Cyberwarfare

Palkin Gupta, UrviDeole, Akshay Kapoor, Devansh Agrawal

Student Final year Information Technology, SVKM's NMIMS MPSTME 1,2,3

***Abstract*—*The globe has shifted into an entirely fresh field of operations in the past centuries: cyber terrorism. This new form of warfare both affects national-state economic and political relations and changes the form of modern warfare. There are therefore a whole fresh array of issues, despite the benefits introduced by contemporary technology. This study will provide some context on cyber-warfare, including how it operates, how it is used and who it is used to safeguard itself against future assaults and how countries use intelligence methods.*

1.0 INTRODUCTION

Cyber warfare is the use of technology to attack a nation, causing significant harm. Cyber warfare means no violence or using weaponry usually associated with the term 'war'. These assaults on the Internet, by destroying, or changing categorized information to undermine networking, sites and facilities, are disabling economic and organizational systems. However, attacking a nation via the Internet will have both extreme consequences for the attacker and collateral damage to the world.Hackers are no longer confined to the intelligence and espionage world. Instead, we can expect a future in which cyber-attacks are a part of conventional warfare and in which hackers who carry out these attacks are increasingly subject to conventional weapons retaliation. Continued internetizing everything from missile systems to electrical grids has resulted in an attack surface which can't be ignored by military actors.With cyber warfare, it is now possible to disable critical infrastrucutre in a major city and disrupt the central services, to steal millions of dollars from banks all over the wolrd, infiltrate defences, extort millions from public companies and sabotage weapon systems. Contrary to nuclear weapons that would blast people within a quarter of a mile and kill nearly all, the death toll from most of the cyber attacks would be slower. People might die from

meat, electricity or gas inadequacies for heat or car crashes triggered by a faulty aircraft network. This could occur in a large area, which could lead to mass injuries and deaths.

More phones are linked to the internet every day and additional data is recorded on those devices and
more guidance is provided. Other countries that invest substantially in pcs as fighting instruments have seen remarkable returns while the attack surface remains to expand. In relation to the well defined capacities of theft and intelligence collection, malware now controls traveling cars, destroys petrochemical power stations, disables electrical grids and much more. All of this can be done by pressing a key from random ranges and is carried out nearly immediately.

It is difficult to control the broad decentralization and scale of Cyberspace from a political point of view. Non-state actors in the cyber war room can take as big a role as government performers, leading to hazardous, at times catastrophic results. Small groups of extremely qualified malware designers are as effective as major government agencies in global politics and cyber warfare. The willingness to share their achievements and developments on the web as a form of weapons proliferation is a major aspect of this capability. This allows less hackers, who were once only a little handful skilled enough to manage large-scale attacks, to become more skilled. Moreover, prosperous black markets buy and sell these cyber guns without respect for their implications for the largest bidder.

2.0 TYPES OF THREAT

Kaspersky Lab's founder equates big cyber systems like Flame and NetTraveler, discovered by his company, to biological weapons, claiming they have the same destructive potential in an interconnected world.

2.1Espionage: It is the act of obtaining, for the sake of personal, economic, political, or military benefit, information secret and information without the permit or knowledge of the holder of information, using proxy servers, cracking techniques an*d* malicious software for the use of internet, networks or individual computers. It includes public activity analysis on websites such as Facebook and Twitter. Such operations, such as non-cyber spying in the victim country, are usually illegal and supported fully by the aggressor country's government. The ethical situation also depends on our point of view, especially on the view of the governments involved. As specifically targeted by cyber espionage for secret information for malicious uses, it does not address the intent or nature of the stolen information. This may appear unnecessarily vague but it is appropriate for the purpose of international law.

Cyber collection is a widely used technique to conduct espionage that involves insertion of a malware or malicious software into a targeted machine and scanning, collecting and exfiltrating sensitive information.
Functionality of cyber collection:

- Scan: Files or documents of interest are scanned to find and copy them.
- Location: GPS sensors attached to the targeted device are used to determine its location and movement.
- Bug: Microphone is turned on to record audio
- Camera: Cameras are activated to capture graphic images
- Keylogger: Each keystroke and movement made by the target can be captured.

Espionage is at least more useful for nations that are perpetrators of external cyber-attacks. For example-

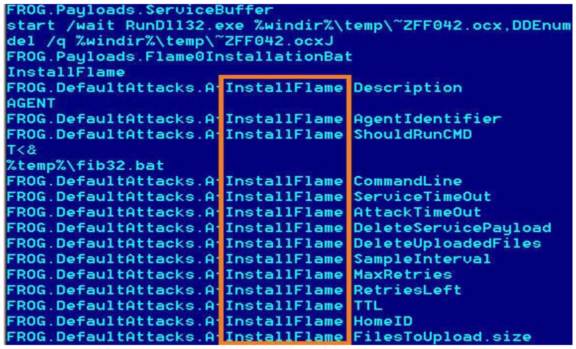
- Edward Snowden showed that the US was spying massively on many countries.
- The Chancellor compared the NSA to the Stasi after the revelation by the National Security Agency of Chancellor Angela Merkel of the NSA had been revealed.
- The NSA records almost all cellular conversations in the Bahamas, without authorisation from the Bahamian Government, and similar programmes.
- U.S. defence contractor computer systems since 2003 Titan Rain samples.

- Infringement of data attributed to China by the Personnel Administration Office in the United States.

2.2 Sabotage: Computers and satellites coordinating other activities are vulnerable components of a system and can cause equipment disruption. Military systems compromise, such as C4ISTAR components responsible for commands and communication, can lead to interception or malicious substitution. Electricity, water, fuel, transport and communications infrastructure can be susceptible to interruption. According to the civil society, the security violations have already gone beyond robbed number of credit cards, and potential goals could include the electricity grid, the Trains or the stock market, according to Clarke.

Stuxnet:Stuxnet is a highly advanced and trailblazing computer virus that exploits unknown Windows zero-day vulnerabilities. This infection then gradually spreads. Its impact is not just seen on PCs but in real-world too; the effects being disastrous and impossible to recover from. Specifically, it targets centrifuges for production of enriched uranium that powers nuclear weapons and reactors.

Stuxnet was discovered by Sergey Ulasenin June 2010 when it was found inside a PC which was behaving erratically by shutting down and restarting constantly. Though it has a high infection rate, it does not affect devices with no involvement in improving uranium.When injected into a device, it checks if the device has an established connection with PLC. They are a form of control systems used widely in industries. Stuxnet causes the centrifuges to spin rapidly and over a long period of time demolishing equipments. The PLCs however come across as working fine making it tough to detect the worm.



```
FROG.Payloads.ServiceBuffer
start /wait RunDll32.exe %windir%\temp\~ZFF042.ocx,DDEnum
del /q %windir%\temp\~ZFF042.ocxJ
FROG.Payloads.Flame0InstallationBat
InstallFlame
FROG.DefaultAttacks.A InstallFlame Description
AGENT
FROG.DefaultAttacks.A InstallFlame AgentIdentifier
FROG.DefaultAttacks.A InstallFlame ShouldRunCMD
T<&
%temp%\fib32.bat
FROG.DefaultAttacks.A InstallFlame CommandLine
FROG.DefaultAttacks.A InstallFlame ServiceTimeOut
FROG.DefaultAttacks.A InstallFlame AttackTimeOut
FROG.DefaultAttacks.A InstallFlame DeleteServicePayload
FROG.DefaultAttacks.A InstallFlame DeleteUploadedFiles
FROG.DefaultAttacks.A InstallFlame SampleInterval
FROG.DefaultAttacks.A InstallFlame MaxRetries
FROG.DefaultAttacks.A InstallFlame RetriesLeft
FROG.DefaultAttacks.A InstallFlame TTL
FROG.DefaultAttacks.A InstallFlame HomeID
FROG.DefaultAttacks.A InstallFlame FilesToUpload.size
```

Fig 1. Stuxnet: An Effective Cyber war weapon

Stuxnet was thought to be developed by the US and Israel to attack Iran’s nuclear facilities. It did, in fact cause significant damage to Iran. The US and Israel, however did not admit their involvement in the attack.

Stuxnet has a set of independent units: 1) a self-replicating malware that implements functionalities relevant to the main piece of information of the attack; 2) a link file which spontaneously implements copies of the malware spread across the network; 3) and a rootkit portion that conceals all infected files and programs, making its detection strenuous or in extreme cases, impossible. It is introduced into a device via an infected USB. It spreads through the network looking for Step7 and introduces the rootkit into the intended device, thus modifying code.

Siemens provided a Stuxnet tool for detection and removal. If an infection is found, Siemens suggests contacting customer support and advises applying Windows security vulnerability fixes and banning the use of third-party USB flash drives. It also advises to change user access codes immediately.

2.3 Denial-of-Service Attack:The computer attempts to make the machine or network resource not available to its designated users by Denial-of-Service (DOS attack) attack or Distributed Denial-of-Service attack (DDoS attack). DoS attackers typically target websites or services hosted on high-level web servers like banks, payment gateways for credit cards and even root name servers. DoS attacks cannot be restricted to computer-based methods since strategic physical attacks can be just as devastating. While submitting authentication permission, the network or server can not locate an attacker's return address which causes the server to wait to close the link. The intruder sends out more encryption messages with incorrect return addresses after the server exits the link. The encryption and waiting cycle will therefore begin again and keep the network or database active.

2.4 Man in the Middle: Also known as MIM or MiTM is an intrusion from an individual in the centre of two entities enabling him to capture, transmit, receive data planned for or not intended to be sent without being notified by any other entity until it is too late. The entities involved, however believe that they are interacting with each other with other when in reality the conversation is being tapped and controlled by an attacker. It is often referred to as a form of eavesdropping. For example, An attacker may mount a Wi-Fi network utilizing a login screen to mimic a hotel system; an attacker could collect some user-sent data, including bank passwords, once a user logs into the network.

2.5 Phishing: Phishing is a type of social media assault that is often used to steal user data, such as login credentials and amount of credit cards. It is when the intruder covers a target by accessing an address, instant letter or text message, as a trustworthy person. The beneficiary is then tricked to click on a malicious link which may result in malware download, device freezing and exposing sensitive data as part of a ransomware attack.The outcome of such an assault may be disastrous. It covers illegal browsing, cash taking, and recognizing theft of people.

Phishing attacks usually depend on email or other forms of electronic communication, like social networks delivering direct messages, text messages and other instant message modes. To order to collect background information on the victim's private and working life, his preferences and behaviour, Phishers may use social engineering and other public information outlets such as social media platforms, such as LinkedIn, Facebook and Twitter. Phishing emails, however, are written poorly and visibly fake but maybe turned a blind eye to at times. In a standard phishing attack, an attacker sends a mass email to workers impersonating an IT department employee. The email is a reminder to clients that they are completing the mandatory annual IT safety training module electronically. However, the training module is managed by the attacker. During the course, the victim(s) is instructed to enter his credentials, which are then sent to the abuser directly.

3.0 Cyber warfare of the big 5

China:

Chinese Information Operations and Information Warfare involves the notion of "Network Warfare," which is approximately similar to the notion of cyber-warfare in the US. Chinese weapons and nuclear weapons have the highest levels of defense budgets in the world. The Foreign Policy magazine provided an estimated range from 50,000 to 100,000 Chinese "hacker army" personnel.

While research has traced a variety of attacks against company and computing infrastructure systems originating in China, the accusation of aggressive espionage has long been accused by western countries; It is almost impossible to know if or not an attack is government-sponsored because it has been difficult to track genuine identities in e-computing.

Although China's cyber-war investment in 1997 was largely intended to compensate for its conventional weakness against the US and Russia, cyber operations are currently being used by the country in order to target its other competitors. It's not surprising that it's focused on India.

US:

The United States is highly reliant on the Internet and thus very vulnerable to cyber attacks as a big advanced economy. Under addition, due to relatively advanced technology and large military spending, the United States has substantial security and force generation capabilities. Cyber-warfare represents an increasing threat to internet-related physical systems and facilities. Harmfully targeting rivals at home or abroad is a potential threat to the US. The United States has established substantial cyber capabilities in reaction to these growing challenges.

As a risk to national safety as well as as a medium of aggression, the United States Department of Defense acknowledges the use of computers and the Internet for combat in cyberspace.

The US Cyber Command centralizes cyber operations command, organizes current digital assets and synchronizes US military networks. It is a Single Combatant Order of the Armed Forces.

Russia:

Russia-sponsored cyber warfare involves denial of service attacks, hackering attacks, misinformation and information dissemination, intervention of government-sponsored teams in public activism, SORM-based internet monitoring, anti-dissident harassment and other practice. Accommodating some of these operations were Russian intelligence messages that were independent of the FSB or formerly members of the 16th KGB Departments, investigative journalist Andrei Soldatov claims.

An overview of "Information Countermeasures" (IPb) by the Defense Intelligence Agency in 2017 identified Russia as "strategic decisive and vital to monitor their domestic population and to manipulate opponents ' states" separating' Data Countermeasures' into two divisions of "Information-Technology" and "Information-Psychology." The first covers network operations in security, targeting and manipulating and the second concerns "trying to change people's actions and confidence in Russia's democracy objectives."

Russian security services have been reported to have carried out a range of denial of service attacks as part of their cyber warfare with other nations, including Estonia cyber attacks of 2007 and Belarus, South Ossetia, Georgia and Azerbaijan cyber attacks of 2008. A teenage Russian hacker named himself, claiming he was charged for breaching NATO machines by Russian State Security Services. At the Department of Data Security he studied computer science. The FSB compensated for his training.

UK:
With the development of a number of operations centers for £ 22 million, the Government has announced proposals to improve British defensive cyber capability.
The centers will be at the forefront of British cyber warfare and will work closely with national security agencies and the military's 77 Brigade advanced intelligence group.
Workers are to provide army research round the clock, counter disinformation and tackle electronic challenges whilst reinforcement for military work in the UK and abroad. "Such latest cyber centres, Tom Copinger-Symes, would enable the army and defense to quickly change how we use evidence, so that we can engage in a way fit to the 21st century with our adversaries.

The project was launched by the Defence secretary Penny Mourdant, during the NATO Cyber Defense Pledge Conference in London, describing wii, "The integration of artificial intelligence and military analysts can help us better understand the risks, seize vulnerabilities and let us get to know the truth much more easily, quashing the sounds of misinformation on our opponents."

In all, Uk language is that that the country is more and more ready to deliberately target or damage the digital networks of other nations as a revenge for threats on our own and related systems. With the overarching momentum of recent security and foreign strategy to drive Britain toward Russia's conventional bogeyman as a counter-force for the better, cyber-war challenges will become highly important.
Using its cyber capability against another nation, the UK has not acknowledged. The goals are publicly recognized only by Islamic extremists in the Middle East.

Germany:
A major program for defending computer networks and vendor processes is developed by the German Government. The National Cyber Defense Center will be responsible for the identification, evaluation and implementation of the steps needed to deactivate the danger by a new institution. The National Cyber Defense Centre. Therefore, there will be a National Cyber Security Committee.

The government's IT experts have become regularly protecting Germany's networks from overt cyber-attacks. Germany suffers from four or five such assaults every day, according to analysts. Given that many structures operated by machines involve German military planning, the control of water resources, energy, nuclear power, and banking, the dangers of such attacks remain clear.
Besides the terrorist threat and advancements of certain rogue states in their capacity to use ballistic missiles, cyber attacks against sensitive networks have been perceived as a increasing safety danger.
Today, many businesses and policymakers rely on the GDPR, but cyber security is not just about data protection but also about securing a country's main infrastructure. This is the position of the second Regulation of the EU, the NIS Directive, which is mostly overshadowed by the GDPR. Such form of attacks have recently been painfully experienced by German authorities.
The recent attack on a variety of ministries is alarming, as the internal computer networks of the state should be far more guarded than legislative networks, where elected officials frequently travel around using mobiles, personal computers that are less shielded than parliamentary desktop computers. Hackers were accused of interfering in German Defense

and Foreign Ministries networks for at least one year and have received plenty of data. The assault on December 19, according to Radio Rbb and DPA, was informed of by the German intelligence service "by knowledge from a friendly country."

4.0 Different Cyber Threat Actors Have Different Motivations-

4.1 Cyberterrorists-

There are two major modern fears about cyberterrorism: cyber-space technology risks and traditional terrorism. While there is no single or internationally agreed definition of cyberterrorism, it consists in general of a politically motivated extremist group or non-state actor using cyber tactics to intimidate, coerce or exploit an audience; force a change in politics; or cause fear or physical harm.

To date, there have been no public records of criminals using the internet to carry out cyber attacks; what has been done that has been related to cyberterrorism is more like hacktivism. Many terrorists, or non-state actors, use cyber to pursue their goals. We use the internet in many ways: for example, to gather information, to learn how to build a bomb; to attract, meet and interact with like-minded people; and to spread propaganda. But being in cyberspace alone does not make a cyber-terrorist a criminal. To commit a terrorist act, cyberspace must be used somehow. Films and media show what could be cyberterrorism: terrorists exploiting digital risks for action.

4.2 Hacktivists-

Hacktivists are typically inspired by a cause— political, economic, or social— from humiliating celebrities to revealing human rights, to waking up a company to its vulnerabilities, to targeting groups whose values they disagree with.9 Hacktivists who steal and disseminate sensitive, proprietary, or sometimes hidden data in the name of free speech. Several times, when conducting a distributed denial of service (DDoS) attack, they try to deny access to a particular service or website, effectively denying legal access by flooding a website with more traffic than it can handle, causing the site to crash.

4.3 State-Sponsored Actors-

State-sponsored actors provide the authority, funding, or technical assistance of a nation-state to advance that country's specific interests. State-sponsored actors have stolen and exfiltrated information on intellectual property, sensitive personal identification (PII), and money for espionage and exploitation purposes and continue to do so. These data appear for sale in rare cases on illegal black markets. Such specifics, however, are usually kept by the actors for their own purposes. Although data from data breaches may not always appear on underground markets, the tools and guidelines for exploiting vulnerabilities that first allowed access to compromised systems can appear. For example, a researcher released the vulnerability used to breach Equifax and the data were posted on hacking forums and included in the hacking toolkits within 24 hours.11 However, it should be noted that there was no formal verification as to who carried out the intrusion into Equifax.

In a few cases, state-sponsored actors have carried out cyber attacks to send a political message— rejecting, weakening, disrupting, or destroying computer systems. An example of this is the Sony Pictures Entertainment attack in 2014, where North Korea tried to advance its political agenda and partially prevent the release of The Interview film.

Instead of seeing what they are doing in violation of rules, government-sponsored actors feel they are acting in accordance with their own laws, and most have accepted that cyberespionage is a legitimate practice of the nation. Deterrence — political, financial and economic implications — is believed by some to play a role in stopping and exacerbating these types of attacks.

4.4 Cybercriminals-

Cyber criminals are motivated by financial gain — they care about making money.14 They need access to our personal, political, and health data to monetize them on illegal black markets. The stolen data from these hacks emerged on black market sites within days, particularly for the retail sector.

Such industries are diverse, dynamic, and segmented— growing rapidly, evolving continuously, and innovating to keep pace with consumer trends and stop retailers from recognizing them through law enforcement and protection. They come in a variety of different types. Some are devoted to a particular service or product. Others provide a variety of goods and services for a full life cycle of an attack— from the tools needed to breach a network to cyberlaundering of the stolen goods. Nearly everyone, at least at the most basic levels, can get involved in these markets.

Cyber criminals function behind encrypted and peer-to-peer networks (such as Tor and OpenBazaar, respectively) and mask their emails and payments using digital currencies and cryptographic technologies (such as Bitcoin).

4.5 The Challenge of Attribution-

After a data breach, it is hard to relate. Electronic data is often inadequate to classify the suspects or their country of origin. That said, there are cases where similarities are found in the software used by numerous commercial security firms and risk management organizations involved in the wake of an intrusion of various attacks. Similar ransomware was commonly used in the 2014 cyber attack on Sony Pictures Entertainment and the 2015–2016 SWIFT data breach (i.e. from North Korea). And many recall the strong possibility that data breaches from the same place (China) came from ransomware from Personnel Management Office (OPM), Anthem, then United Airlines.

Such various actors of cyber threat are interacting.

Although there are variations between each of the cyber threat actors and disparities in motivation, there is some degree of fluidity between the groups. Many people use the same tools and techniques in many situations, sometimes because they are the only available options, and sometimes because this helps in logical reasoning or shifting the blame to another side. In some countries, state-sponsored actors can collaborate to carry out an attack with "citizen hackers" or their country's cybercriminal elements.

5.0 People: Who Participates In Cybercrime Markets?

In these sectors, there are often hierarchies and specialized positions: managers sit at the top, followed by subject experts with advanced knowledge in specific fields (e.g., package designers, data traders, cryptanalysts, veterans). Next are intermediaries, distributors and sellers, preceded in general by membership.

At the bottom of the hierarchy, the market represents the consumer. Mules and virtual money mule systems come into play here — the highest level of customer interaction.

Mules use multiple methods to turn the stolen credit card and ecommerce accounts into functional currency, such as completing wire transfers and delivering items with 8 stolen funds bought overseas. Mules may be witting participants (well trained and organized operations) or naïve participants (involving naïve people).

The number of participants in these black markets has risen as entry barriers decline.

Barriers to reach and compete in these markets today are negligible — essentially, all that is necessary is an internet connection and a smartphone. This is because of the expanded proliferation of websites, forums and talk platforms where items can be bought and exchanged. Increased availability of as-as-as-as-service systems, point-and-click apps, and easy-to-find online tutorials make it easier for technical novices to take advantage of what these markets offer or just use someone to strike them. Increasing the number of blogs, books, YouTube videos and Google guides on "how to use exploit kit X" and "where to purchase credit cards" also encourages entry into the lower levels of these markets, particularly for those who want to be shoppers.

Surprisingly, these markets are highly reliable — reputation is very important, and most companies and customers are what they think they are and what they claim they are doing. Reputation involves either earning credentials with others and a good reputation and defending oneself (e.g. having good customer reviews).

Because agreements can not be lawfully enforced in black markets, businesses are constantly plagued by rippers who do not provide the goods or services they sell and are an exception to the high reliability of the industry. Rippers tend to be registered and quickly removed by administrators (for example, to delete their accounts). Although new names help them to access new networks quickly, a credibility that avoids cheating takes time to restore.

6.0CYBERPEACE

If we are to move past the zero-sum complexity of existing cybersecurity viewpoints — and thus cyber-peace — we must avoid portraying the problem as one of cyber-insecurity and negative peace. As well-known by Alexander Wendt, "anarchy is what states make of it," In other words, the concept of anarchy is not a given. If actors construct concepts affects if they behave (and react). Cyber is a term, like anarchy. Human beings construct it, both physically and conceptually, so in Wendtian terms we can think about it.

Next, we must reframe the debate on cybersecurity along the lines of human safety. Cybersecurity, as argued by the previous section, is beyond state security. It goes beyond state security as cyberspace and cyber vulnerabilities challenge the traditional paradigm of state-as-solution. Since the model of state-as-solution is not working, we must question why we tend to try to take the state as an object of protection. I say we should rather look at the wrong security benchmarks: people. Human security is looking at those acts that threaten the safety of an individual. Such attacks may come from two directions, as conceptualized in the literature on human security: violent and non-violent threats. In short, human security is viewed as a process of conflict and development that seeks to protect the individual from both fear and desire.

Secondly, we should adopt a positive framework for peace as well. The theory of positive peace by Johan Galtung resulted in the field of "peace and conflict studies" or the study of "conditions of work for peace." Galtung aimed at recognizing the philosophical and empirical roots of current stable societies and creating peace. The theory and subsequent realistic adaptation can be a heuristic view of safety and cyber harmony.

Galtung's concept of peace is based on the fact that peace is the absence of conflict from the theoretical point of view. His architecture of aggression, however, is complex. Instead of violence being a limited definition of physical or lethal injury, he argues that violence is far more than physical incapacitation, "or deprivation of health... in the hands of an individual who wants this to be the consequence.” To Galtung, "If it's all about terrorism, and peace is seen as its negation," then we neglect too many other aspects of violence to hold "as an ideal" peace.

He describes six dimensions of violence on his account: physical and psychological; negative vs. positive; object-oriented; direct / personal vs. indirect / structural; intended vs. unintended; and potential vs. latent.

Violence can then occur between individuals, between individuals and structures, or even between systems. It not only focuses on a human agent, but also includes objects and physical and psychological conditions. Therefore, on Galtung's view, there are two distinct types of "peace as the absence of abuse": negative peace and meaningful harmony. The absence of direct personal aggression is negative peace. Nevertheless, the lack of structural violence is positive peace. Therefore, creating sustainable peace is shifting the social structure that allows for stratification, discrimination, and imbalance. It is a more comprehensive term than the absence of people who physically or mentally directly harm each other.

From the viewpoint of cybersecurity, both human protection and constructive peace mechanisms provide us with a stronger purchase of cybersecurity in cyber peace hopes. This is because cybersecurity goes beyond the idea of violence as bodily harm and is wider than that of crime. In reality, claims positing cyber "war" will never happen because war is essentially of "aggressive nature," where aggression is "often theoretically or actually lethal," has too narrow a focus. In addition to unnecessarily limiting what constitutes as an act of war, it ignores the full range of coercive and violent acts that can happen to individuals by digital means.

Therefore, it makes sense to locate the key security referent not with the government, but with those agents operating in and through cyberspace. Indeed, as Dunn Cavelty argues, instead we should look at how to secure individual citizens by reducing cyber vulnerabilities. To her, even an over-emphasis on protecting digital structures and "critical infrastructure" is unbalanced and not a true "public good" because even this view of cybersecurity "mainly benefits the few and already strong institutions and has no or even adverse effects on the rest."

Using the individual as the basis of protection for all other possible claims of rights means we should explain how the other safety items are properly connected to the human being. What could protect such secondary objects? We have information / data, property / infrastructure, apps, and artificial agents as well. In a way that gives meaning or value to human life, each is linked to human life. 5 "Human life" can, however, be divided into two distinct categories: cyber-peace: cyber-security Through the Lens of Positive Peace, 9 that of individuals and their well-being; and that of society needed to sustain their human lives. Obviously, this latter definition would include arguments that the government should protect against threats to "national security," but these claims are focused on the rights and lives of individual agents.

Potential actors that could affect any of these institutions are: individuals, artificial forces, corporations, non-state actors, governments, and the cyberspace system itself. We are, in short, individuals and systems. Insecurity — in and out of cyberspace — can occur in any of these possible combinations due to vulnerabilities in networks, devices, software, hardware, information, the objects to which they are related, or the behaviour or practices of individuals using any of these items. Therefore, the way we try to achieve security in any of these fields always requires a forward-looking approach towards the very goals of security: stability.

Cyber peace is the ultimate cyber security nation. Yet it's not a pure absence of threats, it's a more comprehensive notion of the very security conditions. Operating within the context of Galtung helps one to include more aspects of violence, so recognizing cyber threats is more possible. Therefore, the opposite side of this coin is that its architecture can also help us understand the protections needed to make people safer against cyber violence types.

Therefore, cybersecurity is a spectrum. Full insecurity is at one end - a state of war; and full security is at another end - a state of cyber-peace. A lot of different types of violence can happen along this continuum, to many different subjects and objects. Then we can unpack what they might be in the cyber background, taking the six dimensions of aggression. This concept is just one way to view violence by cyber means and is not intended to be exhaustive in cyberspace:

Thinking at the different ways in which one can be subjected to violence, and what a cyber alternative might be, we may begin to identify ways to mitigate or remove these forms of violence. In other words, the cyberspace structure allows for the kinds of insecurities that allow an agent to exploit a vulnerability in an entity that is either directly linked to the human body for life-sustaining or life-enhancing purposes or exploits a vulnerability in protocol weakness, structural vulnerabilities on the Internet, programming errors, or use malicious code to cause psychological violence. Cyberspace structural violence is a necessary condition for the presence of personal cyber abuse.

7.0 References

[1*] Andy Greenberg, The WIRED Guide to Cyberwar, WIRED, accessed 14/9/19 (August 2019)*

[2] Steve Ranger, What is cyberwar? Everything you need to know about the frightening future of digital conflict, ZDNET, accessed 14/9/19 (December 2018)

[3] Chloe Albanesius, Cyberwar Is Here: Are You Ready?, accessed 25/9/19 (September 2019)

[4] Erendor, M., & Tamer, G.(2018) The new face of the War Cyber Warfare

[5] Robinson, M., &Janicke, H.(2014) Cyber warfare : Issues and challenges

[6] Sun Tzu, The Art of War, Shambhala Publications, 2005

[7] Anabelle Graham, The 5 most common cyber attacks in 2019, itgovernance, accessed 30/9/19 (May 2019)

[8] Josh Fruhlinger, What is a cyber attack? Recent examples show disturbing trends, CSO, accessed 1/10/19 (November 2018)

[9]https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf