Cyberwarfare and its Effects on Critical Infrastructure

Humairaa Yacoob Bhaiyat and Siphesihle Philezwini Sithungu
Academy of Computer Science and Software Engineering, Faculty of Science, University of Johannesburg, South Africa
humairaabhaiyat@gmail.com
siphesihles@uj.ac.za

Abstract: The growth and capabilities of cyberspace have brought about many advantages to societies. Individuals and businesses have used cyberspace for easier communication, but nation-states also utilise it to improve the functioning of their critical infrastructure. Critical infrastructures provide vital services such as the health, safety and security needed for the efficient functioning of societies. However, vulnerabilities in cyberspace have made cyberattacks such as cyberwarfare possible. Cyberwarfare is an international concern due to the negative impact it can have on critical infrastructure. This paper aims to discuss cyberwarfare and the potential effects that it can have on critical infrastructure. This paper follows a theoretical research methodology to provide an understanding of cyberwarfare. In addition, the paper provides a better understanding of the impact that cyberwarfare can have on critical infrastructure. The paper contains an exhaustive definition of cyberwarfare. Since cyberwarfare is a type of cyberattack, it is similar but not the same as other cyberattacks such as cybercrime and cyberterrorism. Therefore, to gain a clear understanding of cyberwarfare, the paper discusses cyberwarfare, cybercrime, and cyberterrorism. The paper also discusses some of the most significant cyberwarfare incidents. Since the effects can be devastating, critical infrastructure must be protected from cyberwarfare. A survey of techniques for protecting critical infrastructure from cyberwarfare is presented. The identified incidents highlight the effects that cyberwarfare can cause. Hence, the possible effects that cyberwarfare can cause on critical infrastructure is discussed. Due to the negative effects of cyberwarfare, nations need to be prepared to protect their critical infrastructure from cyberwarfare. Therefore, the paper also discusses the authors' stance on South Africa preparedness to defend themselves in the event of cyberwarfare.

Keywords: cyberattack, cyberwarfare, critical infrastructure, critical information infrastructure, effects, SCADA systems

1. Introduction

Developments in Information and Communication Technologies (ICT) has led to adverse consequences within cyberspace (Izycki & Vianna, 2021). Cyberwarfare has utilised cyberspace to conduct attacks whose effects are felt both in cyberspace and the physical world (Almeida, Doneda & de Souza Abreu, 2017). The effects of cyberwarfare are highly detrimental to the Critical Infrastructure (CI) of a nation. Incidents of cyberwarfare have already occurred in states such as Russia, Iran, and the United States. Therefore, techniques to protect against such cyberwarfare incidents are vital. Countries such as Russia, Iran, North Korea, and Israel have already started preparing to protect themselves from such incidents (Colarik and Janczewski, 2012). But are countries in Africa, such as South Africa, prepared to defend themselves against cyberwarfare?

This research paper aims to discuss the concept of cyberwarfare and the possible effects it can have on CI. The paper is structured in the following manner to achieve this objective: Section 2 explains what cyberwarfare is. Section 3 provides a discussion on cybercrime, cyberterrorism, and cyberwarfare. Section 4 provides a discussion of the different cyberwarfare incidents that occurred worldwide. Section 5 provides a few techniques that can be used to protect CI from cyberwarfare. Section 6 highlights the possible effects of cyberwarfare on CI, and section 7 discusses the authors' stance if South Africa is prepared to defend itself against cyberwarfare. The last section, section 8, concludes the paper.

2. What is Cyberwarfare

Currently, there are several definitions of cyberwarfare. Clarke and Knake (2010) describe cyberwarfare as actions where a nation-state will penetrate another nation's networks or systems to cause damage or disruption. This definition implies that the target and source of cyberwarfare actions are only between nation-states to advance a national agenda such as information superiority. However, Robinson, Jones and Janicke (2015) describe that cyberwarfare includes state actors and non-state actors such as businesses or hackers whose aim is not a national agenda. Another definition described by Cornish, Livingstone, Clemente, and Yorke (2010) is that cyberwarfare is a conflict between states, but it can sometimes involve non-state actors. The target of these attacks can be industrial, military, civilian targets or a server room hosting several client information. This definition implies that cyberwarfare targets can be different infrastructures, including state and non-state actors. Cyberwarfare includes network attacks and special and technical operations and defence (Parks &

Duggan, 2011). It usually involves actions that can cause political or military effects (Almeida, Doneda & de Souza Abreu, 2017).

Cyberwarfare uses cyberspace to cause cascading kinetic effects (Almeida, Doneda & de Souza Abreu, 2017). Kinetic effects are actions that can affect something or someone in the real world (Parks & Duggan, 2011). These kinetic effects can create results that either cause or contribute to a severe threat to the security of a nation or result in actions taken to respond to such a threat (Almeida, Doneda & de Souza Abreu, 2017). Cyberspace is a virtual space that uses electronics or electromagnetic spectrum to store, modify, exchange, and create information using ICT (Mueller, 2020; Robinson, Jones & Janicke, 2015). Cyberwarfare actions include disruptions to CI and information conflict that can lead to material and social disruptions (Parks & Duggan, 2011). Similar cyberattacks that can also lead to disruptions is cybercrime and cyberterrorism. The following section discusses cybercrime, cyberterrorism, and cyberwarfare to understand what they are and how they differ from one another.

3. Cybercrime, Cyberterrorism and Cyberwarfare

Section 3.1 addresses cybercrime, section 3.2 explains cyberterrorism, and section 3.3 looks at cyberwarfare.

3.1 Cybercrime

Chandra and Snowe (2020) describe cybercrime as an action that uses computer technology to commit a crime. Cybercrime can be classified into two groups, “cyber-enabled” crime and “cyber-dependent” crime (McGuire & Dowling, 2013). Cyber-enabled crimes existed before but are now easier to pursue due to computer technology. Examples are white-collar crime, identity theft, drug trafficking, stalking, etc. Cyber-dependent crimes are crimes that would not exist without cyber technology. These crimes use malware to perform criminal acts (Sarre, Lau & Chang, 2018).

Cybercrime has been growing due to the number of financial benefits. It is easy to obtain money and data due to many users in cyberspace with limited knowledge of how technology works (Bernik, 2014). Cybercrime, cyberterrorism, and cyberwarfare all fall under the same category: cyberattacks (Gazula. 2017). But what makes cybercrime different from cyberterrorism and cyberwarfare is the attacker’s intention. Cybercrime is often committed for personal reasons such as personal gain or the desire to harm others physically or psychologically (Brenner, 2006). An example of an incident of cybercrime occurred during January 2010 and August 2011 when a 23-year-old man, Edward Pearson, stole 200,000 Paypal account details, 2,700 bank card numbers, and 8 million identities using the malware ZeuS and SpyEye. This is an example of cybercrime with the intention of personal gain (Broadhurst, Grabosky, Alazab, Bouhours, & Chon, 2014).

3.2 Cyberterrorism

Cyberterrorism describes acts that use computer technology to intimidate a civilian population, influence the policy of a government, or influence the conduct of the government through intimidation (Robinson, Jones & Janicke 2015). Brenner (2006) states that cyberterrorism is different from cybercrime because cyberterrorism attacks are often due to political reasons rather than personal reasons.

Cyberterrorism and cyberwarfare have similar characteristics, goals, and manner of execution, but the difference between these two cyberattacks is their strategy, targets, and the perpetrators. Cyberterrorism is believed not to be sponsored by a state, while cyberwarfare is often sponsored by a state (Vilić, 2017). The strategy of cyberterrorism involves acts of violence through mass destruction, assassination, or kidnapping (Robinson, Jones & Janicke, 2015). A cyberattack that targets networks and computers is believed to be an act of cyberterrorism when the effect of the attack causes destruction enough to produce fear that can be comparable to a physical act of terrorism (Vilić, 2017). However, there have not been many acts of cyberterrorism (Brenner, 2006).

3.3 Cyberwarfare

Cyberwarfare acts are often seen as political and military motivated war (Cornish et al., 2010). Cyberwarfare uses different weapons in “virtual wars” such as Trojan horses, viruses and worms. These “weapons” are used to disable systems to cause a loss of information or prevent it from functioning. In addition, different software is used to overload Critical Information Infrastructure (CII) to cause disruption or misuse. CII are internet networks or systems responsible for the supervision of CI and the programs that the state and large institutions use (Vilić, 2017).

The common factor between cybercrime, cyberterrorism and cyberwarfare is that the law is often behind and struggles to keep up. Applying existing laws to cyberwarfare is a challenge because of the "weapon" used to carry out cyberwarfare (Robinson, Jones & Janicke, 2015). In addition, there is concern that pursuing cybercriminals across national boundaries can infringe national sovereignty (Goel, 2011). One of the most comprehensive works put together by experts comes from NATO, which describes how existing laws on arm conflict can be applied to cyberwarfare. The Tallinn Manual is not yet lawfully binding, but it can still provide guidance (Robinson, Jones & Janicke, 2015). The following section will discuss past cyberwarfare incidents.

4. Cyberwarfare incidents

This section discusses some of the cyberwarfare incidents that occurred worldwide. Section 4.1 highlights some incidents that occurred in the United States; section 4.2 discusses incidents in the Middle East; section 4.3 highlights incidents in Africa; and section 4.4 highlights incidents in Ukraine.

4.1 Incidents in the U.S.

In 1999 numerous United States government websites were targeted. It was suspected that Chinese hackers were the cause of this attack due to the reported accidental bombing of the Chinese embassy in Belgrade by the U.S. (Goel, 2011).

Another incident that was discovered was in 1998 when U.S. officials discovered an advanced persistent attack (APT) that infiltrated several U.S. CI. The APT known as Moonlight Maze infiltrated the Department of Justice, Department of Defence, and other federal agencies (Kobus, 2016). The infiltration occurred for 2 years, and thousands of unclassified, sensitive information was stolen. This included military hardware designs, military installations, troop configurations and other information on U.S. infrastructure. The Moonlight Maze was traced back to a mainframe computer in Russia, but Russia denied any involvement (Haizler, 2017).

4.2 Incidents in the Middle East

An incident of cyberwarfare that has affected CI was the Stuxnet computer worm that sabotaged Iran's nuclear facilities (Almeida, Doneda & de Souza Abreu, 2017). This worm was built together by the U.S. and Israel. Stuxnet targets the programmable logic controller (PLCs). PCLs are computers that automate industrial electromechanical processes. Iran discovered the worm in 2010 in their uranium plants. The target of Stuxnet was Industrial Control Systems (ICSs) such as supervisory control and data acquisitions (SCADA) systems. By targeting these CII, Stuxnet gathered information and sent it to an entity that released the information. This caused the final product to be unusable (Kobus, 2016). In addition, the nuclear centrifuges that operated on these ICSs self-destructed due to Stuxnet (Theohary & Rollins, 2015).

In September 2012, a new malware was used in a cyberwarfare act. The incident was caused by a cyberespionage malware called Shamoon. Shamoon targeted companies in the oil and energy sector. One of the companies affected severely was Saudi Aramco, a Saudi Arabian company in the oil and energy sector. Shamoon, a self-replicating and self-injecting malware, attacked 30,000 workstations of Saudi Aramco (Knopová & Knopová, 2014).

4.3 Incidents in Africa

During the Jasmine Revolution in Tunisia, the AMMAR, a government owed Internet Service Provider hacked user accounts for the entire population of Tunisia. In retaliation, adversaries launched Distributed Denial of Services (DDoS) attacks against government and AMMAR websites (Kobus, 2016).

In 2016 two hacktivists' groups known as #OPAfrica and Anonymous Africa started targeting South Africa due to corruption and perceived social injustices. Anonymous Africa launched DDoS attacks against political parties in Zimbabwe, South Africa and government agencies and companies involved in corruption and the Gupta family. Furthermore, #OPAfrica caused data breaches by attacking South African government systems such as the arms procurement agency, the Government Communications and Information Services, and other vulnerable websites (Van Niekerk, 2018).

4.4 Incidents in Ukraine

Ukraine also experienced a cyberwarfare incident when malware was implanted on Android devices. This malware was used to track and target the Ukrainian artillery units. The tracking occurred from late 2014 through 2016. It retrieved locational data and communications data from these artillery units. The hacking group responsible for this was linked to the Russian government. It was reported that 9000 users had the malware running on their applications (Gazula, 2017).

Another incident occurred again in Ukraine in December 2015. Blackenergy, a Trojan, infected the Ukrainian electricity distribution network. This attack interrupted more than 225,000 people's electricity supply. Furthermore, it was reported that Blackenergy was intended to be used during the electoral period in Ukraine to destroy videos and image files that would influence the election (Izycki & Vianna, 2021). These incidents of cyberwarfare have caused adverse effects on the CI it has targeted. Table 1 summarises these cyberwarfare incidents and evaluates why these incidents can be classified as cyberwarfare. The following section discusses the possible effects of cyberwarfare on CI.

Table 1: Summary of cyberwarfare incidents and why they can be classified as such

Incident	Reason this is a Cyberwarfare incident
Attack on U.S. government websites by Chinese hackers	The target of the attack was a government website caused by a non-state actor. The attack was due to political reasons, and the attack caused severe disruptions.
The Moonlight Maze APT attacked several U.S. CI.	The target of the attack was a state's CI, and the attack was believed to be caused by another state (Russia). The attackers stole sensitive information that caused political issues.
The Stuxnet worm sabotaged Iran's nuclear facilities.	This attack is cyberwarfare because the target of the attack was a state's CI: Iran's nuclear facilities. The destruction of the nuclear centrifuges indicates a cyberwarfare incident since cyberwarfare incidents typically aim to cause disruption or destruction to CI.
Shamoon malware targeted companies in the oil and energy sector, including Saudi Aramco.	The target of the incident was the oil and energy sector, which qualifies as CI for many nations. The disruption of the CI indicates that this was a cyberwarfare incident.
DDoS attacks were launched against the government and AMMAR, a government-owned Internet Service Provider in Tunisia.	This is a cyberwarfare incident because the target of the DDoS attacks were the Tunisian government websites and a state-owned company. The attacks, which caused serious disruptions, were due to political reasons. The attacker was a non-state actor.
Anonymous, a Hacktivists group, launched DDoS attacks against Zimbabwean and South African government agencies, political parties, and companies. #OPAfrica caused data breaches on South African government websites.	The attacks qualify as cyberwarfare because they specifically targeted government websites. While the attacker was not a state actor, the attacks still caused disruptions on the nations' systems, which is often the aim of cyberwarfare.
A malware was implanted on Android devices that tracked and targeted Ukrainian artillery units	This is a cyberwarfare incident because Russia, a state actor, was linked to this attack against another state, Ukraine. This attack retrieved information from Ukraine's CI by tracking and targeting the Ukrainian artillery.
Blackenergy infected the Ukrainian electricity distribution network.	Cyberwarfare usually targets CI. This incident targeted the electricity distribution network, Ukraine's CI. The incident caused a significant disruption that affected more the 225,000 people.

5. Techniques to protect Critical Infrastructure from Cyberwarfare

The following section discusses some techniques that can be used to protect CI from cyberwarfare. Section 5.1 discusses the system modelling technique, section 5.2 discusses the defence-in-depth strategy, and section 5.3 highlights techniques related to human aspects of security.

5.1 System Modelling

Due to the high complexity of CI, it is necessary to model the complexity of these systems. Modelling can help study and identify vulnerabilities in the CI. This can be done through designing virtual environments which can provide a simulation of features of CI (Merabti, Kennedy & Hurst, 2011). In addition, attacks can also be simulated through war games. War games include simulating attacks on the SCADA system, which helps mitigate attacks because it helps identify weaknesses (Nicholson et al., 2012). The United States launched a war game in 2010 February. This war game was known as Cyber Shockwave (Nelson, 2011). The war game infected 5 million smartphones using a Trojan. This infection then manifested into a DDoS attack that affected government systems. The results of the war game simulation revealed that the U.S. was not prepared to defend itself against a cyberwarfare event (Nicholson et al., 2012). Therefore, such simulations (as tools used in system modelling) can improve the protection of CI.

5.2 Defence in depth

CI should adopt a defence-in-depth strategy. This requires having multiple layers of security such that if an attack penetrates one layer, it cannot penetrate the next layer. These layers employ different technologies and intrusion detection systems (IDS) to secure CI (Hurst, Merabti & Fergus, 2014). The technologies that can be applied can be general preventative measures used in general IT systems such as anti-virus, firewalls, IDS etc. (Nicholson et al., 2012). The defence in-depth needs to implement three levels of security: low, medium, and high. Medium and high levels of security are designed specifically for employees such as managers and system administrators who has access to sensitive information systems and infrastructure assets. In contrast, the low levels of security are for employees who only have basic access (Hurst et al., 2014).

CI infrastructure that adopts this defence-in-depth strategy can also employ Unified threat management (UTM) systems (Hurst et al., 2014). UTM systems provide protection for network, hardware, and software layers. It achieves this by combining several security technologies such as pattern recognition systems, firewalls, IDS and analysis middleware (Zhang, Deng, Chen, Xue, & Lin, 2010). UTM systems can secure CI because they are a unified architecture with different security techniques and are easy to deploy (Hurst et al., 2014).

5.3 Human aspects

Humans are often the weakest link in the security of systems. Security policies, procedures, and protocols need to be defined to prevent attackers from exploiting humans (Nicholson et al., 2012). Training and awareness programs on security also need to be applied.

In addition, there is often a shortage of security experts that can secure CI from cyberwarfare. It is in the best interests of governments to invest in specialised security training to create a talented workforce that can help a nation protect against cyberwarfare from other nations (Tiirmaa-Klaar, 2016). Therefore, training and education to create security experts can protect CI against cyberwarfare.

6. Possible effects of Cyberwarfare on Critical Infrastructure

CI is often controlled by remote systems known as Industrial Control Systems (ICSs). ICS also include SCADA systems (Mcginthy & Michaels, 2019). Cyberwarfare targets ICSs to threaten the integrity, confidentiality, and availability of these systems. If an attack successfully achieves this, it can have dangerous effects such as disruption, alteration, or destruction of CI (Montgomery, 2018).

Cyberwarfare can disrupt CI by attacking the integrity of the SCADA systems. For example, if a cyberwarfare event targets and changes the control signals of the SCADA systems, it can cause it to malfunction, which can also affect the availability of the system (Kovacevic & Nikolic, 2015). If a SCADA system becomes unavailable, the CI it manages (i.e., power distribution, water and waste distribution services) will be disrupted. If these services are disrupted, it can result in major economic losses and affect the livelihood of citizens (Thakur, Ali, Jiang & Qiu, 2016). The disruption caused by attacking SCADA systems was seen in the 2010 attack of the Stuxnet worm on Iran's uranium plants discussed in section 4.2 (Kobus, 2016). If a cyberwarfare incident disrupts a single CI sector, the effects of this attack can propagate to other CI sectors. This can occur due to the interdependencies and dependencies among the different CI sectors (Kovacevic & Nikolic, 2015). For example, water management systems require electric power generation infrastructure to supply water. Therefore, cyberwarfare attacks can spread to different sectors, which is a significant threat to CI.

The disruption that cyberwarfare can cause can persist for long durations of time because of the difficulty to perform updates and software patches on SCADA systems (Cárdenas, Amin, Lin, Huang, Huang, & Sastry, 2011). Before patches are applied, they must be thoroughly tested, and performing upgrades requires planning and placing the systems offline (Kovacevic & Nikolic, 2015). Therefore, the effects of cyberwarfare can last for a long time.

Cyberwarfare attacks can alter CI by breaching the confidentiality and integrity of data supplied to the central monitoring systems that manage CI. A cyberwarfare attack could supply inaccurate data to these systems through a virus. This could result in the SCADA system reacting to this false data, which can cause the CI to perform dangerous actions (Nicholson, Webber, Dyer, Patel & Janicke, 2012). In addition, cyberwarfare can destroy CI by causing failures to the SCADA systems, and that can result in causing damage to physical systems that can be irreparable. It can lead to consequences on the public safety and health of citizens (Kovacevic & Nikolic, 2015). Therefore, the effects of cyberwarfare on CI can affect the physical world, and one of the major concerns that the failure of CI could cause is the loss of human life (Nicholson et al., 2012). Due to the number of dangerous effects that cyberwarfare can cause, it is essential to apply techniques to protect this CI. But with the threats of cyberwarfare and protection techniques, is South Africa ready to protect itself against a cyberwarfare incident? The following section discusses this.

7. South Africa's readiness for Cyberwarfare

South Africa (SA) is not prepared to defend itself against a cyberwarfare attack. While there has not been a major reported cyberwarfare incident, the number of cyberattacks in South Africa have increased due to increased connectivity (Peter, 2017). SA's responses to these attacks demonstrated that it is not prepared. For example, the recent attack on Transnet's information technology networks severely disrupted Transnet's CI services. Transnet is an SA-owned rail, port and pipeline company that experienced disruptions that interrupted their cargo movement. As a result, cargo terminals at Cape Town stopped operating, resulting in Transnet switching to manual processes. Transnet's response to switching to a manual approach indicates that Transnet was not prepared for an attack targeting their CI. Unfortunately, public information is limited, making it difficult to determine what security technique to protect their ports (Reva, 2021).

Another incident was the attack on the City of Johannesburg (CoJ) systems. CoJ experienced a network breach that allowed unauthorised access to their information systems. As a result of the attack, CoJ had to shut down customer-facing systems such as e-services (Moyo, 2019). CoJ shutting down a customer-facing system as a response showed unreadiness for an attack of that nature. In this case, applying defence-in-depth could assist CoJ in protecting their CIs since having multiple layers of security could prevent the network breach from penetrating other layers of the system.

Another attack that further highlights SA's unpreparedness against cyberwarfare is the ransomware attack that targeted 66 Life Healthcare hospitals. The ransomware attack caused several administrative delays forcing the hospitals to switch to manual processing systems (Bottomley, 2020). Such an attack could be mitigated by applying system modelling (to identify vulnerabilities), defence-in-depth (to add multiple layers of security) and human aspects (such as staff training and awareness programs).

In addition, SA's lack of cyberwarfare readiness is due to South Africa's legislative systems. In addition, there is currently a lack of international cyber defence treaties that specifically address cyberwarfare (Grobler & van Vuuren, 2012). The lack of treaties makes it extremely difficult to prosecute criminals from different states (Goel, 2011) and contributes to South Africa's lack of readiness because there is no legal agreement on the consequences that attackers who commit cyberwarfare can face. While South Africa has taken legal steps to protect against cyberattacks by passing legislation such as the Cyber Crimes Act (Moyo, 2021), it is still not enough to prepare South Africa for cyberwarfare. The Cyber Crimes Act covers cybercrime and not cyberwarfare, which are two different cyberattacks performed for different reasons, as discussed in section 3.

Qualified professionals are leaving South Africa for opportunities overseas, which means South Africa is losing a valuable workforce in sectors such as infrastructure and development (Thompson, 2021). From section 5.3, it was noted that skilled experts in fields such as security are needed to protect against cyberwarfare. But since South Africa is losing experienced professionals, which puts further strain on effectively preparing for a cyberwarfare incident. Skilled staff is needed to implement technologies to create resilient CII. Since there is a lack of an experienced workforce, technologies for protecting CII have a higher likelihood of being outdated. Therefore, South Africa might not have the right tools and approach against a cyberwarfare incident. The following section will conclude the paper.

8. Conclusion

Different concepts were discussed to meet the objective of the paper. The main aspects addressed were first understanding cyberwarfare by considering various definitions. Cyberwarfare is seen as actions whose aim is to bypass a nation's networks or computers that can result in significant damage or disruption. There are currently different views of cyberwarfare. Some definitions describe that cyberwarfare actions are only between nation-state actors (Clarke & Knake, 2010). Other definitions specify that it can also involve non-state actors (Robinson, Jones & Janicke, 2015). Cyberwarfare can be confused with other cyberattacks such as cybercrime and cyberterrorism. Therefore, the paper discussed each of the three concepts. It was found that cybercrime is often committed for personal reasons. In contrast, cyberterrorism is committed due to political reasons to cause fear, similar to a physical terrorist attack.

Several incidents were discussed to understand the dangers of cyberwarfare, including why they were classified as cyberwarfare. Incidents such as Stuxnet highlighted some of the possible effects of cyberwarfare on CI. Due to these effects, techniques that can protect CI are required. Techniques like system modelling can help identify weaknesses in CI (Nicholson et al., 2012). Moreover, human aspects are essential since humans are usually the weakest link in cyberattacks. Effects such as disruption and damage to a nations CI were also discussed to show that cyberwarfare can have a devastating impact on CI. Lastly, the paper looked at whether South Africa is prepared to defend itself against cyberwarfare. Our opinion that South Africa is not ready was supported by how South Africa responded to cyberattacks incidents such as the Transnet attack. In addition, the lack of legal treaties addressing cyberwarfare contributes to South Africa's lack of readiness. Therefore, the objective of the paper, which was to discuss cyberwarfare and its effects on CI, was met.

References

Almeida, V.A.F., Doneda, D. and de Souza Abreu, J. (2017) "Cyberwarfare and digital governance", *IEEE Internet Computing*, Vol. 21, No. 2, March, pp 68-71.

Bernik, I. (2014) *Cybercrime and cyber warfare*, John Wiley & Sons, Hoboken.

Bottomley, E. J. (2020) *"SA hit as hackers target hospitals during Covid-19 crisis- here's what Life may be facing",* [online], Business Insider, SA hit as hackers target hospitals during Covid-19 crisis – here's what Life may be facing (businessinsider.co.za).

Brenner, S.W. (2006) "Cybercrime, cyberterrorism and cyberwarfare", *Revue internationale de droit 7enal*, Vol. *77*, No. 3, pp 453-471.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B. and Chon, S. (2014) "An analysis of the nature of groups engaged in cyber crime"*, International Journal of Cyber Criminology*, Vol. 8, No. 1, January-June, pp 1-20.

Cárdenas, A.A., Amin, S., Lin, Z.S., Huang, Y.L., Huang, C.Y. and Sastry, S. (2011) "Attacks against process control systems: risk assessment, detection, and response". *Proceedings of the 6th ACM symposium on information, computer and communications security*, March, pp 355-366.

Chandra, A. and Snowe, M.J. (2020) "A taxonomy of cybercrime: Theory and design", *International Journal of Accounting Information Systems*, Vol. 38, September, pp 1-20.

Clarke, R.A. and Robert, K.K. (2010) *Cyber war: the next threat to national security and what to do about it?,* Harper Collins.

Colarik, A.M and Janczewski, L.J. (2012) "Establishing cyber warfare doctrine", *Journal of Strategic Security,* Spring Vol. 5, No. 1, pp 31-48.

Cornish, P., Livingstone, D., Clemente, D. and Yorke, C. (2010) *On cyber warfare,* Chatham House, London.

Gazula, M.B. (2017). *Cyber warfare conflict analysis and case studies,* Massachusetts Institute of Technology, Cambridge.

Goel, S. (2011) "Cyberwarfare: connecting the dots in cyber intelligence". *Communications of the ACM*, Vol. 54, No. 8, August, pp 132-140.

Grobler, M. and van Vuuren, J. J. (2012) "Collaboration as proactive measure against cyber warfare in South Africa", *African Security Review*, Vol. 21, No. 2, June, pp 61-73.

Haizler, O. (2017) "The United States' cyber warfare history: Implications on modern cyber operational structures and policymaking", *Cyber, Intelligence, and Security*, Vol. 1, No. 1, January, pp 31-45.

Hurst, W., Merabti, M. and Fergus, P. (2014) "A survey of critical infrastructure security". *International Conference on Critical Infrastructure Protection*, Vol. 441, pp 127-138, Springer, Berlin, Heidelberg.

Izycki, E. and Vianna, E.W. (2021) "Critical Infrastructure: A Battlefield for Cyber Warfare?"*, ICCWS 2021 16th International Conference on Cyber Warfare and Security*, pp 454-464.

Knopová, M. and Knopová, E. (2014) "The Third World War? In The Cyberspace. Cyber Warfare in the Middle East". *Acta Informatica Pragensia*, Vol. 3, No. 1, pp 23-32.

Kobus, J. (2016) *Cyberwarfare: The evolution of war*, Utica College, Utica.

Kovacevic, A. and Nikolic, D. (2015) "Cyber attacks on critical infrastructure: Review and challenges", *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance*, pp 1-16, University of Belgrade, Serbia.

Mcginthy, J. M. and Michaels, A. J. (2019) "Secure industrial Internet of Things critical infrastructure node design", *IEEE Internet of Things Journal*, Vol. 6, No. 5, pp 8021-8037.

McGuire, M. and Dowling, S. (2013*) Cybercrime: A review of the evidence: Summary of key findings and implications*, Home Office Research Report 75, London: Home Office.

Merabti, M., Kennedy, M., & Hurst, W. (2011) "Critical infrastructure protection: A 21 st century challenge", *2011 International Conference on Communications and Information Technology (ICCIT)*, pp 1-6.

Montgomery, M. (2018) "Proliferation of cyberwarfare under international law: virtual attacks with concrete consequences", *S. Cal. Interdisc. L.J.*, Vol. 28, pp 499-521.

Moyo, A. (2021) "President Ramaphosa signs Cyber crimes Bill into Law", [online], I.T. Web, https://www.itweb.co.za/content/LPp6VMrDJJovDKQz.

Moyo, A. (2019) *"City of Johannesburg hit by cyber attack",* [online], ITWeb, https://www.itweb.co.za/content/dgp45qaG8gZ7X9l8 .

Mueller, M. L. (2020) "Against sovereignty in cyberspace", *International Studies Review*, Vol. 22, No. 4, 20 September, pp 779-801.

Nelson, C. (2011) "Cyber Warfare: The Newest Battlefield", [online], Computer Science & Engineering Washington University in St.Louis, https://www.cse.wustl.edu/~jain/cse571-11/ftp/cyberwar/.

Nicholson, A., Webber, S., Dyer, S., Patel, T. and Janicke, H. (2012) "SCADA security in the light of Cyber-Warfare", *Computers & Security*, Vol. 31, No. 4, June, pp 418-436.

Parks, R. C. and Duggan, D. P. (2011) "Principles of cyberwarfare", *IEEE Security & Privacy*, Vol. 9, No. 5, 26 September, pp 30-35.

Peter, A. S. (2017) "Cyber resilience preparedness of Africa's top-12 emerging economies", *International Journal of Critical Infrastructure Protection*, Vol. 17, March, pp 49-59.

Reva, D. (2021) "Cyber attacks expose the vulnerability of South Africa's ports", [online], Institute For Security Studies, https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports.

Robinson, M., Jones, K. and Janicke, H. (2015) "Cyber warfare: Issues and challenges", *Computers & security*, Vol. 49, March, pp 70-94.

Sarre, R., Lau, L. Y. C. and Chang, L. Y. (2018) "Responding to cybercrime: current trends", *Police Practice and Research*, Vol. 19, No. 6, 20 September, pp 515-518.

Thakur, K., Ali, M. L., Jiang, N. and Qiu, M. (2016) "Impact of cyber-attacks on critical infrastructure", *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, pp 183-186.

Theohary, C. A. and Rollins, J. W. (2015) *Cyberwarfare and cyberterrorism: In brief*, Congressional Research Service, Washington.

Thompson, W. (2021) *"Brain drain a threat to economic recovery, warns RMB boss",* [online], BusinessDay, https://www.businesslive.co.za/bd/economy/2021-02-10-brain-drain-a-threat-to-economic-recovery-warns-rmb-boss/.

Tiirmaa-Klaar, H. (2016) "Building national cyber resilience and protecting critical information infrastructure", *Journal of Cyber Policy*, Vol. 1, No. 1, March, pp 94-106.

Van Niekerk, B. (2018) "Information warfare as a continuation of politics: An analysis of cyber incidents", *2018 Conference on Information Communications Technology and Society (ICTAS)*, pp. 1-6.

Vilić, V. M. (2017) "Dark web, cyber terrorism and cyber warfare: Dark side of the cyberspace", *Balkan Social Science Review*, Vol. 10, No. 10, October, pp 7-25.

Zhang, Y., Deng, F., Chen, Z., Xue, Y. and Lin, C. (2010) "UTM-CM: A practical control mechanism solution for UTM system", *2010 International Conference on Communications and Mobile Computing,* Vol. 1, pp 86-90.