Towards the Legal Protection of Critical Infrastructure in Africa Against Cyberwar and Cyberterrorism

Ngalim, Bernard

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Ngalim, B. (2023). Towards the Legal Protection of Critical Infrastructure in Africa Against Cyberwar and Cyberterrorism. *Journal of Cyberspace Studies*, *7*(2), 115-146. https://doi.org/10.22059/jcss.2023.363504.1090

Original Article

Towards the Legal Protection of Critical Infrastructure in Africa against Cyberwar and Cyberterrorism

Bernard Ngalim

(Received 28 April 2023; accepted 27 June 2023)

Abstract
This article reviews the legal framework governing the protection of critical infrastructure in Africa with an emphasis on threats like cyberwar and cyberterrorism. As African governments and businesses increasingly depend on the internet and information systems, there is a need to enact appropriate laws to protect critical infrastructure from cyberattacks that could jeopardize the economic and national security postures of African countries. The article outlines the need for appropriate legal instruments to protect critical infrastructure as African businesses increasingly rely on the internet and information systems. The lack of adequate laws regulating critical infrastructure does not translate to the absence of critical infrastructure in African countries. Ghana, for instance, has a legal framework governing critical infrastructure. These infrastructures are common in most African countries but lack the required legal framework to protect them. It is important to note that despite the Budapest Convention and African Convention on Cybersecurity and Personal Data Protection, there is no international legal framework regulating cyberwar and cyberterrorism. Considering these factors, this article reviews Ghana's Cybersecurity Act and the Directive on Critical Information Infrastructure and uses the United States framework for comparative analysis. In addition to reviewing the types of attacks critical infrastructure could face, the article looks at the legal framework for managing incidents that could arise from cyberattacks targeting critical infrastructure.

Keywords: critical infrastructure, cyberattacks, cybercrime, cybersecurity, cyberterrorism, cyberwar.

Bernard Ngalim: University of the Free State, Bloemfontein, South Africa | Email: 2020574279@ufs4life.ac.za

Introduction

As cybercrime rises in Africa, reports do not indicate attacks on critical infrastructure. However, should African countries wait to suffer cyberwarfare, cyberterrorism and cyberattacks on critical infrastructure before developing a legal framework that regulates the protection of critical infrastructure? The International Police (INTERPOL) reports that over 90% of African companies operate without necessary cyber protection mechanisms (INTERPOL, 2021). This article reviews the legislative steps taken in Africa to require businesses to enforce protections against cyberattacks particularly against cyberwarfare and cyberterrorism. This article will draw examples from the United States legal framework governing the protection of critical infrastructure. The United States is the world's leader in critical infrastructure protection. This article draws inspiration from the United States developed framework to inform the development of critical infrastructure protection frameworks in Africa. Due to the surge in global terrorist threats during the 1990s, governments shifted from ensuring infrastructure adequacy to including regulations protecting critical infrastructure against potential terrorist attacks (Moteff, 2004). The United States Cybersecurity Infrastructure and Security Agency (CISA) requires businesses and government to protect critical infrastructure against incapacitation, or destruction is vital. Destroying or incapacitating critical infrastructure negatively affects the economy, human rights, dependent on national security, health, and safety (CISA, n.d.). Critical infrastructure could be physical or virtual, serve humanity, and enhance human dignity. This article is important because it reviews the importance of critical infrastructure as "people's individual lives often orbit around the internet, whether at home, at work, or almost anywhere else. Even decades-old infrastructure—from roads and rails to water pipes and the energy grid—now relies on digital equipment for construction, operation, and modernization" (Tome et al., n.d.). Since critical infrastructure is a broad concept, this article focuses on the legal framework governing critical infrastructure that connects to the internet and relies on information technology to function effectively and serve humanity.

In recent years, cyberterrorists and state actors have disrupted economies by launching cyberattacks against critical infrastructure in countries with advanced economies. Industrialised countries have taken legislative and regulatory measures requiring industry and government services to continuously protect critical infrastructure from attacks. Continuously monitoring and providing necessary cybersecurity

controls limit the damage or pre-empt cyberattacks targeted at critical infrastructure. While cyberterrorists may limit themselves to the denial of critical services, steal proprietary information, or request ransoms before releasing attacked critical infrastructure, their attacks can have long-lasting effects on human dignity and economic activities. African governments and relevant stakeholders, especially businesses must recognise these threats and their consequences and adapt frameworks that mandate the protection of critical infrastructure. The global, flexible, and rapidly expanding effects of cyber attacks require a concerted effort and collaboration between industrialised and developing countries. Recent trends demonstrate that cyberattacks are increasing in industrialised countries despite technological and regulatory advancements (McKinsey, n.d.). This article is relevant to African policymakers and academics who seek to structure critical infrastructure in Africa to protect against future attacks. First, I lay the foundation for understanding the concept and importance of critical infrastructure and its relationship to economic growth and the protection of human rights. Second, I present cyber terrorism and cyberwarfare as dangerous critical risks to critical infrastructure. Third, I trace international legal obligations requiring protection against attacks on critical infrastructure. Fourth, I review the regulatory frameworks in Ghana and Cameroon regulating critical infrastructure. I chose Ghana and Cameroon because they have cybersecurity laws and are anglophone and francophone, respectively with different colonial legacies that underpin their legal, administrative, and business environments and cultures. Although Cameroon is not entirely Francophone, the legal framework adopts the French system. The similarities between the two countries are the existing cybersecurity legal frameworks. The differences are the legal and administrative systems. A comparative study will explain how African governments anticipate and prepare for future cyberattacks. Another outcome will be the value they attach to business continuity and economic development in the face of such attacks.

1. The importance of protecting critical infrastructure to Africa

Infrastructure is relevant in advancing economic growth and developing all economies since it provides the foundations on which businesses grow (Uzoh & Baulo, 2013). Considering the importance of infrastructure to Africa's economic growth, African governments must ensure that the recent surge in technological advancements coupled with economic growth are protected by legal and technical mechanisms. Critical infrastructure, such as transportation, information and communication

systems, and energy systems, plays a vital role in enhancing businesses and protecting human rights by enabling the efficient movement of goods and services and ensuring access to essential services. According to INTERPOL, Africa has witnessed significant distributed denial of service (DDoS) attacks on critical infrastructure, including the 2016 Mirai botnet attack on Liberia, which crippled the country's internet with over 500 Gbps, and a more recent attack on a South African ISP resulting in a full-day service outage (INTERPOL, 2021). By protecting critical infrastructure against threats such as cyberattacks and terrorism, governments can help ensure the safety and security of their citizens and promote economic growth and development.

a. Lack of a universally accepted definition of critical infrastructure

Critical infrastructure has a long history dating back to ancient civilizations like Rome and Greece, where systems such as waterways played a vital role in both civilian life and military operations (Newbill, 2019). Initially hidden and protected, Rome's waterways eventually became vulnerable to attacks by enemies who targeted and disrupted the water supply (Ibid). Critical infrastructure has always included infrastructure supporting the economy and ensuring that food, water supplies and transportation systems like railways function appropriately (Ibid). During World War II, the Allied powers bombed Germany's railways destroying their transport system. By destroying Germany's transportation system and incapacitating the circulation of goods and people, Allied powers proved that critical infrastructure serves the government, the military and civilians. Some infrastructure is vital for the functioning of a country, and its destruction or incapacitation can have severe consequences for all aspects of society. International humanitarian law protects civil infrastructure and prohibits belligerents from attacking them during war and "although *critical infrastructure* is not found within the four corners of either document, there are regulations pertaining to the protection of civilian hospitals, medical transport, and passage of medical supplies, food, and clothing (Ibid). This background gives an idea into the concept of critical infrastructure and its importance to the existence and survival of communities. As noted, this definition reflects the physical state of critical infrastructure and applies mostly in the past. However, with the advancement of technology and the internet, critical infrastructures have become interdependencies connected to the internet and servicing each other. This aspect changes the critical infrastructure landscape and legal architecture governing their protection. Different countries and regions have adopted different legal frameworks to protect their critical

infrastructure depending on their needs and the changing landscape of threats facing these infrastructures. However, one thing is constant. The protection of critical infrastructure seeks to protect the economy and national security. The definitions below give an idea of the trend in the definition of critical infrastructure.

1. The United States Patriot Act defines critical infrastructure as,

> *"systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"* (Patriot Act, 2001).

2. The National Institute of Standards and Technology (NIST) clarifies that,

> *"the critical infrastructure community includes public and private owners and operators, and other entities with a role in securing the Nation's infrastructure. Members of each critical infrastructure sector perform functions that are supported by the broad category of technology, including information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT). This reliance on technology, communication, and interconnectivity has changed and expanded the potential vulnerabilities and increased potential risk to operations"* (NIST, 2022).

In the United States, the government designated critical infrastructure sectors through "a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security (Executive Order on Improving Critical Infrastructure Cybersecurity, 2013)."

1. According to the OECD,

> *"Critical information infrastructures, "CII", should be understood as referring to those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-*

> *being of citizens, or on the effective functioning of government or the economy"* (OECD, 2008).

2. According to Ghana's Cybersecurity Act,

> *"critical information infrastructure means a computer or computer system designated under subsection (1) of section 35."* (Ghana's Cybersecurity Act, 2020: S. 97).

While all these definitions share the concept of critical infrastructure and its importance to the economy and national security, their definitions, scope, and legal contexts diverge. They reveal the nuanced and multi-dimensional nature of critical infrastructure in today's world. Considering the fast-evolving technology and the diversified legal contexts, effectively regulating and protecting critical infrastructure requires a flexible and adaptable approach. Such approaches must consider the national contexts and the possible implications of the disruption of critical infrastructure in the regional and global stages. As Africa moves towards the continental free trade zone, disruptions of critical infrastructure in one country could affect the entire region. One thing that remains constant is the crucial role critical infrastructure will play towards Africa's economic growth. These definitions focus on the impacts the destruction or incapacitation of critical infrastructure can have on the continuous survival of an economic system. This explains why the Executive Order highlights that designating critical infrastructure based on potential risk fits the protection purpose. Interestingly, Ghana's Cybersecurity Act is hyperfocused on the interconnectedness of the internet and computer networks and ignores their implication for the normal functioning of the economy. While all these definitions share the concept of critical infrastructure and its importance to the economy and national security, their definitions, scope, and legal contexts diverge. As African countries move towards diversifying their economies and increasingly connecting to the Internet and constructing critical infrastructure, it is relevant to develop definitions and legal frameworks encompassing the physical and technical aspects of critical infrastructure. Adopting legislation from a risk-based approach permits stakeholders to evaluate potential risks that can befall the critical infrastructure and allocate resources accordingly. The absence of a universally accepted definition of critical infrastructure explains why different governments identify sectors that are critical to the continued survival of their countries. This should not prevent African countries from developing relevant legal frameworks to enhance their

economic growth and national security as discussed below. This article uses critical infrastructure interchangeably with critical information infrastructure.

b. Critical infrastructure is advancing economic growth in Africa

The relationship between infrastructure and economic growth in Africa cannot be overemphasised as businesses require some form of infrastructure to produce output (Dibie & Okwonko, 2000). In the modern age, science and technology have advanced the development of infrastructure which have become critical for the operation of growth and enterprise, business, and innovation (Ibid). The liberalisation of African economies in the 1980s and investments in information and communication technologies (ICTs) spurred economic growth (Rufus & Bufumoh, 2017). The spread of internet infrastructure induced the diffusion of ICT products and services on the continent, including a substantial increase in mobile phone subscribers and broadband internet penetration (Ibid). The rise of ICT changed the course of business, and traditional industrial businesses are increasingly shifting the course of business to adjust to the ever-increasing demands of technological advancements. For instance, communication speeds have increased, and businesses have faster and easier access to diversified markets worldwide (Kesici Çalışkan, 2015). ICT has also increased the edge of competition as technology-producing nations leverage their technological skills to advance their business products and impose their superiority through military superiority in the marketplace (Ibid).

Despite the exponential rise in technologies that spur economic growth around the world, Africa needs to catch up in advancing and producing her own technology to catch up with the rest of the world (Corrigan, 2020). Africa's slow advancement in ICT development essentially highlights the importance of technological innovation for economic development in Africa to compete with the rest of the world. Industrialised and fast growing economies are approaching the fourth industrial revolution, where technological advancements like artificial intelligence, advanced robotics and cyber-physical systems are reshaping critical infrastructure and advancing economic growth (Qureshi, 2020). Advancements in ICT benefit the development of critical infrastructure and spur economic growth. However, African nations working to advance ICT should consider the growing risks of cyberattacks, including cyberterrorism and cyberwarfare. These risks can severely harm innovation and destroy an economy unless appropriate risk mitigation and legal frameworks accompany innovation and oblige

stakeholders to comply. As more technologically advanced countries have experienced, cyberattacks can have devastating consequences and can undermine the gains made in economic growth. African nations must implement measures to protect critical infrastructure against cyber threats, particularly cyberwarfare and cyberterrorism. While focusing on economic development and national security, critical infrastructure advances human rights. Regulating critical infrastructure protection is not only an economic imperative but also a social and public requirement.

c. Critical infrastructure have an impact on human rights

Like economic growth, the development of critical infrastructure can significantly impact the enjoyment and fulfilment of human rights in Africa. By improving and expanding critical infrastructure systems such as transportation, communication, and energy, Africans can have better access to essential services such as education, healthcare, and employment opportunities. This can help to promote and protect their human rights by enabling them to live healthy, productive lives and participate fully in society. The integration of technological advancements such as genetics, biology, big data, and artificial intelligence (AI) has led to a revolution in the healthcare sector (Weenk, 2020). These advancements have improved research, drug production, personalised medicine, clinical workspaces, diagnosis, and care delivery (Ibid). Digitised health has also improved efficiency and effectiveness through prescription management, remote healthcare, monitoring, and interconnected medical devices and networks known as the Internet of Medical Things (IoMT) (Ibid).

For example, enjoying and fulfilling the right to health is largely influenced by ICT. The COVID-19 pandemic demonstrated the importance of digital technologies in supporting the public-health response worldwide (Budd et al., 2020). Technologies such as mobile phones, online datasets, connected devices, machine learning, and natural language processing were used to support population surveillance, case identification, contact tracing, and evaluation of interventions (Ibid). These technologies have also helped with communication with the public and provided relatively low-cost computing resources for analysing large amounts of data (Ibid). The pandemic has highlighted the potential of digital technologies to enhance public health efforts and improve our ability to respond to health crises (Ibid). While emphasising the need to advance and protect critical infrastructure for economic purposes, every human being relies on effectively functioning

critical infrastructure. Consequently, their protection should not only be a question of national security and economy but also of public concern.

Despite the advances discussed above, cybersecurity has become a strategic issue for healthcare facilities as they are often targeted by hackers due to their obsolete defences and poor IT organisation (Le Bris & El Asri, 2017). This situation is exacerbated by the misuse of IT systems by employees with low risk awareness and a lack of proper funding for Information Security, while the democratisation of hacking techniques has increased the number of potential perpetrators (Ibid). Of the different types of cyberattacks against hospitals, the most significant concern is a ransomware attack that would disrupt patient treatment and force a shutdown of hospital operations. In March 2020, a ransomware attack happened at Brno University Hospital in the Czech Republic, treating vulnerable COVID-19 patients and forcing them to redirect patients to other hospitals (Riggi, n.d.). According to John Riggi, "A ransomware attack on a hospital crosses the line from an economic crime to a threat-to-life crime – and therefore should be aggressively pursued and prosecuted as such" (Ibid). This example of the right to health shows how the protection of critical infrastructure affects the enjoyment of human rights. Noting that the erection and development of critical infrastructure comes with accompanying cybersecurity risks and threats that African governments must integrate into their calculus of advancing economic growth through ICT development. In developing critical infrastructure legal frameworks, African governments should factor the public interest in effective protection.

2. Types of cyberattacks that target critical infrastructure

Cyber-attacks targeting critical infrastructure seek to control or shut down systems rather than steal data (Allianze, n.d.). Recent research found that "54% of the 500 US critical infrastructure suppliers surveyed had reported attempts to control systems, while 40% had experienced attempts to shut down systems" (Ibid). In recent years, countries and companies are increasingly coming to terms with the fact that critical infrastructure can be vulnerable to cyberattacks with potentially serious consequences (Bolonga et al., 2013). Cyberattackers use malware as weapons to disrupt or stop critical infrastructure systems from operating, causing significant harm and disruption in services (Ibid). Rabia Tahir defines *malware* as "short for […] malicious software, as the name suggests malwares are intended to harm computers and computer users by stealing information, corrupting files or by just doing mischievous activities to annoy users" (Tahir, 2018). Malware could be

viruses, worms, trojan horse, rootkit, spyware, adware, cookies, sniffers, keyloggers, spam, or ransomware (Ibid). In addition to malware, Lisa Goth rightly argues that cyberattacks employ phishing, denial of service, man in the middle, crypt jacking, SQL injection and zero-day exploits (Goth, n.d.). Once cyberattacks exploit vulnerabilities in a structure and install these malicious programs, they collect sensitive information, replicate the malware, disrupt the critical components making the system inoperable (Ibid). These malicious operations could amount to cyberwarfare or cyberterrorism and have financial, human, economic or national security implications.

a. Cyberterrorism

While some argue that the risk of cyberterrorism is not imminent and that current cyberattacks on critical infrastructure resemble common cyberattacks, the rapid advancement of technology suggests that the potential for cyberattacks with life-threatening consequences, equivalent to terrorist attacks, may emerge (Shiryaev, 2012). Lewis disagrees with the concept of cyberterrorism by positing that instances similar to what others describe as cyber-terror scenarios, such as water system failures, power outages and air traffic disruptions, are normal service disruption events that do not affect national security (Lewis, 2003). This view does not sit well with the criminal law requirements of *actus reus* and *mens rea* to qualify an act as a crime. An analogy that puts James' argument into perspective is a car accident and its criminal consequences. If a driver of a 70 seater bus gets into an accident and everyone on board dies, that driver is not held responsible for committing a crime if he did not intend to commit a crime. Whereas, if a group of individuals intentionally decide to force a driver to drive a 70 seater bus down a ditch, those people would potentially be charged with terrorism or capital murder. The motivation that caused cyber attackers to commit a cybercrime automatically changes the legal interpretation attributed to the act.

Lewis further argues that at a national level, failures in critical infrastructure systems are frequent, and for cyber-terrorists to make a significant impact, they would need to launch simultaneous and sustained attacks on multiple targets, which is an impractical scenario for most hackers, terrorist groups, or nation states (Ibid). Referring to the ordinary meaning of terrorism, Igor Primoratz opines that terrorism has a structure with a primary and a secondary target where the secondary target is directly hit to intimidate the primary target into doing things they otherwise would not do (Primoraz, 2019). From

this view, Primoratz's understanding of terrorism specifically focuses on a primary and a secondary target. Accordingly, the terrorists' focus on cyberterrorism cannot be widespread or have multiple targets. However, these disagreements signal the lack of a consensus on the definition of cyberterrorism. The absence of a common definition does not eliminate the risk of attacks targeted at critical infrastructure. African policymakers should focus on the required protections needed to prevent critical infrastructure from attack and not the definitions of cyberterrorism.

Denning's attempt to fill the gap in the definition of cyber terrorism opens the way to the identification of material elements that could constitute the crime of cyberterrorism. According to her, "cyberterrorism is the convergence of cyberspace and terrorism [and] refers to unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" (Denning, 2000). This definition invokes Igor's terrorism structure of a primary and secondary target where either a government or the population represent either of the targets and is conducted to attain a particular political or social goal. Additionally, "to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples" (Ibid). Like Lewis, Denning categorises cyberterrorism based on the impact of the cyberattack (Ibid). However, unlike Lewis, Denning considers attacks targeting critical infrastructures and causing their disruptions as cyberterrorism (Ibid). She would not consider attacks causing disruptions to nonessential services or their functioning as cyberterrorism but as a costly nuisance (Ibid).

In 2017, the WannaCry cyberattack that hit the United Kingdom's National Health Service (NHS) spread to more than 200,000 computers in about 150 countries and prevented hospitals from accessing patient records, forcing hospitals to cancel or delay appointments and diverting ambulances to different hospitals (Ibid). It is important to note that the malware spread very fast and the "NHS was among those hit by the attack, with more than 600 NHS organisations affected, including 34 directly affected hospitals. Staff were unable to access IT systems and medical devices such as MRI scanners, causing disruption that continued for a week after the virus was brought to a halt" (Alford, 2019). The UK government reported that the Wannacry cyberattack cost them an estimated 92 million British pounds as lost output and information

technology support during and after the attack (UK Department of Health and Social Care, 2018).

Despite the devastating consequences of the Wannacry cyberattack, including the fear, intimidation and financial loss, the cyberattack is not rated as cyberterrorism. As I mentioned earlier, the qualities of a crime must be judged by the attackers' intentions and acts. Although the consequences of the WannCry cyberattack could qualify as cyberterrorism, the attacker's intention did not speak to causing widespread pain and damage. In this case, the attackers of the WannaCry cyberattack did not intend to intimidate or coerce a government or its people in furtherance of political or social objectives. Rather, they used the cyberattack as ransomware, demanding the payment of bitcoins worth $300 to unlock each infected device, 'with a doubling of the charge after three days, and the threat of all data being lost if payment was not received within a week" (Collier, 2017). It should be noted that these cyberattacks spread across the entire economic spectrum. In 2021, the Colonial Pipeline ransomware cyber attack led to the disruption of the delivery of gasoline and other products in the United States where the attackers were paid about $5 million in ransom before the hackers released the system (Turton et al., 2021). Colonial Pipeline was not categorised as cyber terrorism because the objective was not to hold the service hostage to advance an ideology, political or social objective but to obtain the payment of ransom. As African countries advance their critical infrastructure and connect businesses to the internet, they should consider these downsides of cyberthreats with significant financial consequences and prepare for them adequately. The legal framework mandating such preparations and protection of critical infrastructure and information technology systems is a mandatory first step as discussed in sections 3 and 4 below. As much as there is no agreed definition of cyberterrorism, critical infrastructure in Africa remains exposed to cyberattacks and requires a proactive approach to anticipate and mitigate emerging risks. Consequently, the challenges surrounding the definition of cyberterrorism should not shift policymakers' focus from protecting real world protections against attacks on critical infrastructure.

b. Cyberwarfare

Several high-profile cyber attacks initially targeted the military (Knapp & Boulton, 2007). For example, in 1986, an incident called the Cuckoo's Egg saw Clifford Stoll track down German hackers who infiltrated American military systems (Ibid). Another instance happened in 1994

when hackers broke into Griffis Air Force Base computers and used them to launch attacks against various military, civilian, and government organisations (Ibid). Like cyberterrorism, there is no universally accepted definition of cyberwarfare. As a result, I will present a few working definitions below.

Cyberwar is "a conflict between states, but it could also involve non-state actors in various ways. In cyberwarfare it is extremely difficult to direct precise and proportionate force; the target could be military, industrial or civilian or it could be a server room that hosts a wide variety of clients, with only one among them the intended target" (Cornish et al., 2010). This article seeks to provide caution as African countries transition to highly sophisticated critical infrastructure that relies on information technology. In this context, it is essential to highlight that perpetrators of acts of cyberwarfare can target military as well as non-military critical infrastructure. Consequently, civilian businesses hosting critical infrastructure must be ready to defend against cyberwarfare.

From a purely national military standpoint, Aldord defines cyberwarfare (CyW) as "any act intended to compel an opponent to fulfil our national will, executed against the software controlling processes within an opponent's system. CyW includes the following modes of cyber attack: cyber infiltration, cyber manipulation, cyber assault, and cyber raid" (Alford, 2000). Although this definition does not specify the quality of the opponent, whether military or civilian, it emphasises the use of manipulating software through cyber infiltration, manipulation, assault or raid to achieve a national interest. Alford's definition of cyberwarfare is limiting as advancing a national agenda may be limiting, as modern warfare can also be driven by religious beliefs or ideologies and business objectives not tied to a national agenda. As discussed in the section above, ransomware cyberattacks, where perpetrators of cyberattacks hold critical infrastructure systems hostage for financial gains, are rampant.

Although, Taddeo uses, "information warfare" to define cyberwarfare as "the use of ICTs within an offensive or defensive military strategy endorsed by a state and aiming at the immediate disruption or control of the enemy's resources, and which is waged within the informational environment, with agents and targets ranging both on the physical and non-physical domains and whose level of violence may vary upon circumstances" (Taddeo, 2011). This definition underlines the idea that acts of cyberwarfare could be acts of the state or private individuals. However, the state's endorsement is required when private entities execute acts of cyberwarfare.

Both definitions converge around the use of ICTs to commit cyberwar, connect cyberwar to military strategy, and highlight that cyberwar's principal objective is the disruption or control of information systems. However, they diverge on the actors involved, the requirement for state consent, the scope of objectives of cyberwar, and the range of targets and agents. The divergent views on the definition of cyberwarfare could significantly affect how governments shape their legal frameworks governing critical infrastructure. Although there is no consensus on the topic, African countries should include cyberwarfare and cyberterrorism in developing legal frameworks to protect critical infrastructure and define them from a risk-based approach. This approach will anticipate the negative manipulation of ICT systems that target critical infrastructure. Including such essential terms in the legal framework makes collaboration with other countries more fluid regarding collecting evidence and investigating the source of such crucial attacks.

National security is a cornerstone of critical infrastructure protection because if enemies successfully disrupt a country's information and security setup, the country can lose its security. The definition of cyberwarfare considers information and communication technologies (ICTs) since cyberwarfare seeks to disrupt or control the enemy's information and communication network. Taddeo's definition highlights that both state and non-state actors could propagate cyberwar, but it must receive official government assent for an act of cyberattack to qualify as state-sponsored. In the absence of international regulating cyber warfare, it is difficult to say with any degree of certainty if a non-state actor's attack against the critical infrastructure of another state amounts to cyber warfare. Generally, international collaboration is a critical feature in the fight against cybercrime. The Budapest Convention requires that governments prevent the commission of cybercrimes from their territories and collaborate and provide mutual assistance in the investigation and prosecution of suspects. While addressing critical infrastructure legislation, African countries should consider the possibility of external attacks by non-state actors without the consent of the state and provide for collaboration and mutual assistance in their new legal framework.

As cyberwarfare rages, it is essential to note that countries and non-state actors are improving their cyber capabilities and can attack critical infrastructure around the world for different reasons. For example, while the United States deployed a secret operation against Iran, Iran infiltrated a New York dam's computer control system and targeted financial institutions, took over their systems and prevented

customers from accessing their accounts online (Karagiannopoulos, 2020). Following these attacks, the United States (US) Department of "Homeland Security warned US companies to consider and assess the possible impact such an attack could have on their business" (Ibid). This example of cyberwarfare between the United States and Iran demonstrates that cyberwarfare may not necessarily be between state actors. A state actor or its affiliates may intentionally attack the critical infrastructure of private businesses in the exercise of cyberwarfare. In the example above, attacking water sources and financial institutions was directed at civilians and private businesses without a direct relationship with the government. This is a reminder that businesses running infrastructure critical to the existence and survival of a nation's economy must ensure they continually assess their cybersecurity and information systems to prevent such cyberattacks. The lack of a unified definition does not indicate the absence of cyberwarfare.

In light of Africa's economic development and the rise of critical infrastructure connected to information technology, it is important to note that cyberattacks on critical infrastructure aim to disrupt services and often demand ransomware. Regardless of whether they are classified as cyberterrorism or cyberwarfare, these attacks seek to achieve their objective by attacking systems. Therefore, African governments and businesses must develop legal and technical controls to prevent or limit the impact of cyberattacks on critical infrastructure and service provision, ensuring business continuity in case of attacks. According to Nathaniel Allen, in 2020, Ethiopia's INSA prevented a cyberattack by Egypt's Cyber_Horus Group aimed at exerting pressure on Ethiopia regarding the filling of the Nile River's Grand Ethiopian Renaissance Dam (GERD) (Allen, 2021). Leakages from AU servers were found to flow to Shanghai after China constructed the new AU headquarters and are suspected of leaving backdoors and planting listening devices (Ibid). Critical infrastructure in Africa, including banks and government entities like Johannesburg's municipal government, have suffered frequent cyberattacks, posing significant financial and operational risks (Ibid). While these developments may not be new to Africa, the frequency and magnitude of cyberattacks that could amount to cyberterrorism or cyberwarfare may increase with the rapidly increasing critical infrastructure and reliance on the internet for the provision of goods and services in Africa. The orderly protection of critical infrastructure starts with effective and enforceable legal frameworks. It is therefore important to review the legal steps taken so far to protect critical infrastructure linked to information systems.

3. International regulation of cyberwar and cyberterrorism

Except for the Budapest Convention on Cybercrime and the African Union Convention on Cyber Security and Personal Data Protection (discussed below), no specific rules in international law are designed specifically to govern cyberspace (Hollis, 2021). In addition to these two Conventions, the United Nations General Assembly has recognised the importance of protecting critical information infrastructure and expressed "concern that threats to the reliable functioning of critical information infrastructures and to the integrity of the information carried over those networks are growing in both sophistication and gravity, affecting domestic, national and international welfare (UNGA).

a. Existing international law regulating cyber terrorism and cyberwarfare

The term "terrorism" is ambiguous, legally undefined and there is no consensus on a definition of the derivative term "cyberterrorism", which is left to the unilateral interpretations of states (Marsili, 2018). The absence of an international legal framework to regulate cyberspace exacerbates the difficulty distinguishing cyberattacks as criminal acts, hacktivism, terrorism, or acts of aggression by nation-states as current international law regulates armed conflicts (Theohary & Rollins, 2015). However, international law applies to cyberspace since customary international law applies in the absence of specific treaties and should serve as the foundation for governing cyberspace (Moynihan, 2019). However, existing principles and rules of international law apply to state activities in cyberspace unless evidence of state practice indicates otherwise (Ibid). The question now turns to how current international law applies to cyberspace and how it regulates cyberwarfare and cyberterrorism.

International laws of war apply to all forms of warfare and weapons, including future weapons (Rodenhäuser, n.d.). Its basic rules prohibit targeting civilians and civilian objects, using indiscriminate weapons and attacks, conducting disproportionate attacks, and require respecting and protecting medical services (Ibid). Cyberattacks can have significant economic costs and disrupt essential services to the civilian population (Red Cross, n.d.). The healthcare sector and other critical infrastructure, such as electricity, water, and sanitation systems, are particularly vulnerable to these attacks and these attacks are reportedly becoming more frequent and severe (Ibid). According to the ICRC, "there is no question that cyber operations during armed conflicts are regulated by international humanitarian law– IHL– just like any other weapon or means or methods of warfare used by a belligerent in a conflict, whether

new or old" (Red Cross, n.d.). Evidently, the ICRC's view is limited to cyberattacks conducted during wartime or when cyber operations are used to facilitate physical attacks during the physical war. This view still leaves unanswered the critical question of whether international law regulates cyberwarfare and cyberterrorism during peacetime. With the absence of a global agreement governing cyberspace, the UN General Assembly passed a resolution acknowledging that ICT can be used for constructive or malicious intentions and urging all nations to employ ICTs for peaceful objectives and avert conflicts stemming from their use (UNGA). However, the resolution is not binding international law. The next part discusses ratified conventions on cybercrime and their influence over protecting critical infrastructure from cyberwarfare and cyberterrorism.

b. The Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime regulates specific crimes committed using ICTs, including illegal access, interception, interference, and deletion of data in articles 4 to 6 (Budapest Convention). Despite the focus on the proliferation of cyberterrorism and cyberwarfare, the Convention does not directly address cyberterrorism or cyberwarfare nor explicitly mentions the use of computers or ICT infrastructure to cause fear or intimidate the public or governments. The Budapest Convention on Cybercrime strongly advocates for cooperation between states in investigating and prosecuting crimes committed using ICTs with a focus on data. The preamble of the Convention clearly states that it "is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct" (Budapest Convention, n.d.).

This objective gives the impression that the Convention would provide substantive and procedural safeguards against using ICT systems to attack critical infrastructure. An analysis of Articles 4 to 6 of the Budapest Convention suggests their potential applicability in regulating critical infrastructure. These articles prohibit unlawful access, interception, and interference with data within an information system. In essence, cyber attackers intending to disrupt critical infrastructure generally access, intercept and interfere with the proper functioning of information systems to impede the production of vital goods and services essential for society's well-being. Again, it is visible from these analyses that even the Second Optional Protocol to the Budapest Convention that advocates enhanced cooperation and collaboration between

member states in investigating cyber crimes does not use language that suggests cyberterrorism and cyberwarfare. The Convention also does not mention critical infrastructure making it difficult to attach the importance of protecting critical infrastructure to the Convention. The absence of these important mentions make the African Convention on Cybercrime the only international treaty that mandates the protection of critical infrastructure.

c. The African Union Convention of Cybercrime and Personal Data Protection

The African Convention on Cyber Security and Personal Data Protection (The Malabo Convention) limits critical infrastructure to cyber or ICT infrastructure. The Convention defines *critical cyber infrastructure* as "infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace (The Malabo Convention)." Although the Malabo Convention restricts its definition of critical infrastructure to cyber infrastructure, it provides a framework for cyberinfrastructure to be used in advancing economic stability, security, public safety, and cyberspace. In today's highly technologically powered world, critical infrastructure functions on an efficiently operating information system. In addition to this definition, article 24 of the Malabo Convention calls on African states to develop national cybersecurity policies that recognise the importance of critical information infrastructure. Even though the Malabo Convention limits the definition of critical infrastructure to information infrastructure, it acknowledges that critical infrastructure constitutes different sectors that are essential to a country's economy and national security. This provides an opportunity to African policymakers to expand the definition of critical infrastructure in their local legal frameworks and establish the explicit relationship between critical infrastructure and the technology that enhances their functioning.

Despite the restrictive definition, the Convention signals the understanding by African states that Africa's economy and national security are highly or shall be potentially highly connected to the information and technologically advanced system, and their operation could potentially be subject to cyberattacks. Article 31 of the Malabo Convention requires States to adopt legislation restricting access to infrastructure classified as "critical national defence infrastructure" because such infrastructure contains strategic national security information and data. Although the Convention does not define "critical

national defence infrastructure", it appears to refer to critical cyber/ICT infrastructure used for national defence services, such as computer systems for national security or military operations (Orji). In addition to these policies, article 25 of the Malabo Convention requires African states to develop legislation identifying sectors sensitive to national security, economy, and information, communication and technology systems as elements of critical information infrastructure.

The Convention recognises that criminal law is a vital instrument to protect critical infrastructure since the rate of cybercrime in Africa is rising. The preamble of the Convention recognises that "the current state of cybercrime which constitutes a real threat to the security of computer networks and the development of the information society in Africa" must be regulated. This acknowledgment does not restrict the scope of cybercrimes or computer networks, and highlights the potential risk to all computer networks, including on critical infrastructure. While imposing obligations on States to adopt substantive criminal and procedural laws to protect information systems, the Convention requires States to cultivate a culture of cyber security. Article 26 of the Convention encourages the cultivation of a culture of cybersecurity among stakeholders and lays "emphasis on security in the development of information systems and networks, and on the adoption of new ways of thinking and behaving when using information systems as well as during communication or transactions across networks". The framers of the Convention likely understood that adopting and integrating ICT as a way of life would engender critical risks that could prove detrimental to the continent if Africans did not properly understand the opportunities and risks involved in connecting to cyberspace. Consequently, the article 26(4) requires States to "adopt measures to develop capacity building with a view to offering training which covers all areas of cybersecurity to different stakeholders and setting standards for the private sector." This requirement is timely and necessary as the private sector operates the vast majority of critical infrastructure and could be an easy entry point for cybercriminals. If all stakeholders protect their systems and regularly monitor them for vulnerabilities, they could substantially reduce cybercrime.

Irrespective of the steps taken to protect ICT systems from cybercrime, cybercriminals are always active and seeking to exploit vulnerabilities to gain access to the systems including critical infrastructure. Considering the importance of critical infrastructure to the economy and national security of African states, article 25 of the Malabo Convention requires severe criminal sanctions against cyber attackers who use ICT systems

to target critical infrastructure. In addition to protecting critical infrastructure, article 26 imposes on States to adopt effective legislation and regulations to regulate "by considering substantive criminal offences acts which affect the confidentiality, integrity, availability and survival of information and communication technology systems, the data they process and the underlying network infrastructure, as well as effective procedural measures to pursue and prosecute offenders." Article 29 recognises attempting to gain or gain unauthorised access to a computer system or using such unauthorised access to commit another crime or exceeding authorised access, which States should punish. Similarly, fraudulently remaining or using presence in a computer system to commit a crime or damage the computer system or data are also crimes under the Convention. Besides other cybercrimes enumerated in the Convention, these are the most significant that potentially infiltrate and disrupt a critical infrastructure from performing as intended. Although other enumerated crimes could hinder critical infrastructure, these appear critical to the functioning of critical infrastructure and computer networks. Although the Malabo Convention does not recognise cyberterrorism or cyberwarfare as crimes, it provides that using ICT to commit offences like terrorism among other crimes should be considered an aggravating circumstance (article 30).

The newly ratified African Continental Free Trade Agreement (AfCFTA), which seeks to advance economic growth and industrialisation in Africa and protect intellectual property rights, fails to make cybersecurity a central mechanism for achieving these objectives. This oversight is not business friendly because, irrespective of its form, cyberattacks can also result in the theft of sensitive information and intellectual property which harms a company's reputation and leads to financial losses. In addition, businesses that rely on information technology may be vulnerable to cyberattacks that disrupt their operations, leading to lost productivity and revenue and hinder their flow within the continental free zone. Businesses may be held liable for cyberattacks that harm customers or other third parties, which can result in legal and financial consequences. Therefore, it is important for businesses to continually assess their cybersecurity and information systems to prevent such cyberattacks. Since the AfCFTA is business focused, it should have complemented the Malabo Convention's silence on the gravity of cyberterrorism and cyberwarfare targeting critical infrastructure designed to foster the free movement of goods and people in Africa. The next section will review the legal protections of critical infrastructure in Ghana and Cameroon although Cameroon has

not ratified the Malabo Convention. Ghana ratified the Convention in June 2019 while Cameroon only signed in August 2021.

4. Regulation of critical infrastructure in Ghana

Before "critical infrastructure" became the word of the art to describe systems vital to a nation's operation and wellbeing, governments protected some infrastructures for military and civilian purposes.

a. Designation of critical infrastructure

In Ghana, section 35 (1) of the Cybersecurity Act (the Act) authorises the Cyber Security Authority may request that the government "designate a computer system or computer network as a critical information infrastructure if ... the computer system or computer network is essential for national security, or the economic and social well-being of citizens." Cameroon's cybersecurity law does not mention critical infrastructure making it difficult to identify a comparison between the designation of these infrastructure between Cameroon and Ghana. However, sectoral laws like the section 7 of the Telecommunications Law (telecoms law) require the protection and safety of users and personnel operating telecommunications networks, the protection of networks and associated control and management information exchange. This recognition does not meet the minimum requirements for the designation of critical infrastructure. The designation of critical information infrastructure considers if it is vital for national security, defence, law enforcement, communication, finance, public utilities and transportation, and other important public infrastructure (section 35(3) of the Act. In designating critical information infrastructure, Ghana's Directive for the Protection of Critical Information Infrastructure recognises that "Cyber-attacks against CIIs are increasing, the magnitude, frequency and impact of such security incidents can impede the pursuit of economic activities, generate substantial disruption to critical services, financial losses, undermine public confidence, and cause major disruption to our economy." The acknowledgement by the Ghana Cybersecurity Authority (GCA) is relevant to Cameroon since the lack of legal recognition for critical infrastructure does not imply their nonexistence. Like Ghana, Cameroon is experiencing economic growth, and the increasing adoption of information technology to spur economic growth inevitably constitutes cybersecurity vulnerabilities through which critical infrastructure could be attacked.

Section 92(1) of Ghana's Cybersecurity Act empowers the GCA to establish the baseline for cybersecurity, including issuing directives to

owners of critical information infrastructure and cybersecurity service providers to ensure the country's cybersecurity (Ghana's Cybersecurity Act, 2020). All designated critical information infrastructure in Ghana must comply with the requirements and procedures for incident response and cybersecurity reporting and procedures for compliance and audit (DCPII).[1]Accordingly, Ghana has designated thirteen sectors as critical information infrastructure.[2] In contrast to the United States, which designated 16 sectors as critical, Ghana designated 13 as critical, excluding commercial facilities, dams, defence industrial, nuclear reactors, materials, and waste from its list. Almost all these sectors of the economy in Ghana and the United States also exist in Cameroon, are connected to information technology and are critical to Cameroon's economic and national security survival. However, they enjoy heightened levels of protection in Ghana and the United States unlike in Cameroon that has not designated critical infrastructure.

b. Risk assessment and audits of critical infrastructure

In order to guarantee that critical infrastructure services remain sustainable and accessible, Section 1016(4) of Patriot Act requires their prioritisation, security and adherence to regulations and standards (The Patriot Act, 2001). Protecting critical infrastructure against cyberattacks requires stakeholders to understand the interdependencies between infrastructure and its network (OECD/LEGAL/0361). A risk assessment process analyses vulnerabilities and threats to the infrastructure and maps the interdependencies and networks associated with the infrastructure (OECD/LEGAL/0361). Risk assessment evaluates compliance with organisational and regulatory frameworks and controls (OECD/LEGAL/0361). These measures encompass prevention, protection, response, recovery, and continuous evaluation, ensuring a strong defence against cyber threats for business continuity (OECD/LEGAL/0361).

Ghana's Cybersecurity Act (Sections 38 and 39) reflect the above requirements by requiring GCA to "carry out a periodic audit and inspection on a critical information infrastructure to ensure compliance." The cybersecurity authority can conduct the audit, assign an authorised auditor, or validate an audit undertaken by the designated critical infrastructure (DCPII). Consequently, the risk assessment and audit processes of critical infrastructure are flexible. This flexibility ensures that internal audit teams can conduct timely internal audits to identify security

1. Ghana's Directive for the Protection of Critical Information Infrastructure.
2. Ghana's Direction for the Protection of Critical Information Infrastructure lists National Security and Intelligence, Information and Communication Technology, Banking and Finance, Energy, Water, Transport, Health, Emergency Services, Government, Food and Agriculture, Manufacturing, Mining and Education.

vulnerabilities and apply corrective measures. To ensure compliance, designated critical information infrastructure must submit audit reports and a risk register to the cybersecurity authority for approval (DCPII). However, planned activities that may impact the availability of services require pre-approval from the authority (DCPII). Due to the indispensable role critical infrastructure plays in the functioning and continuity of society, the unavailability of these systems can lead to significant disruptions, losses, and widespread fear and chaos. Consequently, it is important that authorities engage in collaborative planning with stakeholders and inform the public of possible disruptions and unavailability of services. This proactive approach not only facilitates prompt detection of cyberattacks but helps authorities to ensure the continuity of services. This communication requirement also satisfies the public interest in the continuos and effective functioning of critical infrastructures since most critical infrastructure serve essential human needs.

5. Duties of designated critical infrastructure

In addition to the audit requirements above, a designated critical information infrastructure shall institute basic technical, operational, and management requirements and controls to ensure the protection of the critical information infrastructure and manage risks and vulnerabilities. The United States' Framework for Enhancing Critical Infrastructure Cybersecurity adopts a comprehensive cybersecurity risk management approach. Common to all cybersecurity risk management frameworks, the core framework adopts five concurrent and continuous functions that should guide management's actions. These functions include identify, protect, detect, respond, and recover (NIST, 2022).

a. Critical infrastructure governance

Ghana's Critical Infrastructure Directive requires designated critical infrastructure to adopt cybersecurity policies conforming with international best practices in the relevant sector relevant to their sector of designation (DCPII). The directive also requires critical infrastructure owners to adopt internal cybersecurity policies that comply with the Authority's directives and obtain the approval of their board of directors (DCPII). Designated critical infrastructure must also appoint a senior manager for cybersecurity governance to oversee and enforce the cybersecurity program (DCPII). Consistent with best practices in the designated sector, the infrastructure's cybersecurity policy shall be reviewed annually, consistent with identified risks and threats (DCPII). Managing a critical infrastructure includes adopting policies

that look at the big picture and implementing measures that secure the infrastructure against cybersecurity attacks (Zhang).

b. Technical and organisational protection of critical infrastructure

Governments are concerned about the adequacy of the cybersecurity mechanisms protecting critical infrastructure, mainly when cybersecurity controls are automated, unmanned and remotely accessed (Dawson et al., 2021). Automated, unmanned and remotely accessed cybersecurity infrastructure can quickly become susceptible to vulnerabilities and exploitation. Consequently, governments are increasing legal requirements to ensure stringent protections when deploying and managing such systems. Ghana's Cybersecurity Authority mandates designated critical infrastructure organisations to adopt technical and organisational measures to protect their systems. Amongst these enumerated measures, the authority recommends the adoption of relevant international cybersecurity best practices, frameworks and standards approved by the Cybersecurity Authority (DCPII). Since the authority does not give details on the identified measures, the next few paragraphs will discuss the controls identified in the Critical Infrastructure Directive in line with relevant NIST controls that are relevant to Ghana's framework.

The Directive requires critical system owners to identify, classify and catalogue critical infrastructure assets (DCPII). It is important to acknowledge that the assets, systems, and functions that comprise critical infrastructure play different roles, attract different levels and types of risks and do not require the same level of protection. This understanding informs the requirement to develop a comprehensive, prioritised assessment of critical infrastructure assets. Developing and maintaining cyber resilient critical infrastructure require "owners and operators identify assets, systems, and networks that are essential to their continued operations and delivery of products and services to customers (NIPP, 2013)." The NIST RMF identifies assets as tangible and intangible elements that contribute to achieving a business objective and cover the necessary information for operations, services, and system management (NIST 800-37 rev 2, 2018). Organisations identify assets and determine the level of protection required based on the value stakeholders attach to a designated critical infrastructure (Ibid). These categorisations follow the organisation's missions or business functions and interconnected systems (Ibid).

Organisations can also catalogue or document assets within the system's security and privacy plans (Ibid). These information

identification, classification and documenting processes help determine the protection plans required for the organisation (Ibid). "Although there are a certain number of methodological solutions that companies can currently adopt to deal with cybersecurity in ..., little importance is given to the analysis of critical assets to be protected and the related assessment of business impacts" (Corallo et al., 2020). As such, they propose "a structured classification of critical assets to be protected against cyber-attacks ... and the potential impacts on business performance" (Ibid). The structured asset classification approach gives an organisation a clear view of the criticality of their assets and their role in protecting the infrastructure from attacks, cyberterrorism or cyberwarfare. Within the context of the growing interconnectedness in Africa and the potential rise in cybercrimes targeting critical infrastructures, African governments must require critical information owners to establish clear sets of critical assets with the goal of identifying the protection levels required for each asset.

A carefully executed asset identification and classification process helps management determine the levels of sensitivity and confidentiality to assign each asset. This facilitates managing access to different assets depending on roles, responsibilities and vulnerabilities. Evidently, access control becomes an essential element of security within the designated critical infrastructure and the process is used to determine who is allowed to access data depending on its classification. Organisations rely on techniques like authentication and authorisation to grant access to critical infrastructure.[1] Ghana's Cybersecurity Act requires that individuals or corporations seeking access to critical information infrastructure obtain prior authorisation.[2] Account controls include account management processes, such as using automated mechanisms to create, manage, disable and deactivate accounts based on need (NIST 800-53 r 5, 2023). Access control through privileged user accounts, role-based accounts, and least privilege require that organisations grant access to critical assets based on specific roles assigned to individuals (Ibid). Since these roles allow particular individuals to perform security-relevant functions, they can access assets that others should not (Ibid). Access management is a wide control family and requires different particular attributes and controls including remote access. When an organisation's assets are accessed from external networks, such as the internet, it can pose a threat to the security of the infrastructure (Ibid). To mitigate this risk, organisations should use automated tools to monitor

1 See generally, https://www.microsoft.com/en-us/security/business/security-101/what-is-access-control.
2 See generally section 40 of Ghana's Cybersecurity Act, 2020. See also the 5.1(b) of Critical Information Infrastructure Directive.

and regulate remote access, and employ encryption to safeguard the privacy and integrity of remote access sessions. Remote access controls are very important since anyone can access data from anywhere without prior authorisation. The automated monitoring tools will immediately notify the asset owner if someone attempts to access the asset from an unauthorised location or an unauthorised device (Dawson et al., 2021). While the focus for cybersecurity could be protecting external threats, internal stakeholders could equally constitute serious cybersecurity threats and vulnerabilities.

The access control strategies discussed above must be complemented with cybersecurity awareness to ensure internal stakeholders do not compromise the security of the infrastructure. Stakeholders who may have legitimate authorisation to access the asset systems include employees, contractors, suppliers, external auditors, customers etc. Despite the legitimate authorisation to access the organisation's infrastructure, they could consciously or unconsciously constitute a threat to the network. Organisations can organise mandatory cybersecurity awareness training that helps internal stakeholders identify insider threats, social engineering, and advanced persistent threats (NIST 800-53 r 5, 2023: 59-64). Cybersecurity training can be categorised according to its content, sensitivity, business organisation, activities, participants, level, availability, or frequency (Beuren et al., 2016). Closely related to training and awareness is media protection. An organisational policy that defines how stakeholders use media, whether removable or static, helps shape the organisation's cybersecurity posture. Media policy would include instructions on media access, storage, transport, sanitisation, and use (NIST 800-53 r 5, 2023: 59-64). As the understanding grows that the Stuxnet worm, which targeted the Iranian Bushehr nuclear power plant, predominantly propagates through USB sticks, it becomes essential to define and enforce controls to regulate the use of media devices (Schneier, 2010). These control mechanisms represent a tiny fraction of the NIST framework. However, these controls will not be significant unless organisations manage, document, and report cybersecurity incidents.

c. Incident management and reporting

Cybersecurity controls will not effectively deter cyberattacks directed at critical infrastructure if these infrastructure owners, government, and other stakeholders do not document and report incidents for continuous learning. It is important to notify competent State authorities about cyber threats and incidents that could incapacitate a designated critical

infrastructure (Schimdt-Berndt, 2023). Timely notification allows authorities to assist the affected entity in managing the incident and design strategies to protect other entities from experiencing a similar incident (Ibid). The importance of timely reporting of cybersecurity incidents informs why critical information infrastructure owners and operators in Ghana must investigate, report and mitigate the impact of cybersecurity incidents within 24 hours of becoming aware of the incident (DCPII). Similarly, operators must report vulnerabilities discovered through audits and risk assessments within 72 hours of discovering or identifying the vulnerabilities (DCPII). While reporting incidents and breaches to State authorities is important to ensure the critical infrastructure sector and related or interconnected sectors are protected against spreads, reporting all vulnerabilities discovered at every audit and risk assessment will put too much pressure on the operator or owner of the critical infrastructure. A risk management register or a plan of action and milestones would help document identified vulnerabilities and indicate the progress made in addressing them.

While Ghana's Directive does not provide steps for processing incidents, NIST recommends that incident response should contain incident handling, monitoring, reporting and a response plan amongst others. Incident response training accompanied with incident response plans should constitute critical components of incident management since system users and responders must understand how to react, document and report incidents. In addition to training, organisations should provide the necessary tools and equipment for incident management (NIST 800-53 r 5, 2023: 275-297). Organisations should activate automated mechanisms to handle incidents and collect the data required for documentation and reporting (Ibid). An essential aspect of incident management is factoring in business continuity in case of a cyberattack that incapacitates critical information infrastructure from performing (Ibid). While organisations should have security operations centres (SOC) that "defend and monitor an organisation's systems and networks ... on an ongoing basis. The SOC is also responsible for detecting, analysing, and responding to cybersecurity incidents in a timely manner" (Ibid). Ghana does not require critical infrastructure operators to operate SOC. Instead, Section 42 of the Cybersecurity Act requires operators to report incidents to the relevant National Computer Emergency Response Team (N-CERT) that is responsible for cybersecurity incidents and coordinate response between public and private stakeholders. The Cybersecurity Authority must equip the N-CERT with relevant tools to effectively respond to cybersecurity incidents. In addition to N-CERT, Ghana's Cybersecurity

Act authorises the Cybersecurity Authority to create Sectoral Computer Emergency Response Teams (C-CERT) based on the criticality and needs of the sector to collect and collate cybersecurity incidents and coordinate responses. This centralised approach reduces the financial and other burdens associated with operating SOC but takes away the important role that SOCs play in continuously monitoring the critical information infrastructure for vulnerabilities, breaches, and violations. This exposes the infrastructure to untimely detection of incidents and the ramifications may be dangerous to the critical information infrastructure and the nation as a whole.

Conclusion

In conclusion, the legal protection of critical infrastructure in Africa is critical for the continent's development and growth. Critical infrastructure is vulnerable to cyberterrorism and cyberwarfare, although they are nascent concepts in the cybersecurity industry and are still developing. As Africa invests in critical infrastructure to drive economic advancement, improve innovation, and encourage the movement of goods and services across the continent, legal instruments are fundamentally needed to protect the critical infrastructure. As seen in this article, cyberterrorism and cyberwarfare can destroy critical infrastructure and endanger the economic and national security postures of countries. Worse, some acts of cyberterrorism and cyberwarfare could be sponsored by state actors. With warfare and cyberterrorism becoming the next level of competition between countries, African nations must protect themselves by adopting the best industry standards. In addition to state actors, malicious individuals can take over an entire critical infrastructure system and run it aground until they have received a ransom. The payment of ransoms plus economic, financial, legal and reputational costs can incapacitate an infrastructure and expose a country to economic and national security risks. Adopting cybersecurity laws and controls is non-negotiable if Africa intends to boost its innovation, economic, and developmental capacities. African policymakers should quickly develop legal processes to protect critical infrastructure from cyberterrorism and cyberwarfare. In the meantime, businesses operating in critical infrastructure sectors as defined in other countries can take industry measures to ensure the protection of their businesses and avoid unnecessary losses. Waiting on the development of accurate legal frameworks may cause significant damage to the businesses if cyberattackers strike their businesses.

Ethical considerations
The author has completely considered ethical issues, including informed consent, plagiarism, data fabrication, misconduct, and/or falsification, double publication and/or redundancy, submission, etc.

Conflicts of interests
The author declares that there is no conflict of interests.

Data availability
The dataset generated and analyzed during the current study is available from the corresponding author on reasonable request.

References

Alford, J. (2019, October 02). *imperial.ac.uk*. Retrieved from https://www.imperial.ac.uk/news/193151/nhs-cyber-attacks-could-delay-life-saving-care/#:~:text=A%20new%20analysis%20has%20revealed,be%20almost%20%C2%A36%20million.

Alford, L. (2000). "Cyberwarfare: Protecting Military Systems". *Acquisition Review Quarterly.* 101-120.

Allen, N. (2021, January 13). *africacenter.org*. Retrieved from https://africacenter.org/spotlight/africa-evolving-cyber-threats/.

Allianze. (n.d.). *alliance.com*. Retrieved from https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html.

Beuren, R., Chinen, K.I., Tan, Y. & Shinoda, Y. (2016). "Towards Effective Cybersecurity Education and Training." Retrieved October 11, 2023 from: https://www.jaist.ac.jp/~razvan/publications/effective_cybersecurity.pdf.

Bolonga, S., Fasani, A. & Martellini, M. (2013). "Cyber security and resilience of industrial control systems and critical infrastructures". In M. Martellini. *Cyber Security: Deterrence and IT Protection for Critical Infrastructures.* SpringerBriefs.

Budapest Convention. (n.d.).

Budd, J., Miller, B.S., Manning, E.M., Lampos, V. et al. (2020). "Digital technologies in the public-health response to COVID-19". *Nature Medicine.* 1183-1192.

ISA. (n.d.). *www.cisa.gov*. Retrieved from Critical Infrastructure Security Agency: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Collier, R. (2017). "NHS ransomware attack spreads worldwide". *Canadian Medical Association Journal.* 786-787.

Corallo, A., Mariangela, L. & Lezzi, M. (2020). "Cybersecurity in the

Context of industry 4.0: A structured classification of critical assets and business impacts". *Computers in Industry*.

Cornish, P., Livingstone, D., Clemente, D. & Yorke, C. (2010). *On Cyberwarfare.* London: Chatham House.

Corrigan, T. (2020). *saiia.org*. Retrieved from https://saiia.org.za/wp-content/uploads/2020/06/Policy-Briefing-197-corrigan.pdf.

Dawson, M. et al. (2021). "Understanding the challenge of cybersecurity in critical infrastructure sectors". *Land Forces Academy Review*, 69-75.

DCPII. (n.d.). Directive for the Protection of Critical Information Infrastructure.

Denning, D.E. (2000, May 23). *faculty.nps.edu*. Retrieved from https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm.

Dibie, A. & Okwonko. (2000). *The Importance of Infrastructure in Business Enterprises. Leading Issues in the Political Economy of Nigeria.* Owerri.

Executive Order on Improving Critical Infrastructure Cybersecurity. (2013). The Government of the United States.

Ghana's Cybersecurity Act. (2020). Ghana's Cybersecurity Act, 2020. The Ghana Government.

Goth, L. (n.d.). *www.leachagency.com*. Retrieved from https://www.leachagency.com/malware-the-main-weapon-of-cyberattacks/.

Kesici Çalışkan H. (2015). "Technological change and economic growth". *Procedia Social and Behavioral Sciences.* 649-654.

Hollis, D. (2021, June 21). *carnegieendowment.org*. Retrieved from https://carnegieendowment.org/files/Hollis_Law_and_Cyberspace.pdf.

INTERPOL. (2021). Africa Cyber Threats Assessment, INTERPOL's Key Insights into CyberCrime in Africa.

Karagiannopoulos, V. (2020, January 10). *theconversation.com*. Retrieved from https://theconversation.com/how-real-is-the-threat-of-cyberwar-between-iran-and-the-us-129573.

Knapp, K. & Boulton, W. (2007). "Ten Information Warfare Trends". In L. Janczewski, & A. Colarik, *Cyberwarfare and Cyber Terrorism.* pp. 17-25. IGI Global.

Le Bris, A. & El Asri, W. (2017). *ESSEC Business School.* Retrieved from blogs.harvard.edu: https://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf.

Lewis, J. (2003). *Assessing the Risks of Cyber Terrorism, Cyberwar and Other Cyber Threats.* Centre for Strategic and International Studies.

Marsili, M. (2018). The war on cyberterrorism. *Democracy and Security.* 172-199.

McKinsey. (n.d.). *Mckinsey.com*. Retrieved from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/

cybersecurity/cybersecurity-trends-looking-over-the-horizon.
Moteff, J.A. (2004). *Critical Infrastructure and Key Assets: Definition and Identification.* Library of Congress.
Moynihan, H. (2019). *The Application of International Law to State Cyberattacks Sovereignty and Non-intervention.* Retrieved October 8, 2023 from: https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks.
Newbill, C.M. (2019). "Defining critical infrastructure for a global application. *Indiana Journal of Global Legal Studies.* 761-780.
NIPP. (2013). Partnering for Critical Infrastructure Security and Resilience.
NIST. (2022). *Framework for Improving Critical Infrastructure Cybersecurity.*
NIST 800-37 rev 2. (2018). Manangement Framework for Information Systems and Organzations. 38-40.
NIST 800-53 r 5. (2023). NIST Security aand Privacy Controls for Information Systems and Orgaanizations. 18-58.
OECD. (2008). *Recommendation of the Council on the Protection of Critical Information Infrastructures.* Retrieved October 6, 2023 from: https://legalinstruments.oecd.org/public/doc/121/121.en.pdf.
OECD/LEGAL/0361. (n.d.). Recommendation of the Council on the Protection of Critical Information Infrastructure. OECD.
Orji, U. (n.d.). "The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability?". *Masaryk University Journal of Law and Technology*.
Patriot Act. (2001). *Section 1016(e)*.
Primoraz, I. (2019). "What is terrorism?". *Journal of Applied Philosophy*. 129-138.
Qureshi, Z. (2020, February). *brookings.edu*. Retrieved from https://www.brookings.edu/articles/technology-and-the-future-of-growth-challenges-of-change/.
Red Cross. (n.d.). *icrc.org*. Retrieved from https://www.icrc.org/en/document/cyber-warfare-ihl-provides-additional-layer-protection.
Riggi, J. (n.d.). *aha.org*. Retrieved from https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed.
Rodenhäuser, T. (n.d.). *icrc.org*. Retrieved from https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law.
Rufus, A. & Bufumoh, P.E. (2017). "Critical infrastructure decay and development crises in Nigeria. *Global Journal of Human-Social*

Science. 17(2), 1-9.

Schimdt-Berndt, S. (2023). "Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive". *Journal of Cybersecurity*, 9(1). https://doi.org/10.1093/cybsec/tyad009.

Schneier, B. (2010). *Forbes*. Retrieved from https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html?sh=1b18b68051e8.

Shiryaev, Y. (2012). "Cyberterrorism in the context of contemporary international law". *San Diego International Law Journal.* 139-192.

Taddeo, M. (2011). "Information Warfare: A philosophical perspective". *Philosophy and Geography*. 105-120.

Tahir, R. (2018). "A study on malware and malware detection techniques". *International Journal of Education and Management Engineering.* 20-30.

The Malabo Convention. (n.d.).

The Patriot Act, 2001. (n.d.).

Theohary, C. & Rollins, J. (2015). *Cyberwarfare and Cyberterrorism: In Brief.* Library of Congress.

Tome, A., Fishbane, L., Siefer, A. & Callahan, B. (n.d.). *Brookings.edu*. Retrieved from brookings.edu.

Turton, W., Riley, M. & Jacobs, J. (2021, May 13). *bloomberg.com*. Retrieved from https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom?in_source=embedded-checkout-banner.

UK Department of Health and Social Care. (2018). *Securing cyber resilience in health and care.* London.

UNGA. (n.d.). A/RES/64/211, Resolution on the Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures.

Uzoh & Baulo. (2013). "Improving critical infrastructure for sustainable development in Nigeria towards the realization of vision 20:2020". *International Journal of Economic Development Research and Investment*. 30-38.

Weenk, S. (2020). "National cybersecurity strategies in the healthcare industry of Israel and the Netherlands: A comparative overview. *Cyber, Intelligence, and Security.* 107-129.

Zhang, Z. (n.d.). "Cybersecurity Policy for the Electricity Sectoor: The First Step to ProtectingOur Critical Infrastructure from Cyber Threats". *Boston University Journal of Science and Technology Law.* 2013.