OIC-CERT Journal of Cyber Security
Volume 3, Issue 1 (April 2021)
7 - 20

The Integration of Cyber Warfare and Information Warfare

Noor Azwa Azreen Binti Dato' Abd. Aziz[1], Engku Azlan Bin Engku Habib[2], and Madihah Mohd Saudi[3]
[1,2]CyberSecurity Malaysia, Selangor Darul Ehsan, Malaysia
[3]CyberSecurity & Systems(CSS) Unit, Universiti Sains Islam Malaysia(USIM)
[1]azreen@cybersecurity.my, [2]azlan@cybersecurity.my, [3]madihah@usim.edu.my

ARTICLE INFO

Article History
Received 20 Mar 2020
Received in revised form 25 Jan 2021
Accepted 08 Mar 2021

Keywords:
Cyber Warfare, Information Warfare, Cybersecurity, Warfare, Cyberspace.

ABSTRACT

Throughout the years, the appearance of cyber warfare and information warfare have changed and enhanced the methods, techniques, as well as the tools strategically, in the information and cyber warfare domain. Many researchers have highlighted the misinterpretation and use of the term cyber warfare and information warfare interchangeably. This paper will first define and differentiate the differences between cyber warfare and information warfare. Then it will discuss the connection and the integration of this two warfare. Cyber warfare and information warfare have its challenges and posed threats to nation-states and the world. Knowledge and skills identified in information and cyber warfare will be discussed in this paper. In this regard, this paper will also discuss physical security and cybersecurity measures in addressing the threats posed by these warfare in this modern age.

I. INTRODUCTION

In this day and age, warfare does not only encompass the physical domain in areas of land, water, air, and space. Most countries around the globe are aware of the fifth domain, which is the cyberspace in their warfare doctrine and operations. This includes warfare attacks against a nation-state, destroying one's critical communication channels, information systems infrastructure, and assets. Furthermore, in this complex world, physical and cyber warfare alone are insufficient. According to the 2019 Cyber Threat Outlook by Booz Allen, information warfare is one of the top cyber threats in 2019. Information warfare activities include an extensive range of tactics such as deception, spreading propaganda, and disinformation that are very important in warfare strategies. Information

ISSN 2636-9680
eISSN 2682-9266

warfare involve not only nation-states but individuals and organizations. Thus far, most countries only used information warfare for political and military purposes such as pushing voters' decisions on their votes and fuelling cultural conflicts [1]. However, that might change soon due to the complexity of today's environment.

II. THE SUBSTANTIAL DIFFERENCE BETWEEN CYBER WARFARE AND INFORMATION WARFARE

The idea and concept of cyber warfare are still new. The growth, commercialization, and high dependence of the internet and digital technology have boomed in the last two to three decades. Cyber warfare is politically motivated. It is an Internet-based conflict that involves attacks on a target's information and system [5]. Another literature written by Peifer, Kenneth V. (1997) defines cyber warfare as "attacking and defending information and computer networks in the cyberspace, as well as denying an adversary's ability to do the same." Cyber warfare activities are all about but not limited to denial-of-service attacks (DoS), attacks on systems, malware attacks, ransomware attacks, system disruption, cyber sabotage, cyber terrorism, and attacks on the Critical National Information Infrastructure (CNII). Actors of cyber warfare can be nation-state, terrorist organization, criminal groups, etc. Actors are capable of carrying out cyber warfare attacks such as [6]:

i. Disrupting the telephone networks.
ii. Using logic bombs. A logic bomb is a malicious program that is set to be activated when a logical condition is met, on a certain time, date or after several transactions have been processed. The program can put the stock markets on a halt and destroy records of any transactions and money can be stolen by breaching the networks.
iii. Attacking a country's power grids, which eventually will cause local dan regional blackouts. This had happened to countries such as Ukraine, Russia, Venezuela, etc.
iv. Causing malfunction and disabling computer systems, onboard avionic computers, or an aeroplane causing it to crash or collide.
v. Misrouting trains causing train crashes and collisions.
vi. Stealing of cryptocurrency or blockchain.

Cyber warfare cannot be separated or isolated from information security. To an organization and nation-state, information is the most valuable asset as it worth a lot of money. Thus, information security is essential and needs to be the top priority of an organization. Without information security, there will be a risk of vulnerabilities and possible threats and attacks to an organization. In general, information is always targeted for manipulation, deception, and espionage in information warfare.

Information warfare is not a new concept. Britain has manipulated information to change American's opinion in 1917 and 1941 to engage in wars with Germany. On the other hand, in Germany, Paul Joseph Goebbels, known as The Minister of Propaganda, took over the national propaganda machinery that was responsible for creating the right image of the Nazi regime to its masses, which is the German citizens (Britannica). He continually makes press statements via the press and over the radio. He keeps raising hope to the masses, mentioning, and conjuring past events in history, as well as referring to some secret miracle weapons that the Nazis have in their grasp.

Both the United States (US) and the Soviet Union have been using broadcasting, the use of covert organizations and funds in their operations in order to intervene with other countries' election during the Cold War [12]. Before the Internet exists, information warfare operations cost a lot of money due to training and movement of spies across borders. Nation-state at that time needs to establish foreign bank accounts and transfer of cash. In the present day, a nation-state remotely achieves a similar outcome at a lower cost. Rather than sending human agents, spyware and other internet tools are used to acquire, alter, and manipulate information across the globe. Funds can be transferred using cryptocurrency, which is harder to detect especially if it uses the tumbling services. Hence, technology and cyberspace easily execute information warfare operations faster, with less cost and low risk.

According to the US Department of Defence, information warfare is "an information-based attack that includes any unauthorized attempt to copy data, or directly alter data or instructions." In a wider perspective, information warfare is not just about the involvement of computers and computer networks [17]. It is much bigger than that. The operation may involve different types of information transfer transmitted through any media which include the operations against information content, its supporting systems, as well as software. In addition, information warfare can involve physical hardware devices that stores the data, human habits, and practices as well as perceptions. This proves that the informational environment is brutal and war on itself.

According to the Joint Chiefs of Staff, information operations, which is also known as influence operations, is defined as the cohesive integration practice and engagement in the computer network operations, electronic warfare, psychological operations, military deception as well as the operation security. In information operation, tactical information regarding the adversaries is compiled and analysed. Furthermore, it is also used to create and disseminate propaganda in order to get a competitive advantage over the adversaries, competitors, or oppositions. There are three components to the information environment, which are the informational aspects, the physical

ISSN 2636-9680
eISSN 2682-9266

aspects, and the cognitive aspects of the environment [13].

- Physical environment aspect is where the individuals, organizations, information systems, and the physically connected networks reside.
- Cognitive environment aspect includes individual and collective consciousness, which information is used, and perception and decision are made.
- Information environment aspect is the intersection of the physical and cognitive domains which information content and flow exist, and a medium which information is collected, processed, and disseminated.

Information warfare activities are all about, but not limited to, psychological warfare, data and identity theft, electronic surveillance, intelligence analysis, public diplomacy, deception, disinformation, espionage, cyberbullying, and social media attacks. Using the social media to spread misinformation, can damage an organisation's reputation or scrutinising and slandering government institutions and their policies. Social media can play the role to confuse the public, make the truth obscure and attack individuals, politicians, and organizations[1]. Information warfare via the social media confuses people and eventually disrupt social harmony and democracy. It will impact the country's national security negatively. [5].

It is stated that the Russians are very skilful and the masters of information warfare ever since Stalin's Rule of Supremacy. Stalin's administration was very skilled in photo manipulation even before Photoshop existed. Stalin and his administration were notorious in rewriting the truth or even history through photographs. The Soviet photo engineers changed and erased faces of revolutionaries, enemies of the state, and other unwanted faces from official photographs so that it would not be recorded in history.

Stalin was famous for his Order 227 statement, which causes fear among the masses. Fear is considered a part of the information warfare. The contents of Order 227 circulated verbally to every single person in the army. The contents are required to be understood and memorised. Stalin, through Order 227, demanded and ordered that every officer, soldier, and political aides to understand that their resources are limitless, to fight until his/her death, and never to retreat. Cowards are unforgiven and were punished severely or even put to death. The laggards or deserters were drawn aside and shot without any reflection or remorse. Dr Martin Libicki in his seven forms of information warfare (shown in Table. 1) described that this kind of warfare contains the element of psychological structure in instilling fear to the troops. However, the elements of Order 227 have affected Stalin's troops rather than the opposing force.

TABLE 1: L Libicki's Seven Forms of Information Warfare

Form	Description
Command-and-control	Disrupting the command effectiveness by attacking the command centres and the people in charge.
Intelligence-based	Reducing the opponent's knowledge and awareness by increasing and equipping your own.
Electronic	Using cryptography and other tools to disrupt or halt the physical platform from transferring information such as network jamming.
Psychological	To play with the human mind and emotions. Can be used to demoralize or influence others.
Hacker	A hacker is a person that exploits the weaknesses and vulnerabilities of a network and computer systems. They find ways to breach security defences.
Economic information	In possession and in control of very important information which can lead to obtaining power.
Cyber	It can be a semantic attack, information terrorism, simulate-warfare, Gibson-warfare, etc.

Since then, Russia still has not lost its touch in information warfare. One of the recent information warfare incidents that involve Russia is about the 13 Russian officials who were caught meddling in the 2016 US Presidential election. They were charged on account of the conspiracy to deceive the US by ruining the functions of the Federal Election Commission, the US Department of Justice, and the US Department of State. They were charged with schemes to commit bank fraud, wired fraud, and aggravated identify theft (BBC News, 2018).

Another incident that has happened was the cyber warfare and information warfare activities against Ukraine by Russia. Russia has several times attacked Ukraine's cyberspace, which includes attacks on its electricity grid, electronic billboard hack, influence their election and the integrity of their data [3] Russia tended to manipulate and fabricate stories and information to shock and caused international dialogue to be put into a halt.

The physical and cyber warfare increased due to global connectivity. Unlike any other nation-states, Russia sees the importance and the impact of information warfare, and they are very active in creating and spreading inflammatory rumours and exaggerate stories via the internet. This has caused a lot of problems for the US, NATO, and the EU. Russia tends to undermine the official version of events by using statements such as "Russia is a misunderstood and misjudged superpower and a necessary counterweight to Western liberal values. On the other hand, it is said that the western countries have experienced a deterioration of their 'traditional values' and has been hypocritical in their views and decisions in the international arena. As a result, Western philosophy, systems, and actions should not be trusted." This is the perfect example of how information warfare is played in cyberspace.

ISSN 2636-9680
eISSN 2682-9266

Alternatively, at the end of 2018, Reuters reported that the Russian Internet search company Yandex was hacked by hackers working from Western intelligence. The hacker covertly maintains access to Yandex for at least several weeks without being detected. A rare type of malware called Regin was used to spy on the user accounts. Its architecture, complexity, and capability are on another level of advancement. Regin is known to be used by the "Five Eyes," an intelligence-sharing alliance consists of countries from the US, Canada, Britain, Australia, and New Zealand. However, the intelligence agencies from these countries have refused to comment on the alliance. Yandex informed that the attack was fully neutralized before any damage is done, and no user data was compromised.

Other than Russia and the US, China has been seen investing more of their time, money and focus, on cyber and information operations, in conducting cyber espionage for political and economic purposes. China mostly targeted the US financial reserve and its defence industrial base. China wants to close the gap in knowledge, skills, and capability with its number one military rival.

III. THE INTEGRATION OF CYBER WARFARE AND INFORMATION WARFARE

Most countries see cyber warfare as a section of information warfare. However, in this technological age, whereby technology, as well as devices, are complex, sophisticated, and interconnected, the aspect of cyber is considered an essential tool in carrying out tasks including information warfare operations. Countries are now seeing cybersecurity as a critical issue. They are now setting up cyber commands and have developed or is currently developing national cybersecurity strategies to deal with the emerging cyber threats [5]. A US Intelligence report in January 2017 suggests that 30 nation-states are developing cyber offensive capabilities. This reveals that cyber warfare and the cyber-arm race have already started to take root and will develop into something even bigger and dangerous [14].

However, having skills in weaponry, fighting, and cyber-attack capabilities are not enough in war situations. Perception management in information warfare is essential as the arms of war. Perception determines actors' decisions and the next course of actions, especially on the battleground. In this digital age, the public and the people worldwide are being sucked in and involved in the battleground. The society involvement in the battlefield is made clear and demonstrated during significant incidents such as the 'Arab Spring' demonstration in Arab countries and the 'Jasmine Protest' in China.

Another term for information warfare is information operations. The military uses the term as a tool for falsifying perception, and it is an integral part of cyber warfare. In cyber warfare, information is used for disseminating and spreading real and fake information. The military is able

to deny or stop access to information. Disinformation and fake news campaigns, as well as propaganda, can be used to deceive the enemy. It can influence public perception and trick them into believing or not believing a piece of information.

The rise and strong presence of the mass media have made governments realize the importance of perception management. Due to the advancement of the internet and digital technology, people are given opportunities to become actors, producers, and involved in information war via social media. The information spreads rapidly and sporadically than wild forest fires in this digital age.

In 2014, some intelligence groups acquire and even manipulate information via the internet. Other than affecting public opinion, information warfare has distorted information and make people believe what they want to believe. This information manipulation shows that there are high levels of decision making involved in the political arena. The manipulation of information and perception is already a lot and embedded in the cyber espionage, intelligence, and military operations, as well as destructive or disruptive cyber operations. The cyberwar information domain is significant for an organization or nation progress forward and achieve its goals [2].

Cyber warfare can be seen as defensive and offensive warfare. An effective cyber defence will be able to protect the network systems against cyber threats such as Denial of Service (DoS) attack, illegal access, cyber intrusion, network modification, or even jamming. It provides access to information, detects and identify the information systems, vulnerabilities and threats. It ensures that there will be an efficient use of the systems with less interference and disruption [2].

On the other hand, there are two functions of offensive cyber warfare. First is to identify, detect, manipulate, and affect an information system. Second is to disrupt or destroy the webbed information systems of adversaries. The attacker's process is reconnaissance, scanning, gaining access, maintaining access, and clearing tracks. With their knowledge, skills, and perseverance, they are able to conduct signal jamming, misguiding information and malware, to alter, manipulate or wipe out important and confidential data of the opponent. They are able to congest the system with misguiding information [2].

Recently, information warfare capabilities are more intense and widely used. Yet, cyber warfare is not merely a tool or a mode of executing information warfare, it is considered the primary mechanism to enhance information warfare manoeuvres. Attacks become more efficient, specific, faster to execute, in-depth, broader usage, and directly interconnected than in the past. Recently, there is a new information warfare on cyber warfare strategy, which involves hacking of the knowledge infrastructure (KI). For example, the spread of scandals, fake news and causing problems to an election-day logistics which puts the KI at risk. Some areas of concern on hacking knowledge infrastructure are in politics, finance, engineering,

ISSN 2636-9680
eISSN 2682-9266

medicine, education, law, and entertainment [10].

Cyber-physical information infrastructure (CPII) has become a new target of cybercriminals. It involves heavily on the command and control of physical infrastructure. The critical national information infrastructures (CNII) sectors such as in Malaysia consist of Government service, defence and security, health service, emergency service, energy, water, banking and finance, food and agriculture, transportation, and information and communication, are frequent targets of cyber-attacks.

Following the targets of national knowledge industries, other targets that might be involved are institutions industries including education, engineering, surveillance, monitoring, investment, advertising, entertainment, and law. Knowledge hacking has progressed tremendously through time due to access and pathways that are easy to manage, and perimeters that can be breached.

Information warfare on cyber warfare is made possible by surrendering and ignoring the check and balance or counterbalance to the cyberspace ecosystem and conveniences. This shows that information warfare is trading security with convenience and not the other way around. The future of information warfare will consist of the combination of net warfare, electronic warfare, cyber warfare, and psychological operations. It will be widely used for offence attack and defence.

The combination of information warfare and cyber warfare use the ICT infrastructure to enhance and accelerate the movement of information. It will cover a wide range of audiences and with a significant impact on a nation-state or organization. Speakers or voice recordings are used in public or military operations to send or circulate a message more quickly and efficiently to the enemy combatants. The records usually aim to distract, confuse, and even anger the enemy combatants.

Another brilliant strategy that combines both the warfare is the use of social networks and targeted e-mail. These channels provide propagation of false information and disinformation by ambiguous people or false authority. The information does not need to be a total lie or part lie, as long as they can put a spin on the information and is able to distract the audience from the absolute truth.

Deception in terms of targets and sources can be used extensively via ICT. It speeds up the decision-making process and automates its consequences. Cyber warfare allows massive investigation on specific information such as a dossier on incidents, events, tendencies, and personalities needed to launch a successful information warfare operation. This is not always a contributing factor, but it can lead to a highly predictable response from the target population.

IV. CYBERSECURITY IN CYBER WARFARE AND INFORMATION WARFARE

It is indisputable that the world has its focus on cyber warfare and information warfare. Countries such as the US, the United Kingdom (UK), China, South Korea and Australia NATO have set up dedicated cyber-security centres to conduct these operations.

Cybersecurity experts in Malaysia have urged authorities to take cybersecurity and cyber warfare more seriously. Combating cyber threats and cyber attacks from nation-states can be very challenging. This is because some of these nation-states have no budgetary constraints in their cyber and information warfare operations.

An example of a state-sponsored cyber-attacks is an Advanced Persistent Threats (APTs) attack. APTs usually refer to cyber attack campaign that uses sophisticated hacking attempts. These attacks are usually persistent, continuously ongoing, and usually targeting an individual, organisation, or country. Their motivation varies from monetary, to cyber espionage, to obtain confidential data or even to spread misinformation, confusion, and chaos.

For instance, hackers from North Korea are more sophisticated as that are equipped with a wide range of knowledge and skills to conduct DoS, data theft, malware/ransomware attack and cyber espionage. The infamous 2016 $81 million cyber heists on the Bangladesh Central Bank were said to have been done by the North Korean hacking group, Lazarus. Hacking has become a handy tool for countries such as North Korea to acquire money and evade sanctions. This is especially useful when the sales of weapons and counterfeit notes are obstructed due to international restrictions.

However, APT attacks are not only executed by nation-states but also organisation or groups. The Carbanak syndicate has attacked banking, retail, hospitality, and other industry to obtain and collect financial information of the targets. The syndicate uses APT-style tactics to compromise their targets. Carbanak was able to employ and engage a commodity or leaked tools so that they are able to stop the abilities of the network defenders' in identifying the Carbanak intrusions. So far, the syndicate is recorded to have stolen $1 billion from banks and other industries.

It is crucial to have a holistic and adaptive approach that identifies potential threats to organizations and impacts on national security and public well-being. Nation-states should look at the overall people, process, and technology of an organization and the nation-state. In addition, valuable data and information need to be protected by security with series layers of defence mechanism. This multi-layered approach helps to raise the security system from many different attack vectors.

It is essential to develop nations to become cyber reliance and to gain the capabilities to safeguard the interests of its reputation, image, brands, its stakeholders, and their value-creating activities. Nation-states should

ISSN 2636-9680
eISSN 2682-9266

implement a more proactive, dynamic, and integrated cybersecurity approach.

People are the weakest link in cybersecurity. Hence, there are two critical aspects of improvement to consider. First, everyone needs to be fully aware of their roles and functions in preventing and reducing cyber threats and cyber attacks. It is imperative to protect cybersecurity issues, risk, and gaps in the organization. Everyone has their responsibilities and roles in securing data and system in the organization. People need to realize that they cannot rely 100 per cent on security devices to prevent cyber attacks. Vulnerability and risk can happen due to human weaknesses. This can be from internal and external threats. Therefore, security awareness and training for employees must be one of the elements for improving cybersecurity in an organization. An effective security awareness program can reduce the risk of cyber threats that are aimed at exploiting people [6].

Second, the organization must recruit staffs specialized in cybersecurity. They continuously need to be well informed, updated with the latest knowledge, trends, skills, and qualifications to ensure appropriate controls, technologies, and best practices are implemented in order to handle current and upcoming cyber threats. All other employees must have knowledge on security, such as organization security policies, best practices in safety, guidelines, incident response and responsibility. Cyber resilience should be practiced throughout the organization. When security is in everybody's mindset, the whole organization can predict, prevent, detect, and respond to the cyber-attacks.

Simulated cyber attack drill needs to be conducted annually or when needed. The drill needs to use the current potential cyber threats and cyber attacks. This is to create awareness and educate its employees with the anatomy of the attacks, to react according to Standard Operation Procedure (SOP) upon encounter. Time to time, cyber attack simulation or cyber drill on cyber attacks such as phishing, will minimize security risk in an organization.

Then there is the process. It is important to implement an effective cybersecurity strategy to identify ways organization’s activities, roles, and documentation are used to mitigate risks to the organization’s information. Due to drastic changes in cyber threats, the organisation needs to adapt and revise the processes timely. If people do not comply with the policies and processes, the organization is deemed inefficient.

It is important for organizations to prepare documented policy, processes, and procedures for their staff’s reference, handbook, knowledge, and awareness in handling vulnerabilities, threats, securing data, and cybersecurity. The policies must be in line with the standards and regulations that are currently implemented in the organization. These policies should comprise provisions related to internal and external workers. The workers are organisation staff, vendors, partners,

clients, stakeholders, and customers. The organisation must also regularly review and amend the documentation, guidelines, policies, and strategies such as the Risk Management Plan, Disaster Recovery Plan, and Business Continuity Management Plan to ensure the Cyber Security Life Cycles (Identity, Protect, Detect, Respond, Recover) are correctly implemented. Implementation of ISO/IEC 27001 in critical departments or units is highly advisable to implant the security mindset as daily routine and behaviour of the employees.

The business process in a cyber enabled space and technology is very important in order to tackle the risks and threats that occur in cyberspace. First, an organisation must identify their cyber risks, controls, and technologies needed. Technology is crucial to prevent, protect, or even reduce the impact of cyber risks depending on the organisation's risk assessment according to an acceptable level of risk. Following are several examples of using Technology to manage cybersecurity:

i. Update software and hardware regularly.
ii. Remove unnecessary services and accounts.
iii. Enhance network security.
iv. Use encryption where necessary.
v. Update anti-virus programs.
vi. Identify existing risks and test controls.

Organizations must consistently identify and address risk through independent risk analysis and conduct security assessments as well as vulnerability testing to stop cyber-attacks. When an anomaly or weakness is detected, the system will raise a red flag. The details of the red flag are then shared with the relevant sectors. If the organisation's system network and technology are properly maintained, the usage of information security controls are able to assist in identifying required protection for the task at hand.

In today's complex digital age, cyber threat takes place across multiple layers. This is called defence in depth. Each layers of the organisation must have their own security defence and measures in order to cover all vulnerabilities. If they are not able to completely stop the attack, at least they are able to slow down attacks before damage is done. It is important for an organization to determine its critical assets, identify any vulnerabilities, and design security in their organization to prevent attacks and detect any breaches. The defence layers are physical, network, host, data, application, business process and organization strategy, and direction (as shown in Fig. 1).

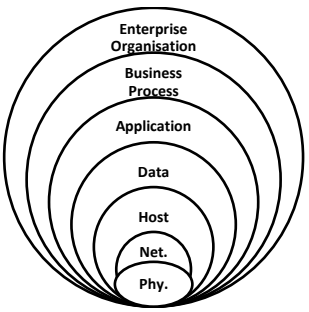

Fig. 1: Defence in Depth

In terms of managing and securing data, the government and organization need to implement confidentiality,

ISSN 2636-9680
eISSN 2682-9266

integrity, and availability in their documentation (CIA). Confidentiality limits access to information. The levels of confidentiality can be Top Secret, Secret, Confidential, Restricted, and Public. Meanwhile, integrity is to make sure that information at hand is accurate and has not been altered by any mean possible. Lastly is availability, which guarantees that relevant information or document are made available to authorized personnel.

Authentication is a method to authenticate a process to recognize and verify valid users or processes. It manages the information users or processes are allowed to access in the system. Whereas non-repudiation is the transparency and assurance that the information exchanges or any transaction may be trusted. It ensures that a party or a communication cannot deny the authenticity of their signature on information, document, or transaction.

Encryption is eminent and crucial to secure data. Encryption is installed and used in devices, computers, file servers, and across networks to assure the privacy of sensitive government, business, and personal information. Encryption technology is now a fundamental enabler for information assurance. It is available in the commercial marketplace throughout the world.

In addressing information warfare, the nation-state needs active transparency in its policies, capabilities, and activities. Transparency is considered a vital component for building trust and confidence between states bilaterally, regionally, and globally. Nevertheless, transparency is not the main aim, yet a toll for promoting further discussion on specific issues of national and international importance.

V. CONCLUSION

The threat of cyber warfare and information warfare is real and needs to be taken seriously. This situation worsens with the rapid spread of information technology, digital technology, and know-how, especially when both integrate or converge with each other. As more computers and devices are connected to networks for increased connectivity, vulnerability increased.

Through information technology advancement, the purpose of data based war in military activities will continue to develop, increase and in time evolve. However, it is a disadvantage to the less advanced nations. Most developed countries will take advantage of the less developed nation which impacted the loss of data, sovereignty, and system control.

This paper aims to provide a better understanding on the differences between information warfare and cyber warfare. It reveals the evolution of technology whereby information warfare and cyber warfare are linked to each other and utilized by nation-states to create a significant impact.

Nation-states and organizations need to develop a holistic and adaptive approach to prevent cyber

threats in cyber warfare and information warfare situations. Other than that, organizations need to implement multi-layered defence and implement innovative, dynamic, and knowledgeable cybersecurity approach against advanced cyber threats.

VI. ACKNOWLEDGEMENT

We like to express our appreciation to Col. Ts. Sazali Bin Sukardi (Retired), Senior Vice President, Strategic Research Division, CyberSecurity Malaysia for his pearl of wisdom and invaluable guidance in completing this conference paper. He is an expert in his field, which is cybersecurity and cyber warfare.

VII. REFERENCES

[1] B. Allen, "2019 Cyber Threat", Outlook. Booz Allen Hamilton Inc.", Washington D.C., 2019.

[2] J. Andreas, and S. Winterfeld, "Cyber Warfare (Second Edition)". Syngress, Elsevier, Amsterdam, 2013.

[3] M. Baezner, "Hotspot Analysis: Cyber and Information Warfare in the Ukrainian Conflict", Centre for Security Studies, ETH Zurich, 2018.

[4] J. Bourque, "Electromagnetic Spectrum Operations, An Approach to the Universal Maneuver Domain", CHIPS The Department of the Navy's Information Technology Magazine October-December 2014 [Online] http://www.doncio.navy.mil/CHIPS/ArticleDetails.apx?id=5572 [Accessed: 22-May-2020].

[5] Essays, UK. "Cyber Warfare Examples Essay", November 2018 [Online], https://www.ukessays.com/essays/information-technology/examples-of-cyber-warfare-information-technology-essay.php?vref=1 [Assessed: 22-May-2020].

[6] Global Information Assurance Certification Paper, "Information Warfare: Cyber Warfare is future warfare", SANS Institute, 2004.

[7] P. Hälsig, "Measures to prevent cyber warfare and information warfare", Model United Nations International School of The Hague, Munish, 2013.

[8] P. Han-na, "North Korea-backed hackers intensify information warfare, financial theft", The Korea Herald, 2019 [Online] http://www.koreaherald.com/view.php?ud=20190326000616 [Assessed: 27 June 2019].

[9] D.B. Johnson, "How China uses cyber theft and information warfare", 2019 [Online] https://fcw.com/articles/2019/05/06/china-information-warfare-dod-report.aspx [Assessed: 24 May 2019].

[10] R. Loui and W. Hope, Information Warfare Amplified by Cyberwarfare and Hacking the National Knowledge Infrastructure. IEEE Computer Society, 2017.

[11] Mitre, Lazarus Group. [Online] Retrieved https://attack.mitre.org/groups/G0032/, [Assessed: 27 June 2019].

[12] J. Nye, "Protecting Democracy in an Era of Cyber Information Warfare", 2018, https://www.hoover.org/research/protecting-democracy-era-cyber-information-war, [Assessed: 22 May 2019].

ISSN 2636-9680
eISSN 2682-9266

[13] I.R. Porche, C. Paul, M. York, C.C. Serena, J.M. Sollinger, E. Axelband, E.Y. Min, and B. J. Held, "Redefining Information Warfare Boundaries for an Army in the Wireless World", Rand Corporation, California, 2013.

[14] S. Ranger, "What is cyberwar? Everything you need to know about the frightening future of digital conflict", 2018, [Online] https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/, [Assessed: 27 May 2018].

[15] M. Robinson, K. Jones and H. Janicke, Libicki's table reference: Cyber Warfare: Issues and Challenges, 2015, [Online] https://www.researchgate.net/publication/276248097_Cyber_warfare_Issues_and_challenges, [Assessed: 28 September 2019].

[16] W. Snyder, The Difference Between Cyber and Information Warfare, 2018, https://blog.cybersecuritylaw.us/2018/02/20/the-difference-between-cyber-and-information-warfare/, [Assessed: 21 May 2019].

[17] S. Wilson, Information Warfare and Cyberwar: Capabilities and Related Policy Issues. Report for Congress, The Library of Congress, Washington D.C., 2013.