer to another very fast as a result it destroys the overall computer network system at the nuclear power plant in Iran (Mallet, 2010). In theory, cyber-attack can produce the same impact as the damage done with traditional, conventional, or nuclear weapons but practically it looks less harmful than nuclear weapons.

Throughout the Cold War period, the power of nuclear weapons and its uses were constantly debated between the Soviet Union and the United States. The debate revolved on stopping nuclear clubs and using nuclear weapons even in highly conflicting situations. However, in the case of nuclear weapons, such operations can be stopped because the attacker can be easily identified, and deterrence also works in this situation. Deterrence works in cyber-attack as well, but it is not much effective due to the hidden identities of attackers. Furthermore, once a cyber-attack has started, it is very difficult to stop because different actors

are involved, each with their own agenda. The non-state actors or patriot hackers are the major challenges to control them (Enabling Distributed Security in Cyberspace, 2011). Also, cyber weapons and tools are utilized routinely both in peace and wartime. This makes it quite difficult to figure out that the states crossed the limit between the act of war and digital peace go into non-belligerency, however, this thing is very clear with nuclear weapons. There could additionally be an issue in defusing digital weapons that had entered a closed network system. Moreover, it is also very difficult to defuse cyber weapons (Bunker, 2005).

Importantly, there are few assumptions underlying the legitimacy of cyber weapons (Cyber Weapons Vs Nuclear Weapons, 2022). These are: first, cyber weapons are not nearly as disastrous as the nuclear weapons bombs. For example, unlike the Atomic bombs that were dropped on Hiroshima and Nagasaki and world are the witness of their impact, digital weapons have not yet to demonstrate their ability to do extraordinary harm on a global scale. Second, digital weapons do not fit within conventional weaponry origins. Third, while the ruinous tendency of nuclear weapons could be seen, and quantified, digital weapons offer no natural casing of reference based on quantity and quality. Fourth, historically speaking, the strategic studies group informed the public about the existence of nuclear weapons in the 1940s and 1950s and educated them on the implications of these weapons, but there are no such moments in the world today that can give an idea about the presence of digital weapons. On a smaller scale, governments have been extremely cautious in disclosing information about their digital weapons or exercises.

In this age of globalization, conflicts are no longer simply fought with conventional weapons, but also with other sophisticated technologies. Today, no state can underestimate the strength of these weapons, and global cooperation is required to confront these threats and make the world a safer place. Today, it is not possible for the state to underestimate the power of these weapons and also needs global cooperation to counter these threats and make the world free from these weapons. No one can deny this reality that cyberspace now becomes the new conflicting zone in the world.

Conclusion

The preceding discussion examines both weapons in detail, from conception to execution. To conclude, the creation and employment of cyber weapons has grown in importance as a problem for global security. Nuclear and cyber weapons are fundamentally distinct from one another, yet there are some similarities in the potential harm they could cause and the necessity for global collaboration to limit their use. Nuclear weapons are more difficult to obtain than cyber weapons since they require more technological know-how and resources to produce and use. Because of this accessibility, it is simpler for non-state actors, including terrorist groups, to obtain and employ cyber weapons. It is difficult to hold those

responsible for cyberattacks accountable due to the ambiguity of attribution and the difficulties in identifying the attack's origin.

Cyber weapons can be used for espionage, sabotage, or other types of attacks, making them more flexible in their deployment than nuclear weapons. Although the use of cyber weapons has not yet reached the same degree of threat as nuclear weapons, the increasing sophistication of cyber actors and the growing dependence on technology in all spheres of life indicate that the impact of cyber strikes will only increase. The policymakers should focus on improving cybersecurity measures, increasing international cooperation and information sharing, and developing norms and regulations around the use of cyber weapons to prevent catastrophic consequences. The development of norms, rules, and cooperative mechanisms by the international community is therefore essential if we are to stop and lessen the use of cyber weapons in the future.

References

21st Century game changing weapons. (2015). Retrieved from Business Insider.

Baram, G. (2018, June 19). *Council on Foreign RThe Theft and Reuse of Advance Offensive Cyber Weapons Pose A Growing Threat*. Retrieved from Council on Foreign Relations: https://www.cfr.org/blog/theft-and-reuse-advanced-offensive-cyber-weapons-pose-growing-threat

Barnes, J. E. (2008, May 28). *Pentagon computer networks attacked*. Retrieved from Los Angles Times: http://articles.latimes.com/2008/nov/28/nation/na-cyberattack28

Bunker, R. J. (2005). *Networks, terrorism and global insurgency*. Psychology Press.

Cirenza, P. (2018). Retrieved from An Evaluation of the Analogy between Nuclear and Cyber Weapons, Stanford University,: https://stacks.stanford.edu/file/druid:sh530vk4641/An%20Evaluation%20of%20the%20Analogy%20Between%20Nuclear%20and%20Cyber%20Deterrence.pdf

Clapper, J. (2016, February 9). *dni.goverment*. Retrieved from https://www.dni.gov/files/documents/2016-02%2009SASC_open_threat_hearing_transcript.pdf.

Cyber Weapons Vs Nuclear Weapons. (2022). Retrieved from Centre fot Strategic and International Studies: http://csis.org/blog/cyber-weapons-vs-nuclear-weapons.

Dale, C. (2014). *The 2014 quadrennial defense review (QDR) and defense strategy: Issues for Congress.* Washington, DC: Congressional Research Service.

Denning, D. (2000). Reflections on Cyberweapons Control. *Computer Science Journal*, 43-53.

Digital Population Worldwide. (2022). Retrieved from https://www.statista.com/statistics/617136/digital-population-worldwide/

Enabling Distributed Security in Cyberspace. (2011, March 23). Retrieved from Department of Homeland Security: http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-whitepaper-03-23-2011.pdf.

Ford, D. F. (1985). *The Button: Pentagon's Strategic Command and Control System.* New York: Simon and Schuster.

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law and Security Review*, 26(3), 298.

Greers, K. (2001). *Strategic Cyber Security. Estonia: CCDCOE.* CCDCOE.

Halpern, S. (2019, July 18). *The New Yorker*. Retrieved June 15, 2022, from https://www.newyorker.com/tech/annals-of-technology/how-cyber-weapons-are-changing-the-

Kemp, R. S. (2012, June 7). *Cyber weapons: Bold steps in a digital darkness. Bulletin of the Atomic Scientists, (2012)*. Retrieved from http://www.thebulletin.org/web-edition/op-eds/cyberweapons-bold-steps-digital-darkness

Kent, F. E. (2012). *The Encyclopedia of Telecommunications.* New York: CRC Press.

Kristensen, H. M. (2006). *Kristensen, H. M. (2006, November 9). Where the Bombs are.* Federation of American Scientists.

Lessig, L. (1996). The Zone of Cyber Space. *Stanford Law Review*, 1403-1441.

Lessig, L. (1996). The Zone of Cyber Space. *Stanford Law Review*, 1403-1441.

Lindsay, J. R. (2019, June 20). *Cyber Operations and Nuclear Weapons*. Retrieved from Nautilus Institute of Security and Sustanability: https://nautilus.org/napsnet/napsnet-special-reports/cyber-operations-and-nuclear-weapons/

Mallet, P. (2010, October 1). *Stuxnet worm brings cyber warfare out of virtual world*. Retrieved from phys.org: https://phys.org/news/2010-10-stuxnet-worm-cyber-warfare-virtual.html

McGuinness, D. (2017, April 27). *How a cyber attack transformed Estonia*. Retrieved from BBC News: https://www.bbc.com/news/39655415

Mell, P. M. (1999). Understanding the World of Your Enemy with I-CAT (Internet-Categorization of Attacks Toolkit). *In Proceedings of the 22nd National Information Systems Security Conference* (pp. 432-443). NIST.

Metzl, J. M. (2019). What guns mean: the symbolic lives of firearms. *Palgrave Communications*, 1-5.

Meyer, P. (2012). Diplomatic Alternative to Cyber warfare: A Near Term Agenda. *RUSI Journal*, 57.

National Security Strategy. (2015, February 1). Retrieved from The White house archives: https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf; The Department of Defense released the unclassified summary of the 2018 National

Oakley, J. G. (2020). *Cybersecurity for Space: Protecting the Final Frontier.* Apress.

Piesing, M. (2014). *The Guardian* . Retrieved 2022, from https://www.theguardian.com/technology/2014/oct/07/god-internet-alexander-bard-syntheism-new-elite

Poulsen, K. (2011, September 27). *U.N. warns of nuclear cyber attack risk*. Retrieved from Security focus: http://www.securityfocus.com/news/9592.

Ronefeldt, J. A. (2001). *Arquilla, J., Networks and Net wars: The Future of Terror, Crime, and Militancy.* Santa Monica: RAND.

Ryan, J. (2013). *A History of the Internet and the Digital Future.* Reaktiion Books.

Schneier, B. (2009). *Beyond Fear: Thinking Sensibly About Security in an Uncertain World.* New York: Copernicus Books.

Schneier, B. (2016, July 22). *Cyberweapons vs. Nuclear Weapons*. Retrieved from Schneier.com: https://www.schneier.com/blog/archives/2016/07/cyber_weapons_v.html.

Stallings, W. (2012). *Computer Security: Principles and Practice.* Boston.

Starr, F. D. (2009). *Cyberpower and National Security.* Dulles: National Defense University Press and Potomac Books, Inc.

Steele, J. L. (2000). *The Gun Digest Book of Assault Weapons.* Krause Publications.

Tom Uren, B. H. (2018). *Australian Strategic Policy Institute*. Retrieved 2022, from Australian Strategic Policy Institute (ASPI)https://www.aspi.org.au/report/defining-offensive-cyber-capabilities

Trump, D. (2017, December 18). *The White House*. Retrieved from https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

Weimann, G. (2011). *Terror on the Internet: The New Arena, the New Challenges.* . United States Institute of Peace.

Zeltser, E. S. (2004). *Malware: Fighting Malicious Code.* Prentice Hall Professional.