Cyber Warfare

Prof. Kiran R. Borade[1], Prof. Monika R. Sindhikar[2], Prof. Tejal S. Sonawane[3], Prof. Gayatri R. Jagtap[4]

[1]Lecturer, Department of Computer Engineering, Guru Gobind Singh Polytechnic, Nashik, India

[2]Lecturer, Department of Computer Engineering, Guru Gobind Singh Polytechnic, Nashik, India

[3]Lecturer, Department of Computer Engineering, Guru Gobind Singh Polytechnic, Nashik, India

[4]HOD, Department of Computer Engineering, Guru Gobind Singh Polytechnic, Nashik, India

Abstract: Persistent disregard for the effects of Cyber Warfare will bring great concern to all. Hackers and governments alike should understand the barriers their ways take. Governments use Cyber Warfare to provide strategic advantage over other countries, to protect themselves from enemies or to harm their opponents. Hackers use Cyber Warfare to obtain personal information, commit crimes, or express sensitive and beneficial intelligence. While both approaches may offer ethical use, the same can be said for another wide range. Knowing and understanding these devices will not only strengthen the ability to detect and counteract these attacks but also provide the means to expose malicious government programs, as the effect of Cyber Warfare can be far worse than the aftermath of a normal war. This paper includes the concept of ethics and the reasons that led to the use of information technology in military warfare, the consequences of using cyber warfare on civilians, legitimacy of cyber warfare and ways to control the use of information technology that can be used in society. Detailed strategies and methods should be developed in this regard. Hence this paper recommends urging science and technology research institutes to improve security and develop security systems to prevent the use of technology in the civil war against civilians.

Keywords: *Cyber Defence, Cyber Security, Cyber Warfare, Future technologies, Cyberspace, Confidentiality.*

I. Introduction

The cyber war refers to the use of digital attacks, such as computer viruses and hacking, in one country to disrupt important computer systems in another, with the aim of causing injury, death and destruction. Upcoming battles will see hackers use computer code to attack enemy infrastructure, fighting alongside soldiers using conventional weapons such as guns and arrows [1][3]. A dignified world still full of spies, hijackers and high-level secret weapon projects, cyber war is the most common - and dangerous - cause of global conflicts. But now the ongoing integration of cyber wars with the lack of clear rules governing online conflicts means that there is a real risk that events could develop rapidly and out of control. There are many weaknesses in many networks that give countries the potential for cyber attacks which are built on basic network infrastructure and processes that control communication within them, and that can be used in service denial (DDOS) attacks, or attacks on critical infrastructure and government and military networks [1]. The purpose of the research paper is to examine the use of cyber wars as a weapon against an enemy that does not have the basic rules that govern the circumstances and determine the circumstances of the attack.

1.1. The goals of cyber warfare:

According to the Cyber security and Infrastructure Security Agency (CISA), the objective of those involved in cyber attacks is to "weaken, disrupt or destroy the US." To achieve their goals, “national cyber warfare programs are unique in creating a threat to all targets that could harm US interests,” CISA said [2]. These threats range from propaganda to hardship and serious disruption to the loss of life and disruption of infrastructure.

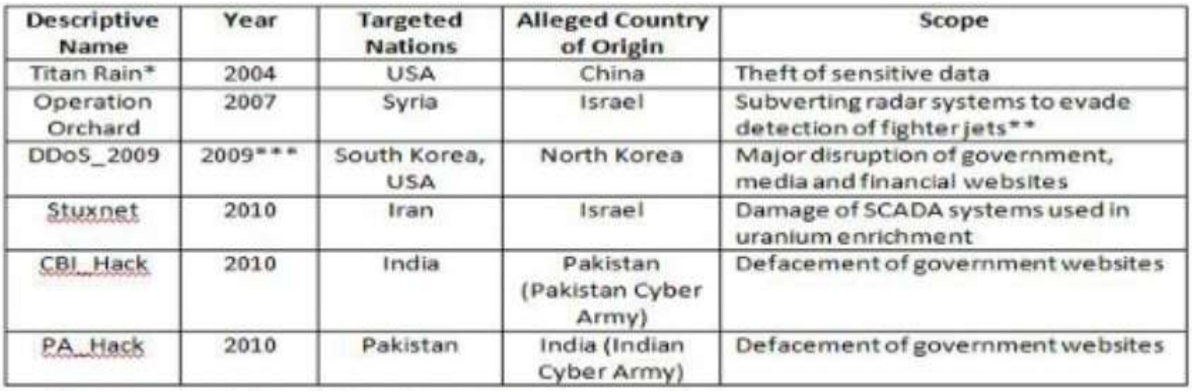
A few examples of threats include: Spyware of technological advances. For example, the National Counterintelligence and Security Center (NCSC) in its 2018 Foreign Economic Espionage report at Cyberspace reports that China's cyber security law mandates foreign companies to submit their technology to the Chinese government for review and that Russia increases its need for source code revision to accept foreign technology which is sold in their land. In 2018, the U.S. Department of Justice fined two Chinese hackers linked to the Department of Homeland Security for identifying intellectual property and confidential business information.

Infrastructure disruption attacks the US economy or, when attacked by the US, impairs the US’s ability to continue its attacks. For example [4], by controlling the route between data management and data acquisition (SCADA) sensors and controllers in sensitive infrastructure, such as the energy sector, the enemy may attempt to damage or damage the power plants or the grid itself.

Cyber attacks are used to sow discord in order to destabilize the government. For example, according to the Report on the Investigation into Russian Interference In the 2016 Presidential Election, written by Special Adviser Robert S. Mueller, III, Russia's Internet Research Agency used social media accounts with interested parties to provoke controversy in the US political system called the 'war of knowledge.'

1.2. Types of cyber warfare attacks:

More and more criminals are attacking governments using their critical infrastructure, including transportation systems, banking systems, power grids, water supply, dams, hospitals and the production of sensitive goods. The threat of cyber warfare attacks is mounting as the nation's sensitive systems become increasingly connected to the internet[5]. Although these systems may be secure, they can still be hacked by criminals hired by nations to gain power and exploit them. Attacks on APT infrastructure can damage the country. For example, an invasion of a national utility system could cause serious damage by causing widespread power outages, but a hydropower-powered invader might also think he could flood by opening dams. Cyber attacks on government computer systems can be used to fund normal military efforts. Such attacks may prevent government officials from communicating; allow attackers to steal private communications; or release personal and citizen personal data, such as Social Security numbers and tax information, to the public [6]. Government-sponsored or military-sponsored invaders may also enter military records of their enemies to obtain information about military bases, as well as what weapons and equipment they use. DoS attacks, which continue to increase worldwide, are expected to be used to combat cyber warfare. Attackers use attack service denial (DDoS) methods to attack government agencies with massive bandwidth attacks, and at the same time infect them with spyware and malware to steal or destroy data. These attacks can incorporate non-existent information into their networks of intentions to create chaos, exit or scandal. There have been a number of documented cases of cyber-attacks worldwide [19], some of which are likely to continue. These cases can be summarized as shown in Figure 1.1.

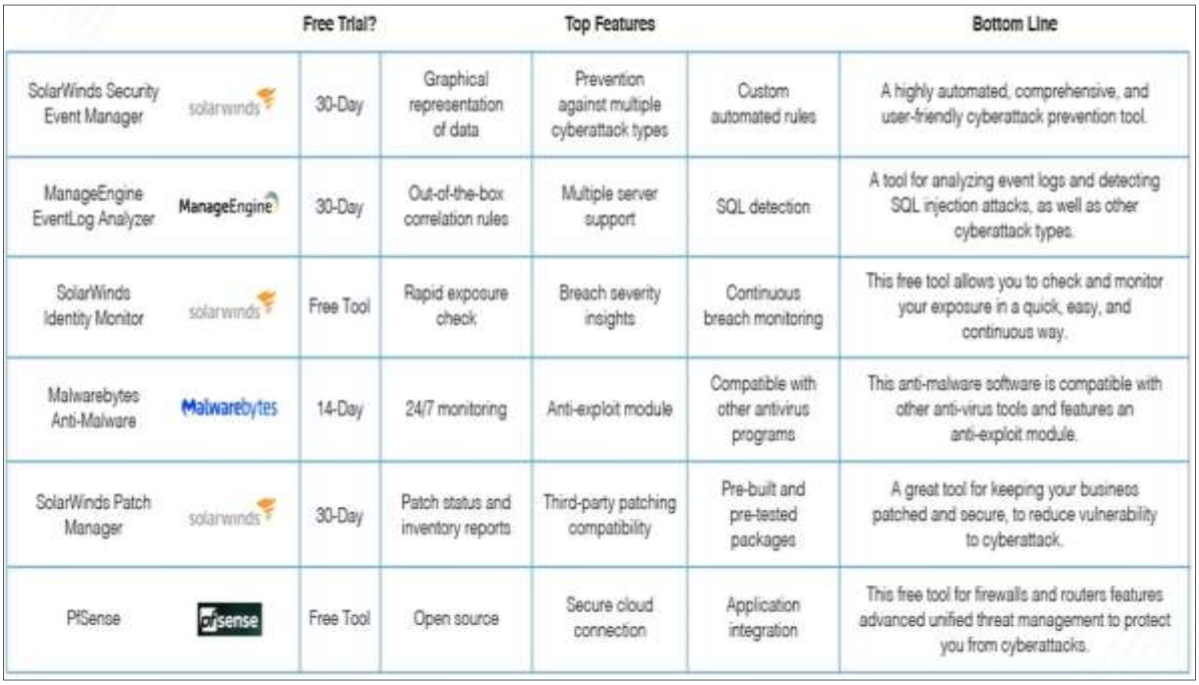


Descriptive Name	Year	Targeted Nations	Alleged Country of Origin	Scope
Titan Rain*	2004	USA	China	Theft of sensitive data
Operation Orchard	2007	Syria	Israel	Subverting radar systems to evade detection of fighter jets**
DDoS_2009	2009***	South Korea, USA	North Korea	Major disruption of government, media and financial websites
Stuxnet	2010	Iran	Israel	Damage of SCADA systems used in uranium enrichment
CBI_Hack	2010	India	Pakistan (Pakistan Cyber Army)	Defacement of government websites
PA_Hack	2010	Pakistan	India (Indian Cyber Army)	Defacement of government websites

Figure 1.1. Some of the nation specific ware fare [19]

1.3. Cyber Security Tools:

There are many useful tools as shown in Figure 1.2 that can be used to protect data and user privacy. Solar Winds SEM is a great tool for detecting SQL injection attacks and vigorously protecting your data server from them. It involves the integration manager to identify suspicious activity, notify you, and respond to potential auto-attacks, in accordance with the pre-set event rules [18]. By using a list of pre-populated vectors that are more commonly found in SQL injection attacks, laws can effectively and quickly detect and prevent these attacks.



		Free Trial?	Top Features			Bottom Line
SolarWinds Security Event Manager	solarwinds	30-Day	Graphical representation of data	Prevention against multiple cyberattack types	Custom automated rules	A highly automated, comprehensive, and user-friendly cyberattack prevention tool.
ManageEngine EventLog Analyzer	ManageEngine	30-Day	Out-of-the-box correlation rules	Multiple server support	SQL detection	A tool for analyzing event logs and detecting SQL injection attacks, as well as other cyberattack types.
SolarWinds Identity Monitor	solarwinds	Free Tool	Rapid exposure check	Breach severity insights	Continuous breach monitoring	This free tool allows you to check and monitor your exposure in a quick, easy, and continuous way.
Malwarebytes Anti-Malware	Malwarebytes	14-Day	24/7 monitoring	Anti-exploit module	Compatible with other antivirus programs	This anti-malware software is compatible with other anti-virus tools and features an anti-exploit module.
SolarWinds Patch Manager	solarwinds	30-Day	Patch status and inventory reports	Third-party patching compatibility	Pre-built and pre-tested packages	A great tool for keeping your business patched and secure, to reduce vulnerability to cyberattack.
PfSense	pfsense	Free Tool	Open source	Secure cloud connection	Application integration	This free tool for firewalls and routers features advanced unified threat management to protect you from cyberattacks.

Figure1.1. Six tools to prevent cyber attacks [18].

The cyber war uses Internet networks to carry out politically motivated attacks on information resources and programs aimed at defending, exploiting, corrupting, denying or disguising themselves in order to gain the enemy's advantage. There are a number of vulnerabilities among critical infrastructure in the international network in various sectors that can be exploited in cyber attacks. These days most countries are looking to apply information technology to all sectors of society. In addition, this could have a negative impact if the technology is not protected by security experts [18][19]. Cyber attacks rely on computer resources and networks that are more vulnerable but more expensive than launching a regular attack. On the other hand, military cyber attacks protect the lives of soldiers from direct attacks. Cyber attacks can be an excellent tool that can be considered a weapon because of its huge impact on targeted information services. There is no direct impact on the military, and instead cyber attacks can be used to target enemy resources without direct confrontation.

I. LITERATURE SURVEY AND METHODOLOGIES

2.1. Cyber War to keep the peace:

The evolution of technology is explainable, and IT development is growing at an alarming rate over the long term. This is a difficult thing to deal with in everyday life, and often decisions are made based on a "direct feeling". A look at current research programs and activities associated with various developments and announcements over the past few years provides a glimpse of what we can expect[1]. The aforementioned "Defence Innovation Initiative" is a good start to discovering what the technological world looks like tomorrow. Cyber Warfare follows the following:

1) KINETICS- Actions must have kinetic effects.
2) HIDDEN AND VISIBILITY- You may have taken effective measures to hide in the cyber world, but everything you do is visible even when no one is watching.
3) APPLICATION- There are no fixed rules of conduct in the cyber world other than those that require global action in order to change.
4) MASQUERADE - There is a business within the cyber world that has the authority, access, or ability to do whatever action the attacker wishes to do. The intent of the attacker is to take ownership of the business in some way.
5) WEAPONS FOR COMMON USE - Weapons are specially used.
6) CHAPTER- Defender and attacker control a very small portion of the internet they use.
7) USE- Anyone who can control a certain part of the cyber used by an opponent can control the opponent.
8) UNRELIABILITY- Cyber pace is incompatible or unreliable.
9) RELATIONSHIP- The physical distance from the target is almost invalid.

2.2. Cyberspace Cyber Military Strategy Rise in cyber wars:

This paper focuses on the use of false IP addresses, external servers and fake names, cyber attackers can act in complete anonymity and related punishments, at least in the given time. The boundaries of cyber pace are difficult to distinguish between soldiers and civilians and between physical and intellectual; and cyber power resources such as provinces or government actors, or representative. Cyberspace is described as the fifth battlefield with the traditional arenas of the earth, air, sea and space. The cyber war is considered to be a new but completely inseparable part of the war zone on many sides. Working on cyber pace is very likely to occur in conjunction with other forms of coercion and combat [2]. However, the methods and techniques of cyber warfare remain undeniable that they differ from these other methods of warfare. This paper has proposed strong and effective cyber military strategies for cyber-height in cyber wars. This paper presents cyber military strategies in three ways. First, we need to strengthen cyber power. This paper includes detailed strategies for our targeted programs or systems such as network, server, and data, etc. Third, must develop a pre-CTO. The pre-CTO includes targeted program, vulnerability, hacking tool, master / zombie server, attack time, etc. Fourth, we need to develop a CDA approach to accurate detection of cyber attacks [3]. Finally, we need to improve the power of cyber psychology. Cyber psychology is defined as propaganda and all other activities that affect the ideas, feelings, attitudes of all countries and groups in order to achieve the goal of national cyber pace policy. Ultimately, cyber military organizations are mechanical organizations or operating differently from other organizations.

2.3. Cyber War: Terms, Problems, Rules and Disputes:

As technology advances rapidly, it surely becomes a part of our daily lives and has positive or negative consequences. It is fair to say that the Internet became an integral part of this technological development. A new phase of international relations and domestic relations between nations and their communities is taking place based on these modern technologies. Instead of traditional methods, many provinces have begun to use new means of communication and have replaced the old ones. They now provide citizens with services through a network such as passport and visa applications, tax and billing, open exchange operations and operations, banking and insurance transactions, military service registration procedures etc. All of these services can be used with computers, tablets and even smart phones with internet connection [3]. Or, there are many advantages to this system, each action has an equal and opposite response. Cyber terrorism, cyber threats, cyber espionage, and cyber war are on the other side of the coin. While human privacy was at stake in combating these dangers, the risks are very high at the national security level. Attackers attempt to steal, harm, destroy or control important information from individuals, organizations, companies and even governments.

2.4. Suggestions for Measuring Cyber Power and Suggested metrics for Cyber Warfare (Cyber Blocking / Cyber Power)

Power can mean many things, to many people. In general, its use is understandable, that is, who is stronger and less powerful. Power is also one of the ubiquitous words that everyone seems to understand but few can explain. Hans Morgenthau described the elements of national power such as geography, natural resources, industrial power, military readiness, population, national character, national character and the quality of communication and government. Nowhere in his description is the use of information perceived as part of power [4]. So this raises a conclusion that the elements of energy have changed in the last fifty years. The short answer is yes and no, depending on the sources, for example today technology is often regarded as a national first aid as opposed to traditional ideas that are more inclusive of tangible assets. This is a major shift from the old analysis that focuses more on just counting military goods and industrial plants.

2.5. Case Study: BDA model of Standalone Radar system

As information and communication technology advances, the importance of cyber pace grows in society, the economy, and in defence of the country and beyond. in the temporary military service has evolved into a form of military service where a wide range of electronic warfare (EW) has been developed due to the development of IT technologies, and military and EW operations in cyber pace are integrated. In the US Army, it emphasizes that cyber warfare and EW operations should be made into a filed form, because it is done mostly for the same purposes [5]. The Department of Homeland Security has also established a Cyber Command to carry out cyber pace operations. At present, the assessment of military damage caused by military operations is one of the most important factors that can affect the success or failure of military operations [5]. Recently, many researchers have been conducted to assess the damage after a cyber attack, but it is difficult to find a study on the EW injury test linked to the cyber war. This paper proposes a basic military damage assessment (BDA) model that provides damage to EW equipment linked to cyber warfare in numerical terms according to the operational rate (MOP) and operational rate (MOE) of EW equipment. After that, set the conditions for taking cyber attacks on EW machines to provide an example of a model app.

2.6. Net neutrality in cyber war content

Real or potential interactions between infrastructures of varying levels of security, from insecure users to sensitive national infrastructure, have made cyber space a hotly contested and overcrowded site [6]. But operating conditions within this domain are more favourable for bad actors than for legitimate actors who want to provide security and protect systems and information. The technical skills to establish governance and cause damage to the domain are still widely distributed, but legal and ethical issues prevent legal actors from fully utilizing them.

2.7. Onion Cyber War Training Method

This paper describes the approach to cyber warfare training based on increasing exposure to a consistent set of basic information elements placed in the operational context. The information in the paper is based on practical experience in providing cyber warfare training and virtual fitness training [7]. Practical experience that provides a training program to prepare soldiers for cyber warfare has allowed the development of a number of key concepts that have proven to be effective. Some of these ideas challenge the traditional, vendor-based, network security training model and challenge traditional structures and roles used in pre-cyber military operations.

Although it has not been introduced as a out of the box solution for training cyber heroes, the principles are important when considering any military force in the development of a training model to support cyber performance. The development of open source tools, such as Cyber Training Lab Manager can provide a competitive environment for using key military features that are not available in tool-based training.

2.8. Ten Years of Cyber: Cyber Protection in X-ing:

This paper analyses the construction of cyber threats and defence capabilities over the past decade, analyses the current situation and makes recommendations for improvement. This paper is structured as follows: first, it describes the general conditions of military action against cyber, including an analysis of the potential of Western countries and their seemingly traditional enemy in the East and especially in Russia. The overall look includes a discussion of the practicality of the steps and a holistic view of upcoming technologies that are critical to cyber security. Finally, the requirements and recommendations for continued cyber security protection are briefly covered. Storage will challenge encryption security programs [7]. Being able to store everything until one can encrypt it requires strong encryption methods, and gives the traditional concepts of the proposed key lengths at certain intervals as insufficient. Second, the size of Quantum will be determined. And the paper stated that quantum computers in general would open up new opportunities for simulation, prediction, and security of systems, while doing so transcend and override traditional security concepts [8]. A recent study published by the University of Cambridge, IBM, and Intel shows great progress in this area. 178 Robots and the concept of “Soldier 4.0” will be very powerful, but at the same level, it depends heavily on IT ranging from the use of exoskeletons to smart bandages to quickly heal wounds or specifically remove traumatic memories from the brain. While DARPA’s Cyber Grand Challenge in 2016 demonstrated the power of defence systems to analyse attacks and modifications, the setup was based on smaller, more limited applications. However, it indicates the future of cyber security, and related programs such as System Security Integrated through Hardware and Firmware (SSITH) will increase the level of attackers.

2.9. Rules for Cyber-Warfare and Tallinn Manual: Case Study

The paper indicates that the Tallinn Manual lists Stuxnet's 2010 attacks on Iran's nuclear program as illegal. The purpose of this paper is as follows: (1) to analyse the historical and technical background of cyber warfare, (2) to examine the Tallinn Manual as it relates to cyber warfare, and (3) to evaluate its Tallinn Manual performance in the study of cyber attack history. The end of the paper tells us that this war represents more cruelty than rational involvement. No matter, the importance of the rules of engagement has been recognized for centuries. It not only rules the rules of engagement in establishing a war procedure, but also restricts the battlefield from operating within a set of known boundaries [9]. As this paradigm changes, as with the advent of the computer war, the rules of engagement must also change so that the international community can better assess the conflicts of Estonia, Stuxnet, GhostNet, and all future attacks on the Cyber Empire. After all, according to Morey's Law, the number of transistors in a circuit doubles almost every two years. Most likely, the cyber war will develop at the same rate.

2.10. The Cyber War: International Conflict, the Cyber War between the Nations and its Return

This paper consists of three parts. The first consideration of the concept of cyber pace, its main component, the issues of identity and online authentication, vulnerability, and threats, the second concept, researchers with the view of "cyber attacks" and the problem of invention cyber espionage, "cyber terrorism," and other forms of cyber attacks. An important part is the "cyber war" which is the basis of military strategy, detection methods, and testing of cyber threats. cyber, its legal framework, participation in the process of national and international organizations, issues of public-private partnerships, and the paper focuses on cyber attacks and cybercrime prevention using advanced technology. A limited range of uncertainties of current and time challenges e the advent of cyber pace are making a scary place [10]. Threats are directed at all politicians, international military leadership, business and law enforcement, and the individual diversity (individual). Each bears the responsibility for rights and obligations in real and digital life, including the protection of their families and nations from new forms of intimidation and attack. There is no prevention of cyber crime, cyber attacks and cyber war. Nations will face many cyber challenges in the coming days. Researchers identify five key trends that could affect the future of cyber security: the development of "cloud" data collection (cloud computing), which comes out under the control of individuals, organizations, and the growth of "large amounts of data." analytical algorithms (big data); effective use of mobile information technology (mobile transformation), demographic change in the development of the internet masses; blur the boundaries between digital and the physical world (Internet of Things).

2.11. Expanding Control and Control Infrastructure for Cyber Warfare Heritage

The purpose of this work is to identify the framework or integration of cyber cons "and the control within the classical constitution and the control of infrastructure. The arrival of cyber resources and military capabilities, as well as additional cyber details [11]. Although many of these infrastructures will operate on their own without resources, there is a need to jump between the two approaches. Such crossovers require much greater flexibility than is required by traditional command and control of positions. Data collection capabilities, and self defence capabilities, protection to protect local networks, to protect connections with field troops, to protect data collection skills, and to identify enemy operations. positioning and the position of enemy property using GPS and as appropriate. Intel Collection about enemy operations and objectives. Hot network location detection and anonymous detection - local identification and operation of areas with high levels of errors, loss of communication, or other activity that impedes normal operation of network infrastructure.

2.12. Principles in the Aftermath of Cyber Warfare: An Arab Citizens Awareness Study:

Persistent disregard for the effects of Cyber Warfare will bring great concern to all. Hackers and governments alike should understand the barriers their ways take. Governments use Cyber Warfare to provide strategic advantage over other countries, to protect themselves from enemies or to harm their opponents. Hackers use Cyber Warfare to obtain personal information, commit crimes, or express sensitive and beneficial intelligence. While both approaches may offer ethical use, the same can be said for another wide range. Knowing and understanding these devices will not only strengthen the ability to detect and counteract these attacks but also provide the means to expose malicious government programs, as the effect of Cyber Warfare can be far worse than the aftermath of a normal war. This paper [12] discusses the concept of ethics and the reasons that led to the use of information technology in military warfare, the consequences of using cyber warfare on civilians, legitimacy of cyber warfare and ways to control the use of information technology that can be used in society. This study uses a research approach to disregarding Arab citizens' awareness of cyber war theory, providing findings and evidence of behaviour in the aftermath of an invading cyber war. Detailed strategies and methods should be developed in this regard. Cyber-attackers can use computers and networks to destroy or destroy the infrastructure that citizens rely on. Most Arabs Citizen agreed that there should be international laws governing the use of the Internet and prohibits any form of attack that results in harm to civilians in all spheres of society. The international community has failed to update the current framework that responds to these cyber attacks. Faced with new and growing challenges to combat these types of cyber attacks and threats, governments and international authorities continue to rely on international law that has not been used to match modern threats and attacks.

2.13. Research Paper Title - Radio-Defined Radio (SDR) as a Testing Cyber-Electronic Warfare (EW) Partnership:

The electronic warfare (EW) works by increasing the amount of electromagnetic spectrum (EMS) of friendly users while denying the same benefits to opponents. In this way, EMS is used as a vehicle to achieve the desired results of strategies or strategies. These seemingly simple statements conceal much of the complexity and contradiction, as seen by the large number of articles and books published on the role of EW in the Journal of Defence Technology (JED) over the past few years. Cyber has the same goals as EW, but it is different in that the method used to achieve the desired results is information technology and networks than EMS. This difference in performance means that the cyber entry barrier is lower than EW leading to different characters, resource areas, motives, etc [13]. One of the biggest challenges for EW is blocking very weak signals from remote transmitters and disrupting remote transmission performance and receivers. The importance of standing skills in EW has led to the development of many relevant technologies. This technology can be exploited by cyber professionals to gain access to remote networks, thus eliminating the need to approach the target of cyber attacks in order to be successful.

SDR systems allow the signal processing features of EW long-distance technology to be used in a simpler way. In addition, the flexibility of SDR systems allows the integration of low-frequency amplifiers (LNAs), high-power amplifiers, antenna configurations, signal detection systems (DF) and other technologies familiar to EW specialists. The fact that the release of the program is available on the computer will greatly help to allow cyber professionals to take full advantage of this EW technology. In this way, existing EW technologies can be used to create a new way to attack vulnerable systems using cyber tactics. Network vulnerability is a major consideration for both cyber and EW. A major challenge in risk assessment is to get a complete picture of all RF transmissions for a particular network. This [13] transmission can involve a wide range of extremely wide frequency and contains a variety of communication processes. While it is possible to use an extremely large number of different systems to test each frequency band and network connections I can use, this method may work. SDR programs offer the possibility to use a single piece of computer-compatible hardware to fully assess network risk.

2.14. Introduction to the Marine Model for Technological and Information Wars

Technological advancement throughout history has increased “policy continuity in some ways in many regions and in new territories. Land exploration has expanded the map of the proverbial warfare of human warfare. The naval, air, and space warfare have all simplified the development of technologies that allow access to these technicians. Many now see cyber as the backbone of war. Like air, sea and space, military combat in this area is powered by new technologies. However, unlike the wind, the sea, and the environment, the cyber environment itself is man-made. And, unlike the air, space and sea, people do not travel in, live or work on cyber pace. There are no visible weapons of attack or defence and no kinetic attack force to cross this path to attack others. No-less, there are important cyber assets and attacks that cross the cyber domain to attack assets in other domains.

Cyber brings new challenges to defining the legitimate intentions of war. It also presents a battlefield where independent individuals, organized crime, extremist groups and state actors have equal access to the military and military equipment [14]. Unlike state actors, however, some groups have little restrictions on their targets, methods and effects of attack. Attacks by groups of government and non-government actors alike can undermine national security, damage the national and regional economy and target private individuals and firms. This is not a paradigm of modern warfare where world actors possess important and almost indisputable skills compared to individuals and groups. It is certainly not the rise of American military power that has led some to point to the United States' conflicts as "one case in which the U.S." It can use its military to destroy military, economic, and political ends.

2.15. Cyber Prevention in Times of Cyber Anarchy - Exploring Diversity in the U.S. And China Strategic Thinking:

The advent of the cyber domain has introduced a new dimension to the wars and ideas of existing strategies, while triggering different responses within different national contexts. In response, the "first wave" of theory and cyber prevention strategies has already emerged. The functions of the structure will require significant development and may also vary due to different cultural strategies and organizational strengths [15]. While certain technological aspects of the cyber domain, such as its current jurisdiction, create more than objective challenges, national responses to the "cyber turmoil," exacerbated by the lack of norms or legal frameworks for building cyber-compliant order, will always be influenced by nature and ideas. In particular, cyber blockade will remain the "national thing," in particular. As such, like traditional prevention, it is basically a function of understanding. Therefore, from a constructivist point of view, opinions from the U.S. And in China about cyber blockade it will influence their efforts to curb cyber threats and use cyber power for the purposes of prevention, even if these two major cyber forces' turn into thinking in it.

2.16. Work Analysis for Cognitive Cyber Cognitive Situation Awareness (CCSA) to Cyber Defence analysts

Although much of the defensive work is done in secret, the effects of failure can be far greater. Such an increase in malice is not limited to computers and server applications. With the advent of Web 2.0, devices and vehicles that are not traditionally connected are now part of the network, or are using services that expose the offensive environment. Medical devices, for example, now pose a risk to patient safety, with very little unwanted disclosure of personal information, and worse, life-threatening through malicious device performance and reporting [16]. The low security of these systems is in stark contrast to the need for some kind of firmness that people are asked to provide consistently. In selecting the appropriate methods for job analysis, paper has done a lot of looking. First, collected general information such as organizational structure, the physical environment, and the participant's understanding of his or her roles and responsibilities in the general population survey, and in the less formal interview. Second, while our aim was to determine status awareness as it relates to intrusion detection and cyber protection in general, the most obvious choice for conducting Targeted Activity Analysis required expert knowledge regarding functions and work environment. This technology was not available in the literature or to us by staff. Choosing a Job Analysis Method in choosing the right career analysis methods, paper has done a lot of things. First, collected general information such as organizational structure, the physical environment, and the participant's understanding of his or her roles and responsibilities in the general population survey, and in the less formal interview. Second, while the objective was to determine condition awareness as it relates to intrusion detection and cyber protection in general, the most obvious choice for performing Targeted Activity Analysis required expert knowledge regarding functions and work environment.

2.17. Cyber Weapons: Printing Framework:

This paper goes on to describe each part of the description provided: A computer program can be a software application or script because programming and writing languages allow data and hardware control over a variety of roles. Created or used because a cyber weapon can be developed (designed and used) and used by the same country, group, organization or individual or used because someone can buy a cyber weapon according to their needs [17]. Later paper more talks more about this subject. Converting or damaging because the purpose of a cyber weapon is to alter or damage temporary or permanent target e.g. system or application, physically or in the digital world. A program or part of an ICT system because the target can be an ICT system e.g. an application, data, device or it could be a non-ICT program that contains an ICT component that represents the carrier directly to the target you want. To achieve the (military) objectives of the opposition because they are aimed at achieving certain goals and objectives. However, the impact can be on neutral or affiliated groups and on those who send it.

Conclusion

Many international agreements have been launched regarding cybercrime. Overall, multi-national and regional legal instruments, as well as national legislation, vary depending on the content and scope of crime distribution, measures and investigative powers, digital evidence, regulation and risk, and international jurisdiction and co-operation. These agreements also vary according to the local or regional and operational standards. These differences create barriers to effective identification, investigation and prosecution of cyber criminals and the prevention of cyber crime. Protections are needed to ensure that laws that restrict access to the Internet and content are not violated and that they comply with the law and human rights. Legal clarity is also required to ensure that laws are not used to restrict access to content in a manner that violates human rights law. The danger lies in the use of machines or workflows which are terms used to describe the increase in law and / or other measures in areas beyond their original level), where laws and investigative powers are introduced to identify one type of cyber crime and then used to identify another In addition, the challenges regarding access to and the consequences of cybercrime arise when "one-of-a-kind Internet content is acquired in a third country" where the content is considered illegal.

REFERENCE

[1] Cahill, T.P., Rozinov, K. and Mule, C., 2003, June. Cyber warfare peacekeeping. In IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003. (pp. 100-106). IEEE.

[2] Eom, J.H., Kim, N.U., Kim, S.H. and Chung, T.M., 2012, June. Cyber military strategy for cyberspace superiority in cyber warfare. In Proceedings title: 2012 international conference on cyber security, cyber warfare and digital forensic (cybersec) (pp. 295-299). IEEE.

[3] Sevis, K.N. and Seker, E., 2016, June. Cyber warfare: terms, issues, laws and controversies. In 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security) (pp. 1-9). IEEE.

[4] Armistead, E.L., 2016, October. Suggestions to measure cyber power and proposed metrics for cyber warfare operations (cyberdeterrence/cyber power). In 2016 International Conference on Cyber Conflict (CyCon US) (pp. 1-7). IEEE.

[5] Choi, S., Kim, Y., Kim, D., Kwon, O.J. and Cho, J., 2018, July. A Case Study: BDA Model for Standalone Radar System (Work-in-Progress). In 2018 International Conference on Software Security and Assurance (ICSSA) (pp. 45-48). IEEE.

[6] Hartmann, K. and Giles, K., 2018, May. Net neutrality in the context of cyber warfare. In 2018 10th International Conference on Cyber Conflict (CyCon) (pp. 139-158). IEEE.

[7] Clark, D.J., 2015, November. An onion approach to cyber warfare training. In 2015 Military Communications and Information Systems Conference (MilCIS) (pp. 1-4). IEEE.

[8] Koch, R. and Golling, M., 2018, May. The cyber decade: cyber defence at a x-ing point. In 2018 10th International Conference on Cyber Conflict (CyCon) (pp. 159-186). IEEE.

[9] Caso, J.S., 2014, June. The rules of engagement for cyber-warfare and the Tallinn Manual: A case study. In The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent (pp. 252-257). IEEE.

[10] Rohith, C. and Batth, R.S., 2019, December. Cyber Warfare: Nations Cyber Conflicts, Cyber Cold War Between Nations and its Repercussion. In 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) (pp. 640-645). IEEE.

[11] Erbacher, R.F., 2005, October. Extending command and control infrastructures to cyber warfare assets. In 2005 IEEE International Conference on Systems, Man and Cybernetics (Vol. 4, pp. 3331-3337). IEEE.

[12] Al Barghuthi, N.B. and Said, H., 2014, May. Ethics behind Cyber Warfare: A study of Arab citizens awareness. In 2014 IEEE International Symposium on Ethics in Science, Technology and Engineering (pp. 1-7). IEEE.

[13] Du Plessis, W.P., 2014, August. Software-defined radio (SDR) as a mechanism for exploring cyber-electronic warfare (EW) collaboration. In 2014 Information Security for South Africa (pp. 1-6). IEEE.

[14] Straub, J. and Traylor, T., 2018, December. Introduction of a Maritime Model for Cyber and Information Warfare. In 2018 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 25-29). IEEE.

[15] Kania, E.B., 2016, October. Cyber deterrence in times of cyber anarchy-evaluating the divergences in US and Chinese strategic thinking. In 2016 International Conference on Cyber Conflict (CyCon US) (pp. 1-17). IEEE.

[16] Gutzwiller, R.S., Hunt, S.M. and Lange, D.S., 2016, March. A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts. In 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA) (pp. 14-20). IEEE.

[17] Maathuis, C., Pieters, W. and Van Den Berg, J., 2016, October. Cyber weapons: a profiling framework. In 2016 International Conference on Cyber Conflict (CyCon US) (pp. 1-8). IEEE.

[18] https://www.dnsstuff.com/common-types-of-cyber-attacks

[19] https://k7press.wordpress.com/2011/12/07/the-art-of-cyber-war/