International Communication: Cyber Warfare and Information Security

Zainab Suhail[1], Fatima Suhail[2]

AMCAP - Journal of Emerging Social Scientist
Vol. 01, No. 01, 15-25, January 2020
http://amcapjess.net/index.php/jess

[1] Practicing Lawyer, Pakistan.

[2] Researcher in the field of Communication Studies, Pakistan.

Abstract

The article aims to address the issue of cyber warfare and the emerging threat of information security of individuals as well as states after the inception of cyber-attacks. It has emerged to be paradoxical for countries who have denied the threat thereof. This article discusses types of cyber warfare and illustrates the dangers of these acts, especially in comparison with conventional or traditional means of war. This article further explores why opposing states engage in cyber warfare and how non-state actors use this for malicious and sinister purposes. The author critically examines existing laws relating to cyber warfare and analyses the impact of said laws on individual information security. New phenomena of information warfare relating to social media are also discussed, and the differences between cyber warfare and information warfare are highlighted. Finally, the author concludes by providing recommendations and solutions to the challenges discussed in this article.

Keywords: Cyber Warfare , Information Security , Laws , Information Warfare, Cyber Attacks

Introduction:

The 21st century has not only changed the political landscape of the world with the catastrophic happening of 9/11, but ubiquitously the world also saw the increase in the magnitude of another kind warfare known as cyber war. As in 2010 the first cyber-attack was initiated jointly by USA and Israel on nuclear vicinity of Iran which destroyed nearly thousand centrifuges. This attack aimed at Iran explicitly plunged the world in to an era of cyber warfare, where without any help of heavy artillery the adversary can incapacitate the other nation. As Gazula (2017) describes the cyber warfare as the form of the war which is not fought on lands with bombs and guns and instead of the standing armies with the help of simple computer and possession of enough computer knowledge the nations can be brought on the verge of bloody war. He also points out that in this age of code war no one is safe.

The incessant trend of cyber-attacks by states or non-state actors has made cyber warfare a hot topic. With the attainment of cyber arms the states are also making cyber security as their utmost priority (Cerny & Hurza, 2017)The threat of cyber warfare has also become concern of international organizations. As United Nations Institute for Disarmament Research (UNIDR)is not only making efforts to make existing laws applicable to cyber world but is also in effort to properly

define cyber warfare. As Melzer (2011) in UNIDR report on Cyber Warfare and International Law defines cyber warfare as a war which is fought in an intangible and unseen battlefield of cyberspace through cyber means and methods. Cyber space over here can be defined as an unseen and abstract location in which enormous number of website and databases exist or are present (Aderbigbe and Bello,2015). Oxford dictionary also defines cyber warfare in a brief and easy way. It elaborates cyber warfare as the usage of computer technology with aim to disrupt the activities of organization or deliberate attacking on computer for strategic and military purposes. In a same way Shanghai Corporation referred to cyber warfare as an attack which affects the "critical structures" such as public institutions and systems which may cause direct repercussions on the national integrity and security of a nation (Melzer, 2011).

Thus, the central point of all the definitions given above is the use of cyber arms in order to disrupt, steal and manipulate the important information present in a computer. This can be done by a state against another state or by non-state actors against organization, other state and individual. In this age of information technology where we are highly dependent on computers for storage of information and data our security undoubtedly is continuously at risk

Dangers of Cyber Warfare:

The latest report of World Economic Forum of 2018 declare cyber-attacks as the most likely attacks to occur even more than terrorist attack. The threat of cyber security has become so imminent that the, intelligence agencies, armed forces, and law enforcement agencies have made cyber security their utmost priority for investment and recruitment. As digital technologies are becoming sophisticated the battle ground of cyberspace is becoming more and more complex with the security of the individuals more on threat .Also refers to the February 2010 report by top American Lawmakers who notified that there is accelerating risk of cyber-attacks on computers and telecommunication. This report also pointed out that numerous key sectors of USA along with other nations are at the potential risk of cyber-attacks including cyber threats to public and private facilities, ,finances, transportation and , medical ,air traffic control systems and other several government functions (Aderbigbe and Bello, 2015). Cyber and network security, and cyber-attacks now actually pose grave and complex difficulties which have reached in to the new areas for public policy additionally also the national security. Computer networks and cyber space is a critical space which by every passing day is changing and has new developments in it. As many studies available also point out the dangers to which we can be exposed. As Lewis (2002) explicates these dangers in the form of an example that by taking control of the floodgates of the dams present in us for instance handling the 300,000 volts of electricity, the attacker or intruder can easily destroy the real world lives and properties with the aid of virtual tools he further called the cyber methods and technologies which can cause this type of massive destruction as Weapons of Mass Annoyance. Indubitably with massive scale of manufacturing and economic activity depending on computer networks and our financial transactions almost also digitalized .The dangers of cybercrime and industrial espionage are surely also hovering upon our heads. Meaningful steps are required to save ourselves from this danger. As in the year of 2000 at car manufacturing company Ford experienced a computer virus infecting 1000 computers. Ford also received 140,000 virus-contaminated e-mails within three hours before the complete shutdown of its network by hackers. To the worst the email service of the company was out of function for approximately a week. However, still with increased

incorporation of technology in our daily lives is also making us vulnerable to the cyber-attacks. As recent article published in the month of April 2020 titled Serious Cyber Security Flaws Uncovered in Ford and Volkswagen Cars revealed that the connected vehicles manufactured by Ford and Volkswagen have security flaws as these flaws easily allows the hacker to hack them.

Types of Cyber warfare:

According to Chatham House report of 2010 there are several forms of cyber warfare which clearly depict the challenges imposed to the security of personal or official data .The computers can be hacked and data can be extracted or accessed in extreme cases modified too. In adverse case scenario the user can be denied permission to their own data. Moreover the data can be used for propaganda or other malicious purposes. This simply portrays the fact that as much as the technology has proved to be fortunate for us. Upon falling in to the wrong hands it can threat us with dire repercussions too. Virtues of technology aside, with its day to day advancement and novellus nature the cyber security experts and relevant authorities should find methods to curb this insistent threat by suggesting new soft wares and programs with the help of which the security of every individual present in cyber space can be guaranteed. Some of the distinct types of cyber warfare which can be used by opponents against each other or can be launched by an individual in the fulfillment of nefarious purposes are given below:

This first is the espionage where **n**ow just by accessing the computer you can know the vital secrets and strategies of your opponent. Surely this is one of the biggest threat .As not only data can be accessed but it can be modified too. Governments worldwide complain publicly about the cyber espionage. Anonymous computer hackers on daily basis covertly and illegally copy vast quantities of computer data .The second is the propaganda where regardless of information true or not .It can be sent in the form of text or image anywhere in the world, even far behind enemy lines for malicious purposes or for causing agitation. Cyber propaganda also includes fake news which are present on Face book and Whats App. For instance the propagation of fake news on Whats App were responsible for lynching of Muslims in India in 2018. The third is named as the Denial of Service (DoS) which is a type of attack where legitimate user has denied access to his or her computer. It is the simplest type of hacking done now days. Here sometimes the hardware of user is also destroyed by inculcating virus in it. The space created by computer networks is difficult area to understand. As Crowell (2017) explains that cyber space is a complicated area of human activity that requires maneuvering via much of day to day life. The humans lives according to him are entwined with the fabric of cyberspace .It is the need of the hour that we comprehend the cyberspace, cyber events and possible risks. Furthermore, the understanding of future adversaries and their usage of malicious codes or software in to machines and soft wares.The imminent risks of future should be the topic of discussion too.

Reasons Of Why Cyber Warfare Is Preferable?

And Incidents of Breach of Information Security:

Assuredly, cyber warfare cannot replace the traditional form of warfare but it has become an important weapon in arsenals of many states for several reasons .First ,the cost and capacity for developing and maintaining cyber arm is much low in comparison to other forms of 21st century kinetic arms (Gazula,2017). Similarly Bello (2015) also states that the expense on cyber arms is not much as it only includes training and paying to cyber warriors and maintaining or purchasing,

hardware and software. Some of the reasons for the preference of cyber warfare are given below plus with the incidents as an example:

Vulnerability of Internet:

Sometimes, the imperfect designs of internet allow the hackers to secretly read and modify information stored on and also traveling between computers. Cyber attackers and hackers armed with incessant evolving malicious code are undoubtedly always ready to make their paths into computer networks (Petr HRUZA, 2017).It happens in the case of Equifax data breach which is given below:

Incident Of Equifax Data Breach:

Equifax , a credit reporting company which controls financial data of more than 800 million customers and 88 million businesses around the globe had to shut down its operations on 31st July 2017 , upon detection of malicious activities in its data .Later ,after the investigations it was revealed that company's portal application frame work was not up to date. And had security vulnerability which resulted in to massive data breach of 145.5 million users which counts as 45% of US population.(Richter, 2018).Thus with increase in the magnitude of technologies the new systems are necessary to be developed which ensure the security of people who are present in the virtual world.

Low cost and Loners as threats:

Another reason of commonality of cyber warfare is because of its low cost. Number of cyber warfare tools are openly available on multiple internet sites worldwide. .The inexpensiveness has allowed the loners sitting at home to carry out deadly attacks. (Bello O. A., 2015).

Hacked: Tumbler, My space and Linked in:

Anderton (2017) points out that even tech giants were also brought to knees by lone attackers the famous social media websites Tumbler, My space and Linked in were hacked in 2016. After investigations it was find out that 500 million passwords were stolen and sold on Dark web. The attack was launched by lone hacker going by the name of "Peace". The Peace also had 71 million twitter passwords for sale on dark web.

National Democratic Committee Email Breach:

Cyber attacks has also not left the world big super power when in 2016 the series of emails of Democratic National Committee were released .This is considered as a massive data breach which impacted the US elections 2016. As Anderton (2017) explained the incident .That the emails leaked showed that the Democratic party leadership had worked to sabotage the election campaign of Bernie Sanders. This caused huge havoc for Democratic Party especially near election. Two cyber-criminal groups known as Tzar team and fancy bear claimed the responsibility.

Anonymity:

Now a days, anonymity is the major concern of the global community .The advantage of anonymity provided by the cyber space is giving huge benefit and magnitude to criminal activities in cyber space. As Former U.S. Attorney General Janet Reno in 2000 pointed out that undoubtedly internet is making our lives easier but it also enormously provides new opportunities for criminal activities (Chawki, 2006). In case of cyber attack it is very precarious to know who launched an attack and this has become threat for the nations and also for the people on an individual level (Chawki,

2006).Below are the incidents given where the feature of hidden identity gave advantage to the perpetuators of attack:

Yahoo:

A data breach which affected, five millions user accounts present at Yahoo took place in 2016.User names ,passwords, date of births and phone numbers were all taken. Yahoo was again attacked in the same year .The data of1 million users was stolen this time. And the attacker is still unknown (Anderton,2017).

U.S Department of Justice:

A cyber-attack took place on US Department of Justice stealing the information of twenty thousand FBI employees the attack took place in 2016 and initiator of the attack is still unknown .While the method of attack is still a mystery and it is said that it took Department of Justice one week to realize about the information breach (Anderton,2017).

Vague Traditional Boundaries:

Due to increase of connectivity because of World Wide Web and social media. It has become an arduous job to determine and distinguish between foreign and domestic initiators of cyber warfare. It is an obvious fact that if we don't know who is attacking us, how possibly we can determine strategy to respond to the incident. Plus another problem over here is that countries are increasingly using this weapon against each other which is now creating a danger of new unseen war which can be more deadly than traditional warfare.

Stuxnet:

In 2010, Iran became first victim of cyber attack when its nuclear facility was attacked in Natanz .Afterwards the malware named as Stuxnet was find in computers of nuclear facility. According to cyber security firm Symantec this virus was very fast as it destroyed more than 1000 centrifuges of Iran (Paul Cornish D. L., 2010). The virus arrived in computers through USB stick which was inserted by someone in computers. The classified program for developing Stuxnet was started under Bush regime and was given the code name "Operation Olympic Games" (Sanger, 2012).The Israel was also involved in this attack. As the newspaper Telegraph reported in 2011 that Israel in 2011 indirectly acknowledged cyber attack when a video created to celebrate the retirement of Israeli Defense Forces head Gabi Ashkenzi listed Stuxnet as one of his successes.

Expanded Role For Perception Management:

Bello (2015) points out that he 24 hours availability has made cyber warfare an effective tool for communication, perception management and propagation of certain agenda. Now nations against each other have ability to use the efficient tools to manipulate the mind of the adversary nation or nations subordinate to it. In order to achieve their hidden motives or for maintaining their hegemonic role. Or domestically the data is also used by nations to set agenda of their own people or for maneuvering the choices and opinions of people

Cambridge Analytica

Cambridge Analytica the political consulting firm that did work for Trump in election campaign of 2016 used the data of 87 million people (Chang, 2018). It had obtained this data from Face book for research purposes. It is not a hidden fact that Face book is involved in the process of data mining and had sell data to the company. But Face book continuously denies the claim and says that data was taken by Cambridge Analytica by arranging a poll on Face book. Now question arises over here

is even if the Face book is not involved in such a massive data breach then how one of the biggest social platform guarantee the safety and privacy of its consumers.

Emerging Contemporary Phenomenon:

After the inception of social media the new dimensions and the latest tools for the controlling the cyber space have as emerged some of the contemporary phenomenon in this regard are given below

Surveillance Capitalism:

Friedman(2019) points towards the term Surveillance capitalism introduced by Harvard Business School professor Shoshana Zuboff's in her book, The Age of Surveillance Capital .In it Zuboff writes that it is of no doubt that human experiences are source or raw material through which their future behavior can be predicted. Further, she says that meager amount of this data is used for service improvement. While the rest of it is declared as a "proprietary behavioral surplus", which is fed into very latest "manufacturing processes" called as 'machine intelligence,' . This data in return is changed or fabricated into "prediction products" that tells what person will do now, sooner and later. And finally, these prediction products are also traded in to a new kind of marketplace that are called as behavioral futures markets.

Information Warfare:

On 31st Jan 2019 a column appeared in New York Times with the name of Imagining 'surveillance capitalism by Thomas L. Friedman .Here Friedman referred that recently the advances in artificial intelligence is taking the world deep into places and into powers where neither individuals nor the governments have experience to deal .The deep surveillance, deep facial and voice recognition is the information being gathered in the machines.

So what if these high tech machines are attacked and all information goes in to hands of people which can use this information and data for their rogue and malicious purposes. Or the question also arises that to what extent foreign governments and multi- national companies can control us on the basis of information which is easily sold by these data mining companies to them.

Faking The Entertainment:

The social media platform generate new quizzes and fun challenges for its customers on daily basis .Kate O Neil the author of book Connecting Human experience across physical and Digital Spaces in this regard pointed out that the recent 10 years challenge on Instagram in which millions of people took part unconsciously handed over their facial recognition data to Face book (Friedman, 2019).Thus Face book can mine this data and now it has the data of how you looked 10 years before and after 10 years and probably what you will look like in next ten years.

Shifting to Information Warfare And Features of Information Warfare:

With these emerging new trends, the world is shifting towards contemporary phenomena where information can be used as a tool to fight the wars.Information warfare is amalgamation of electronic and cyber warfare as well as psychological operations into a single fighting organization (Stupples, 2015) . Here information is used as a weapon to achieve competitive advantage over the opponent. Damjanović (2017) explains the feature of information warfare as at macro level in information warfare the forces sometimes with the help of cyber-attack gather information about their competitor in order to know their strategies and strengths and plan accordingly. At micro level private or public entities obtain information about their audience or people so that their opinion can be manoeuvred .Sometimes on the basis of the past experiences their future behaviour

can be predicted with the help this data. The countries against each other can obtain information and use this information for propaganda and other malicious purposes.

Difference Between Cyber Warfare And Information Warfare:

White (2019) Cyber warfare and information warfare are considered as same things but in reality there is a difference between them as illustrated in Table 1 given below:

Table 1:

Difference between cyber warfare and information warfare.

Cyber warfare	Information warfare
System attacks	Unauthorized access to obtain information
Denial of Service attack	Data theft
Computer viruses	Electronic surveillance
Disruption of system	Analysis of information
Cyber sabotage	Social media attacks to obtain data
Cyber terrorism	Use of cookies to obtain data

International Efforts:

In past steps were taken to gather the nations on one platform on this critical issue but it seemed like they were not willing to do so may be because of their hidden motives .Hathway (2012) states that in 1999, the United Nations in Geneva sponsored international meeting of experts . The purpose of the meeting was to better understand the repercussions of emerging digital technologies on information security. Then in 2002 another follow-up session of General Assembly also took place in which the technology able nations on one platform accepted the issue of information security .But nothing was done afterwards. Again in July 2010, the cyber security specialists from fifteen countries including major cyber powers like United States, China and Russia gathered at one platform of United Nations. And submitted the set of recommendations for cyber security of nations as well as information security of individuals. These recommendations were so vague that nothing could be done further (Hathway,2012).

No results despite of so many efforts actually states the fact that nations which have control and are more able in information technology are not willing to define or set parameters of cyber warfare and information warfare may be because of hidden motives.

Cyber Warfare: Existing International Laws:

Last year United Nations Secretary General Antonio Gutteres in a convention at Munich said that with emerging cyber technologies and risk of cyber warfare threatening the world we need laws to protect ourselves. He also pointed out that another problem we are facing is that we don't know that whether International Humanitarian Law or Geneva conventions apply to the cyber warfare (Filder,2018).Some of the existing international laws for traditional warfare which can be applied to cyber warfare (Melzer,2011) are given below:

Jus Ad Bellum:

Jus ad bellum actually means use of force . Article 51 of UN character refers to the "use of force". It actually gives state a full permission to use force and protect itself if its territorial integrity is in danger or its sovereignty is challenged.

Cyber Operations:

For cyber-attack there is no specific law given. But if one country breaches the privacy of another country in terms of cyber-attack .Then the other country can "use force" for its defense. And can also justify it under this use of force (Stupples,2015).The problem over here is that there is no certain definition that what is cyber-attack. And if the effected country takes help of use of force then what will be the criteria of use of force .Will it be armed conflict or cyber attack?(Melzer,2015).

Jus in Bello:

Sometimes also defined as the "law of armed conflict" .It applies in situations of armed conflict and mainly focuses on the security and protection of people during armed conflict

Cyberwarfare and Jus in bello:

Jus in bello states the conditions for the protection of people during traditional warfare. But nothing in Jus in Bello defines the laws of information security of an individual during the cyber conflict.

Imminent Risks, Problems and Steps:

Clearly in this world there always has been the division between the rich nations and the poor nations. Though the technology has grant us the new ways of learning and doing things. On the contrary it has created huge gap between technology rich nations and technology poor nations. The hindrance at the end of technology poor nations is that they are unable to protect themselves too from these imminent cyber-attacks For instance in case of data mining the technology rich nations which mostly possess all the populated social platforms have data of people which they can use and control to their advantage and exploit it for commercial purpose or in any way they want. The technology poor nations are not only exposed to the threat posed to them by technology rich nations. But the dangers constituted towards them by individual terrorist organizations which may be technologically able to jeopardize their systems and their citizens which are not safeguarded by the integrated abstruse and involute cyber security system.

With the evolution in the fields of technology and information at hand; the possible risks of cyber aggression which actually involves the efforts to destroy the due edifice of information and can also destroy the effective functioning of system related to economy and society. This is called as societal warfare (Mazarr et al, 2019).At micro level the individuals are not only facing privacy problems but there are some persistent risks which may be generated by their governments. For example now the governments having access to individual's social media accounts can be deny access to their accounts in case if they generate some material against the policies of the government. In this regard Mazzar et al (2019) also point out the conflict between networks will escalate. The nations will increase their virtual warfare capabilities against retaliations generated as a result of outsiders or inside actors. Thusly, the per se discussion point to the current threats which governments, individuals, organizations may face.

In future it seems like that the nations will depend more and more on information and technology systems. Surely demanding the up to the mark information security systems as well as security institutions equipped with latest knowledge for the due protection of these systems.

Indubitably the matters of national security with each passage of time will have ever increasing dependency on technology and strong and developed systems. Keeping this all in view the resilient and robust information security systems are needed but it seems like that the governments in per se matter will have huge dependency on the private companies as Mazzar et al (2019) also explicates that the line between the public and the private endeavors is increasingly blurring. The national security especially in terms of cyber security will depend on private actors rather than public investments. In addition to all of this, the literature in this terms of changing information environments and different forms of cyber threats and solutions towards this imminent threats are very few in numbers. The suppressing need of the hour is to invest in information landscape in the development of literature which can give broad view towards the ever changing landscape of information environment and its likely dimension, dynamics and the evolution which can aid the governments in taking the careful steps towards this pre destined warfare. Plus in this regard how populations can be educated in terms of the systems of information security and how they can also avoid manipulation or propaganda.

Recommendations:

In the light of the articles reviewed some recommendations in this regard which can be considered are that the technology able nations should come on one platform and design a proper framework in order to bring data mining companies under the constraint of laws in order to ensure the information security of individuals. Secondly, it is the need of the hour to differentiate between cyber war, cyber-attack, cyber terrorism and cyber criminality on an international level .So that laws can be designed according to these offences. Thirdly, the cyber force should be made in which representatives of all countries should be present .This force should be responsible for the risk detection in case of cyber offence by non-state actors And should be able enough to combat with it.On fourth the technology able nations should gather at one platform and should aid in designing of proper framework of laws through which the world can be plunged out from the threat of cyber warfare .While on the other hand the non-state actors carrying out malicious attack can be punished. Genuine treaties should be signed between countries in which the information security of people who are not engaged in cyber malpractices should be ensured. Lastly, the countries should also introduce strict laws in their countries in order to curb the menace of cyber-attacks.

Conclusion:

Cyber warfare is the biggest danger that the world is facing based on the recent cyber-attack incidents seen. It is not just the countries which can launch cyber-attacks against each other. Now non-state actors can also with the help of cyber arms are able to do anything for instance freezing our bank accounts stealing our information and using it for malicious purposes and destroying the GPS system etc. The threat of cyber warfare is undeniable it is the need of the hour to make laws .Especially after the emergence of social media the information security of states and personal information security of an individual's should be ensured. Otherwise, the nations are slowly reaching at the verge of bloody war which will destroy everything.

Albert Einstein said:

"I know not with what weapons World War III will be fought but World War IV will be fought with sticks and stones." (Flangan,2017)

References

Anderton, K.(2017, March 2017). *8 Major Cyber Attacks of 2016*. Retrieved from https://www.forbes.com/sites/kevinanderton/2017/03/29/8-major-cyber-attacks-of-2016- infographic/#1f2885ef48e3

Bello O. A., Aderbigbe F. M..(2015). Cyber warfare. The New Frontier of International War fare. *International Journal of Sustainable Development Research 1*(1),1-4, doi: 10.11648/j.ijsdr.20150101.11

Cornish, P., Livingstone, D., Clemente, D.,& Yorke, C. (2010). *On cyber warfare* (Report No 978 1 86203 243 9). London: Chatham House. https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf

Chawki, M. (2009). Anonymity in cyberspace: Finding the balance between privacy and security. *International Journal of Technology Transfer and Commercialization 9*(3).183-199. doi: 10.1504/IJTTC.2010.030209

Chang,A.(2018 ,May 2*).The Face book and Cambridge Analytica scandal, explained with a simple diagram*. Retrieved from https://www.vox.com/policy-andpolitics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

Cherneko, E., Demidov,O.,Luckynov,F. (2018, February 23) *Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms* .Retrieved from https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.

Crowell,R.M.(2017). Some Principles of Cyber Warfare Using Corbett to Understand War in the Early Twenty–First Century. Report No (19) The Corbett Center for Maritime Policy Studies. Retrieved from https://www.kcl.ac.uk/dsd/assets/corbett-paper-no19.pdf

Damjanović, D. Z. (2017).Types of information warfare and examples of malicious programs of information warfare. *Vojnotehni čki glasnik / military technical courier 66*(4).1045-1059. Retrieved from http://orcid.org/0000-0001-8169-4507

Friedman, T.L. .(2019, January 31).Imagining Surveillance Capitalism. *New York Times.* Retrieved from http://www.nytimes.com

Filder,D.(2018,March 15).*The UN Secretary-General's Call for Regulating Cyberwar Raises More Questions Than Answers*. Retrieved fromhttps://www.cfr.org/blog/un-secretary-generals-call-regulating-cyberwar-raises-more-questions-answers.

Flangan,M.(2017, April 27). *World War IV will be fought with sticks and stones.* Retrieved from https://www.smh.com.au/opinion/world-war-iv-will-be-fought-with-sticks-and-stones-20170421-gvpafh.html

Gazula, M. B. (2017). *Cyber warfare conflict analysis and case studies* (Doctoral dissertation, Massachusetts Institute of Technology. Massachusetts. Retrieved from http://web.mit.edu.

Hruza, P., & Cerny, J. (2017). Cyber warfare. *International Conference Knowledge based organization23*(1).155-159. doi: 10.1515/kbo-2017-0024

Mazzar,J.M, Bauer.R, Casey.A, and Matthew.J.L, (2019).The Emerging Risk of Virtual Societal Warfare. Social Manipulation in a Changing Information Environment. Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org.

Lewis,A.J.(2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies. Retrieved from https://csis-website prod.s3.amazonaws.com/

Ritcher, W.(2018 ,July 24*). Results Are In: How Americans Faced the Equifax Hack where Personal Data of 45% of US Adults Were Stolen*.. Retrieved from https://wolfstreet.com/2018/07/24/how-americans-faced-equifax-hack/

Stupples,D. (2015 ,December 03*).What is information warfare?*. Retrieved from https://www.weforum.org/agenda/2015/12/what-is-information-warfare/

Serious Cyber Security Flaws uncovered in Fords and Volkswagen Cars.(2020, April 9).[Blog Post]. Retrieved from https://eandt.theiet.org/content/articles/2020/04/serious-cyber-security-flaws-uncovered-in-ford-and-volkswagen-cars-that-could-endanger-drivers/

White, R. (2018, February 20). The Differences Between Cyber and Information Warfare [Blog post]. Retrieved from https://blog.cybersecuritylaw.us/2018/02/20/the-difference-between-cyber-and-information-warfare/