Volume 3 (2025)

ISSN: 2959-3018 (print) / 2959-3026 (online)
thecommonwealth.org/cyber-journal

The Commonwealth Cyber Journal

The Commonwealth

Foreign, Commonwealth & Development Office

About the journal

The Commonwealth Cyber Journal (CCJ) is an annual journal published by the Commonwealth Secretariat that features peer-reviewed, policy-influencing articles and commentary by academics, policymakers, practitioners and experts on the benefits, challenges and risks of digital technologies. It seeks to analyse challenges and opportunities arising from different aspects of cybercrime, cyberlaw and cybersecurity, and to serve both as a toolkit and resource for practitioners, legislators, and academics cybercrime and as a decision support instrument for stakeholders (state/non-state actors) as they seek to strengthen their countries' cyber legislation.

The journal's areas of focus include but are not limited to: state actors and cyber warfare; ransomware and phishing; proceeds of crime; terrorism, privacy and security of data; intellectual property; infringement and counterfeit; online harassment and cyberstalking; election cybersecurity; virtual courts and electronic evidence; cybersecurity and the economy; digital currencies; and child online safety. Articles published in the journal specifically focus on the Commonwealth region, and/or include case studies concerning one or more Commonwealth countries; similarly, article authors are typically drawn from Commonwealth countries.

For full details, including aims and scope, and guidelines for submission, see thecommonwealth.org/cyber-journal

Commonwealth Cyber Journal \ 1
ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cyber-journal

Editorial

Nkechi Amobi

The Commonwealth Secretariat, sponsored by the UK government, continues to undertake numerous capacity-building initiatives to enhance the cyber resilience of its member countries through collaboration and innovative practices.

As the digital landscape continues to evolve at a staggering pace, the *Commonwealth Cyber Journal* provides a vital platform to explore the pressing cyber challenges and opportunities facing nations across our shared community. Technological innovation offers remarkable opportunities and undoubtedly makes our lives more convenient and our society more efficient, but these changes also bring with them exposure to issues in the areas of security. As the Commonwealth continues to embrace the possibilities of the digital age, we are confronted with complex and evolving cyber threats that transcend borders.

This edition of the *Commonwealth Cyber Journal* brings to the forefront key issues that demand our collective attention and action. We are proud to present articles offering insights and practical approaches to protecting critical information infrastructure, an area of growing concern as essential services and national assets increasingly rely on interconnected systems. Lessons shared in this edition highlight the vulnerabilities of member countries and the innovative strategies being deployed to secure these vital sectors. As digital platforms become arenas for harassment, coercion, and harm, the need for a coordinated response rooted in human rights and gender-sensitive approaches becomes more paramount. The contributions in this issue challenge us to consider how cyber policies practices and guidelines may better protect the most vulnerable among us.

This volume assesses how honeypots are becoming increasingly valuable tools in understanding and mitigating cyber threats. Exploring this technique within the Commonwealth context offers practical guidance and broader reflections on proactive cybersecurity measures. As a diverse family of nations, we have much to learn from one another, and the *Commonwealth Cyber Journal* remains committed to amplifying these conversations. We encourage all readers— policymakers, practitioners, researchers, and the public—to engage with the ideas presented in this edition and consider how they may be applied within their contexts. Cybersecurity is not solely a technical issue but a matter of national resilience, human security, and collective responsibility.

As we look ahead, let us reaffirm our shared commitment to a secure, open, and inclusive cyberspace for the benefit of all Commonwealth citizens.

The *Commonwealth Cyber Journal* (*CCJ*), published by the Commonwealth Secretariat, serves as a platform for disseminating cutting-edge research, policy influencing articles, case studies and commentary from practitioners, policy-makers and academics in the field of cybersecurity and cybercrime. The objective of the *CCJ* is to assist Commonwealth countries to strengthen their anti-cybercrime legislative, policy, institutional and multilateral frameworks to uphold the rule of law in both virtual and physical spaces.

In this issue

In this third issue of the *Commonwealth Cyber Journal (CCJ)*, contributors explore a range of important topics. These include the use of Advanced Cyber Defence (ACD) by private corporations to safeguard their operational data and that of their customers. The issue also addresses the effectiveness of current laws and regulations in preventing cybercrime and protecting personal information within the Commonwealth.

Other articles in this volume explore international legal frameworks for combating Online Child Sexual Exploitation and Abuse (OCSEA) and compare them with existing legal systems in the MENA region. Additionally, contributors examine the global challenge of cybersecurity in smart grids from the perspectives of several Commonwealth countries, and national cybersecurity frameworks.

Furthermore, the issue examines the connection between cybercrime and online gambling, as well as legislation targeting cyberstalking and technology-facilitated intimate cyberviolence.

In *The Use and Legality of Honey Pots, Tracers, and Trackers in Australia*, **Brendan Walker-Munro et al**. tackle an important topic in cybersecurity today. As cyber attackers—state-sponsored, criminal, or opportunistic—become increasingly sophisticated, the role of proactive defence mechanisms like ACD comes to the forefront. This paper introduces the most common forms of ACD, including decoy assets and tracking technologies, and examines the significant legal, ethical, and regulatory dilemmas associated with their use. Through a focus on Commonwealth jurisdictions, notably Australia, the authors propose much-needed legal reforms to enable ACD as a legitimate tool for private sector resilience—an important contribution to ongoing global cybersecurity policy and law debates.

In his article, *Strengthening Cybersecurity and Data Protection Frameworks in Commonwealth Member Countries: Policy and Institutional Approaches*, **Otshepeng Mazibuko** examines how Commonwealth countries are addressing the gaps in safeguarding personal information. The article assesses the unevenness in current regulatory frameworks and international cooperation in a world where data flows seamlessly across borders. Highlighting key issues such as cybersecurity capacity building, cross-border data sharing, and digital sovereignty, Mazibuko calls for a renewed

commitment to international collaboration that balances local needs and realities. This is an essential roadmap for Commonwealth countries seeking to strengthen their cyber resilience while respecting individual rights.

Mohamed Hemdani's piece, *Cyberstalking and Intimate Partner Violence: How Technology Escalates Abuse (OCSEA)*, offers a comparative analysis of international and MENA regional legal frameworks. By examining jurisdictions such as Egypt, Saudi Arabia, and the UAE and comparing them with systems like the United Kingdom, Hemdani reveals critical gaps and cultural complexities in addressing OCSEA. Given the global nature of these crimes and the vulnerabilities they exploit, his call for harmonised, culturally sensitive, and enforceable legal frameworks is both timely and urgent.

The article *Cybersecurity Threats to Critical Energy Infrastructure: Challenges and Opportunities for Developing Nations*, written by **Rohini Haridas et al.,** focuses on a critical yet underexamined area: energy infrastructure. As nations embrace the benefits of smart grids, the vulnerabilities inherent in these interconnected systems grow. Drawing on the case of India, this paper highlights the specific challenges developing countries face—limited resources, policy gaps, and the accelerating digitisation of critical infrastructure. The analysis highlights the need for comprehensive security frameworks that can keep pace with the rapidly evolving threat landscape of energy systems.

Focusing on Nigeria, **Samuel Iheanyi Nwankwo**, in his paper *Strengthening Nigeria's Cyber Frontier: Building Resilience Through Legal Innovation*, addresses the urgent need for a modernised cybersecurity framework in one of Africa's largest economies. Through a detailed examination of Nigeria's fragmented and outdated legal and institutional landscape, Nwankwo proposes a "resilience-based blueprint"—a forward-looking approach that integrates preparedness, adaptability, and recovery into national cybersecurity efforts. His recommendations for proactive legislation, robust incident response, and capacity building provide an actionable pathway to enhancing Nigeria's—and, by extension, similar jurisdictions'—cybersecurity posture.

From the African continent to South Asia, **Md Masudul Islam Khan** et al. highlight *The Nexus between Cybercrime, Financial Fraud, and Online Gambling in Bangladesh*. Their research examines how illicit online gambling platforms could facilitate money laundering and fraud, exploiting gaps in regulation and enforcement. By shedding light on how social media, digital payment systems, and bureaucratic inertia contribute to this growing problem, the authors advocate for urgent legislative reforms and improved cross-border cooperation to tackle these emerging cyber-financial crimes.

Chioma Aneh's article, *Cyberstalking and Intimate Partner Violence: How Technology Escalates Abuse*, explores cyberstalking as a form of technology-facilitated intimate partner violence (TFIPV) in Nigeria, Kenya, and South Africa. It examines how digital tools, such as spyware and social media surveillance, are used against victims, highlighting legal gaps and inadequate support systems. Despite global frameworks like the Budapest Convention, African responses remain fragmented. The study advocates for

harmonising laws, improving law enforcement training, enhancing digital literacy, and holding tech companies accountable while emphasising survivor-centred approaches in cybercrime strategies.

Together, these contributions reflect the diversity of cyber challenges confronting Commonwealth nations—spanning advanced industrial economies and emerging markets alike. The *Commonwealth Cyber Journal* remains committed to fostering dialogue, research, and action that bridge legal, policy, and technical domains, recognising that cyber threats are as varied as they are complex.

The Commonwealth

Commonwealth Cyber Journal \ 5
ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cyber-journal

The Use and Legality of Honeypots, Tracers and Trackers in Active Cyber Defence

Brendan Walker-Munro[1], Andrew Cox[2], Grant Haroway[3], Joe Otway[4], Duncan Unwin[5] and Sascha Dov Bachmann[6]

Abstract

Australia, as an open market economy and democracy, is both dependent and reliant on the internet and online security for its prosperity, way of life and the functioning of our democracy. Cybersecurity, as a prerequisite for ever-increasing interconnectivity, is under assault from cyber-attacks and malicious cyber activity being conducted by states and 'hybrid actors', such as cybercriminals and syndicates.

Cyber-attacks pose a serious threat to the security and integrity of entities, especially when they involve trusted insiders who have access to sensitive data and systems. To counter this threat, this paper proposes that use of active cyber defence (ACD) – such as fake files and credentials that alert the security team when accessed by unauthorised users or tracking devices that report the network activity and location of genuine trading information – can deter and detect malicious actors, often more efficiently and effectively than other methods alone. By using these ACD techniques, organisations can increase their chances of preventing and identifying cyber-attacks, as well as of collecting evidence for potential legal action. However, this paper also acknowledges that there are some challenges and risks associated with the use of ACD, particularly in, though not limited to, the private sectors, such as ethical, privacy and regulatory issues. Therefore, this paper provides a legal analysis of the implications of using teasers and tracers in different jurisdictions, and highlights the following points:

1 Senior Lecturer (Law), Faculty of Business, Law and the Arts, Southern Cross University, Australia. Email: brendan.walker-munro@scu.edu.au
2 President, Active Cyber Defence Alliance Inc.; Principal Consultant, Avantgard
3 Managing Director, SiegeBrake Cyber Incident Readiness
4 Cyber Security Architect
5 Practice Manager, Business Aspect
6 Professor in Law, Canberra Law School, University of Canberra

- The use of ACD may constitute entrapment, deception or fraud depending on the legal definition and interpretation of these terms in different countries.
- The use of ACD may violate the privacy and data protection rights of the employees and customers of the financial institutions, as well as the third parties who may be affected by the cyber-attacks.
- The use of ACD may conflict with the contractual obligations and fiduciary duties of organisations, as well as industry standards and best practices.

This paper offers some recommendations and future directions for research, such as developing a clear and transparent policy for the use of teasers and tracers, obtaining the consent and co-operation of the relevant stakeholders, and conducting a risk assessment and evaluation of the effectiveness and impact of the techniques.

1. Introduction

> *'Ignorance of the law excuses no man; not that all men know the law, but because 'tis an excuse every man will plead, and no man can tell how to refute him.'*
>
> John Selden (1584–1654), English jurist, scholar and polymath

It is an unsurprising truism that in a field as thorny as cybersecurity, the use of inconsistent terminology and ill-defined concepts has created a storm of unnecessary complexity and confusion. Nowhere is that confusion more apparent than in the field of 'active cyber defence' (ACD). In one sense, the term ACD has arisen out of a desire for public policy to recognise that private actors 'are not allowed to retaliate or gather evidence beyond the perimeter of their own networks' (Broeders 2021: 1). Thus, a private actor can protect their own network but cannot – and never can be – authorised to 'hack back' a cyber-attacker, even in the direst of circumstances (Walker-Munro et al. 2022: 5). However, this has created a legal position across numerous jurisdictions that the cybercriminals (both organised and opportunistic) and foreign intelligence actors who engage in cyber-attacks are at less legal risk than the organisations who set out to protect against those attacks (Walker-Munro and Dov Bachmann 2024).

In another sense, the term ACD has arisen to provide a dichotomy between acts which identify and/or expose a cyber-attacker from all other forms of cyber defence, which are necessarily 'passive'. Indeed, it is on this basis that numerous analyses have suggested that firewalls, antivirus software, network resilience and good 'cyber hygiene' would occupy this latter category (Curry 2012; McGee et al. 2013; Dewar 2014; Creado and Ramteke 2020).

The US Department of Defense is widely regarded as having coined the term ACD, defining it as using military systems or capabilities 'to discover, detect, analyze, and mitigate threats and vulnerabilities' (United States Department of Defense 2011). Rosenzweig (2013: 2) then added that ACD must also 'operate at network speed using sensors, software and intelligence to detect and stop malicious activity ideally before it can affect networks and systems'. Dewar went further, proposing that ACD was in fact 'an approach to achieving cyber security predicated upon the deployment of measures to detect, analyse, identify and mitigate threats to and from communications systems and networks in real-time, combined with the capability and resources to take proactive or offensive action against threats and threat entities including action in those entities' home networks' (Dewar 2013: 10).

Then, in 2017, the National Institute for Science and Technology (NIST) defined ACD holistically to describe *any* capability, tool or technique which offers '[s]ynchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities' (NIST 2024), with a particular emphasis on the production of cyber-threat intelligence. ACD was then provided with some additional nuance through the work of Lin, Harknett and Smeets, who suggested a delineation between ACD which involved an 'attack' on a system (with the intention of damage or destruction) and 'exploitation' (with the intention of gathering information or intelligence about the attacker/s or their network/s and system/s) (Lin 2010; Lin 2016; Harknett and Smeets 2022).

This paper proposes a synthesised definition which subsumes that nuanced approach to suggest ACD involves the use of 'sensors, software and intelligence to actively – rather than passively – detect, expose and potentially disrupt a cyber-attacker during a cybersecurity incident'. Therefore, one aim of this paper is to socialise that definition of ACD in the literature on cybersecurity.

A second aim is to provide a brief overview of the evolution and development of technologies and related concepts in ACD, often referred to as the 'honey world' because of references to technologies like honey tokens and honeypots (because they appear to be legitimate system resources, and are thus attractive to potential cyber-attackers like honey is attractive to bears (Juels and Ristenpart 2014)). These are techniques that intentionally expose vulnerabilities or false information (also referred to as faux data) to lure, deceive or confuse potential attackers, while monitoring their activities and collecting evidence.

The third aim is to examine and discuss the legal implications and challenges (using Australia as a contextual case study, but with international examples where appropriate) when private companies seek to use honey tokens, honeypots and related techniques. These issues can involve the possible violation of privacy rights, data protection laws, computer misuse statutes or entrapment doctrines. The paper concludes by identifying the areas where the use of ACD-related techniques remains controversial and which require further legal and regulatory clarity.

2. Context

At the Commonwealth Heads of Government Meeting in London in 2018, the Commonwealth Cyber Declaration was signed, which emphasised a strong commitment to common standards, harmonised legal approaches and improved interoperability, including 'through the use of Commonwealth model laws' (The Commonwealth 2018). However specific legal approaches to ACD across the Commonwealth are fragmented and nascent, to the extent that they exist at all.

In Canada, criminal laws still prohibit the use of 'hacking' as a defensive capacity, even despite recognition of ACD in Canadian cybersecurity policy since at least 2017 (Government of Canada 2017). Indeed, even the laws supporting both Canadian intelligence and military forces to engage in ACD have been criticised for undermining interoperability with NATO and US allies, as well as the 'lethargic' pace in establishing the necessary military and civilian capabilities (Rudolph 2021). Malaysia, Singapore and New Zealand permit their national intelligence and police forces to engage in limited forms of ACD, usually under the imprimatur of broad enabling legal authorities (Walters 2023). A study by Thinvane and Christine (2020: 8) that included numerous Commonwealth nations found:

> *'Almost half of Asia-Pacific states have no national cybersecurity strategies yet. Some instead have master plans that cover aspects of cybersecurity in the form of national digital policy (e.g., Pakistan, Brunei, Lao People's Democratic Republic), ICT masterplans (e.g., Cambodia, Solomon Island, Micronesia), and e-governance masterplans (e.g., Myanmar). Countries such as Indonesia, Mongolia, and Pakistan have laws and programmes related to cybersecurity, including cybersecurity centres and national computer emergency/incident response team (CERT/CIRT), but do not have a cybersecurity strategy yet. Meanwhile, some countries, such as Nepal and Fiji, are still in the process of drafting their strategies.'*

African nations fare even more poorly. A study by Ajayi (2016) showed that of the 54 nations making up the continent, only four have laws that explicitly deal with countering cybercrime. Thus, much of the emerging debate on ACD in the private sector in the Commonwealth has come by way of research in the United Kingdom (which in turn has been informed by debate in the US) so the paper reviews those jurisdictions before examining the contextual case study of Australia.

In the US, ACD and 'hacking back' have been interwoven into public debate for many years. Private companies – indeed, many of the major technology companies like Google/Alphabet, Meta and Apple – are headquartered in the continental US, and are prohibited from hack-backs by title 18 of the US code (section 1030), also known as the 1986 Computer Fraud and Abuse Act or CFAA. In addition, numerous US federal statutes positively prohibit the use of certain ACD tools and techniques (Cook 2018). Attempts by Congress in 2017 and again in 2019 to resolve this dilemma using the appropriately titled Active Cyber Defence Certainty Act failed to receive support and has never been

resurrected (Broeders 2021: 2). However, it seems widely regarded that the use of 'tarpits and honeypots, denial and deception, and beaconing on your own network' are acceptable forms of ACD conduct by US entities (Center for Cyber and Homeland Security 2016).

The UK, on the other hand, has taken more of an enablement approach towards ACD, in that the private sector would provide such capabilities to government under the close inspection and supervision of the Crown. Former Prime Minister David Cameron made clear in the 2015 *National Security Strategy* that ACD tools – including a full spectrum of capabilities to detect, analyse and track cyber-attacks pre-emptively – would be considered as 'national capabilities, developed and operated by the private sector' (Cameron 2015). However, like many other jurisdictions, the UK seems mired in policy limbo, lacking a specific definition of the term and clear operational guidance as to how ACD will actually be done. Sexton, for example, wrote that relying on the private sector to provide any form of security for government was not only paradoxical but risked legitimising the use of cyberweapons for corporate interests (Sexton 2016).

In Australia, a concise policy position remains largely elusive. There is no federal (Commonwealth) policy on ACD, having failed to address it in successive defence White Papers (Ball and Waters 2013) as well as the recent 2023–2030 *Cyber Security Strategy* (Department of Home Affairs 2023) and *Cyber Security Bill* (Department of Home Affairs 2024). This is not without industry consistently raising ACD as a matter for policy and legal clarification. In the absence of that position, numerous actors in the private sphere have attempted to delineate a position that ACD involves 'offer[ing] a diversion tactic that makes the cyber-criminal think they're on to something of value' (Powell and Dolan 2021) or 'the use of countermeasures by businesses and corporations to identify, slow down or hinder hackers in executing cyber attacks and malicious cyber activities' (Walker-Munro and Dov Bachmann 2024). At the same time, others in industry have constructed positions which attempt to align ACD either with existing Australian law (Shackelford et al. 2019), or with industry guidance produced or provided by the government (Powell 2021). Yet it appears from the literature that the Australian government has no formalised public position on the activities of ACD (other than those undertaken under the imprimatur of its intelligence services (Hanson and Uren 2018)).

Taking a broad and generalist approach to the various jurisdictions, one could, therefore, surmise that the law struggles to recognise the concept of ACD. From that above examination of the literature, it is generally considered that the internal network of a trading corporation is that corporation's *domaine réservé*, such that engagement in limited forms of deception in the pursuance of ACD is legally acceptable. There are several edge cases which the next section deals with: specifically, where the potential exists for internal networks utilising deception methodologies to still be customer-facing in some aspect and thus potentially incurring a claim against misleading trade practices or prohibitions against 'passing off'. Depending on the jurisdiction, such claims can be offset

by a broad statement in corporate documentation – such as a privacy policy or terms-of-use statement – that discloses to customers that their use of a particular network or system may involve the use of ACD.

3. Case for using ACD

The various methodologies or practices of ACD can be difficult to precisely define or formulate. However, the following is a non-exhaustive list of common ACD techniques or tools.

- **Tracers:** Cookies or similar programs attached to genuine trading information, which periodically transmit back to the incident response team network transmission and movement information, including IP addresses and/or physical locations of potential attackers' systems or networks, if the data are exfiltrated from the host system (Zhang and Thing 2021).
- **Honey objects, honey tokens, honeywords and honey encryption:** Falsified files, databases and user credentials which appear genuine to an external actor but alert the incident response team when accessed. As the files and/or credentials themselves are falsified, there is no genuine need for those files to be accessed (Juels and Rivest 2013; Juels and Ristenpart 2014).
- **Honeypot:** A broader term referring to an entire system (e.g. a web server) or system resource (e.g. a network) that is designed to be attractive to potential intruders, which is configured to alert when an attempt is made to access it. Typically, these are deployed within the boundaries of an organisation (Han et al. 2018).
- **Deception networks/systems/operations:** While nominally aligned with honey resources, deception activities generally rely upon the creation and maintenance of false (but realistic) networks and system resources intended to permit real-time monitoring of cyber-attackers. Given there is no legitimate need for users to be in a deception network, generally any activity in such locations will be unauthorised (Bushby 2019; Steingartner et al. 2021).

As a broad generalisation, the use of deception and 'honey' objects in ACD is considered legally permissible. This is because there is no legitimate need for a customer or other authorised user to ever need to access a 'honey' object – as the object is known by the business to be false, and managed accordingly, there is no way a customer or authorised user would ever find their way to that object. The result is that, by exclusion, any access of that file must be with malicious intent. Equally, the use of 'tracing' technology, such as a piece of code or software which captures an IP address or physical address of the person accessing the system, is legally fraught. In almost every case, consent must be provided, even if that consent is constructive in the sense that it forms part of the standard contractual obligations of persons accessing a given network or resource.

Thought must also be given to internal staff, i.e. employees and contractors. These individuals must be notified (either through employment contracts and/or organisational policies) that the corporation employs ACD, and given sufficient details about those programs to ensure the employee or contractor gives their informed consent to operate in a monitored environment. Generally, specific details are unnecessary. But there must be sufficient and cogent reasoning governing the recording of employee activity to avoid lawsuits later on, i.e. that network monitoring occurs 'for security and acceptable use'.

Even though honeypots can be useful for detecting and analysing cyber-attacks, they also pose some legal challenges that cybersecurity practitioners need to be aware of, in part due to the lack of policy and legal clarity. Depending on the jurisdiction, the use of honeypots may violate laws related to privacy, data protection, computer misuse, entrapment or unauthorised access. Moreover, the interaction between the honeypot operator and the attacker may create liabilities or obligations that are not clearly defined or regulated.

4. Legal issues

There are several interconnected but discrete issues associated with the use of ACD. This paper separates these issues into two categories: those related to international law, and those arising under domestic legal restrictions.

4.1 International law

This paper deals briefly with limitations arising under international law as these are largely beyond its scope. Numerous scholars have done an excellent job of enumerating these international legal problems, including that attribution during a cyber event can be nearly impossible even months afterwards (Berghel 2017; Tran 2018) and that attribution is a sovereign political decision that private companies are usually not authorised to make (Rid and Buchanan 2015; Wanner and Ghernaouti 2019). Such responses might be ruled 'use of force' under international law (Waxman 2011; Halberstam 2013; Corn and Jensen 2018) or even encourage endless cycles of 'Tom and Jerry' retaliatory actions (Gallagher 2022). Although scholars are generally in agreement that the level of permissiveness for ACD will not specifically cross a use of force threshold at international law, this is not always the case with some of the higher-end uses of ACD, and may not actually implicate states that seek to respond even to the mildest provocation (Van Dine 2019). Broeders (2021: 3) described it this way:

> *'If a company follows an attacker down the rabbit hole of the global internet there is no* a priori *telling in which country and jurisdiction it is going to resurface. If private parties conduct disruptive [ACD] operations on foreign, perhaps even state operated or affiliated networks, this can easily have an escalatory effect as foreign actors are likely, and may*

> *even be keen, to take offense. Especially in the current times of heightened geopolitical tensions some states will not look kindly on private companies that are legally licensed by the American government to conduct intrusive and disruptive cyber operations.'*

Looking at domestic legal restrictions, there appear to be several concise domains where ACD can cause private companies a degree of legitimate caution.

4.2 Criminal law

The first and most prominent domain generally relates to the common criminal prohibitions against unauthorised access to computer resources, i.e. hacking. Given that numerous states are signatories to the *Budapest Convention on Cybercrime*, most jurisdictions will have criminalised computer infiltration, data theft and similar acts as part of their ratification processes, which can include some techniques of ACD (Basu and Hickok 2020).

Many western states do have prohibitions against actions by private corporations which would allow unauthorised access to *any* system, even that of a cyber-attacker during a live incident. Canada (Gerke 2021), Japan (Jun 2023), Singapore (Housen-Couriel 2021), the US (Dewar 2014; Broeders 2021) and the UK (Sexton 2016; Montasari 2023) stand out as exemplars of legislative regimes where gaining unauthorised access to any form of computer resource is a crime, irrespective of the nature of the actor and/or the nature of any provocation such an actor may be facing.

However, the specifics of each jurisdiction are patchy and largely unexplored. As the Global Commission on the Stability of Cyberspace (2019: 45) warned in 2019, '[s]ome states do not control or may actively ignore these practices... However, in many states such practices would be unlawful, if not criminalized, while in other states they appear to be neither prohibited nor explicitly authorized'.

Australia's position is likewise that access to any computer that is unauthorised will be unlawful (Walker-Munro et al. 2022). The *Criminal Code* (Commonwealth of Australia) creates, for example, an offence (section 477.3(1)) where a person causes any unauthorised 'impairment' of communication to or from a computer, and that impairment is unauthorised. The use of tracers, deception networks or honey objects could conceivably cause modification in an attacker's data which impairs their ability to access the network; after all, one of the purposes of ACD is to preclude the attacker from ongoing access to corporate information. Another section of the *Criminal Code* (Commonwealth of Australia) creates an offence (section 478.1(1)) for 'unauthorised access to, or modification of, restricted data', where such data are restricted by an access control system. If a private corporation employing ACD were to gain intelligence about a cyber-attacker, behind, for example, a firewall or password-protected file, this could also lead to the commission of an offence for engaging in ACD. Without an immunity (which government agencies enjoy), private corporations could face the very real prospect of criminal charges and conviction.

Further, these legal regimes usually do not extend traditional defences into the cyber domain, i.e. self-defence to 'allow for the use of force against an attacker and thus render an otherwise illegal act lawful, provided it was necessary to defend one's own interests' (Stevens 2020: 320). In some cases, the failure to recognise self-defence flows from a legal disconnect where 'data' or 'information' are not recognised as a tangible form of property, the likes of which can be protected by a party engaging in otherwise unlawful conduct (Rosenzweig 2014; Hoffman and Nyikos 2018). In others, the limitations for the application of self-defence doctrines arise because, while data and information can be considered special forms of property, the scope and purview of rights which vest in that digital property (and hence how those rights can be defended) differ markedly from tangible real-world items (Lawrence 2007; Boerding et al. 2018; Grimmelman and Mulligan 2023). Focusing on Australia, computer data and information are not defined as 'property' under the *Criminal Code* (Commonwealth of Australia) or the *Corporations Act 2001* (Commonwealth of Australia),[7] and so cannot be subject to the doctrine of self-defence.

There are other defences worth examining: namely state of emergency, necessity and provocation. 'State of emergency' is a legal doctrine which can excuse certain illegal conduct where it is in response to an 'emergency' in which the illegal conduct was the only reasonable way of escaping or de-escalating that emergency (Ackerman 2003; Jakab 2006; Crusto 2015). 'Necessity' involves a response to a particular threat, described generally as where 'he or she carries out the conduct constituting the offence in response to an emergency which forced him to ward off immediately an immediate peril against himself or his property or against another person or his property' (Al Qudat 2009). 'Provocation' as a doctrine generally operates in English law systems to reduce a charge of murder to manslaughter because 'the accused killed during a sudden loss of self-control caused by provocation which was enough to make a reasonable man do as he did' (Ashworth 2009; Gruber 2015). All three defences have potential applications to using ACD, dependent on the law of the jurisdiction in question.

For example, the use of ACD could be excused if the ACD is a response that is reasonable and proportionate to the circumstances of a cyber incident – where that ACD involves potentially unlawful conduct such as accessing another person's computer or network or modifying or impairing data transmission. If an incident is in real-time or ongoing or involves serious compromise of sensitive or personal information and/or real-world damage or destruction or requires the use of ACD as the only available option of intervention (i.e. all other 'passive' measures have failed), the use of ACD under doctrines of emergency are more likely to be legally excusable. Necessity could also excuse such conduct if a three-element test is met:

7 Where property includes any 'legal or equitable estate or interest (whether present or future and whether vested or contingent) in real or personal property of any description', but does not cover computer data, information or intangible property of that sense: *Corporations Act 2001* (Commonwealth of Australia), section 9.

> *'First, the criminal act or acts must have been done only in order to avoid certain consequences which would have inflicted irreparable evil upon the accused or upon others whom he was bound to protect…The [second] element…[is]…that the accused must honestly believe on reasonable grounds that he was placed in a situation of imminent peril…thus if there is an interval of time between the threat and its expected execution it will be very rarely if ever that a defence of necessity can succeed. The [third] element of proportion simply means that the acts done to avoid the imminent peril must not be out of proportion to the peril to be avoided. Put in another way, the test is: would a reasonable man in the position of the accused have considered that he had any alternative to doing what he did to avoid the peril?'*
>
> R V Loughnan [1981] VR 443: 448

Provocation, as a partial defence to murder only, will likely never apply. But from a legal philosophy perspective, it does have some attraction in ACD because it could be used as a defence to excuse otherwise criminal conduct in response to the 'provocation' of a cyber-attack being conducted on a private organisation.

In Australia, the *Criminal Code* (Commonwealth of Australia) provides for defences of 'duress' (section 10.2) and 'sudden or extraordinary emergency' (section 10.3), but not provocation. In cases of both duress and emergency under Australian law, a person is not criminally responsible for conduct in response to situations of emergency or threats if the illegal conduct is the only reasonable response. Clearly the facts of a given ACD incident will matter. An argument could be easily made for example if a cyber-attack is occurring in real-time, and an ACD technique is immediately required to prevent sensitive data exfiltration or real-world impacts, i.e. the Colonial Pipeline incident which paralysed fuel supplies across the US eastern seaboard (Easterly and Fanning 2023). If the cyber-attackers have had access to the network or servers of a private entity for a period, such as several months, ACD is less likely to be an excusable response. Provocation on the other hand, as a partial defence to murder, is dealt with as a matter of state law in Australia and is slowly being eroded by a greater recognition that it has excused violent conduct in the past (Ramsey 2010). Its application to ACD is, therefore, unlikely to ever arise without a substantial body of law reform.

4.3 Privacy law

For many western states, there are also implications for privacy. Under the General Data Protection Regulation of the European Union (EU) for example, cyber-threat intelligence generated by ACD activities may contain confidential or protected information, which in turn has implications for how that information can be captured, analysed or shared with other entities and bodies to protect against cyber-attacks (Albakri et al. 2019). The collection of data or information, such as name, physical address or IP address, which could lead to identifying a person, may also be treated as 'personal information' subject to privacy statutes, and may be prohibited from collection, use or disclosure unless the

person to whom that information relates gives free and informed consent (Irving 2013; Miraglia and Casanove 2016). These provisions are increasingly being tailored to counter the emergence of behaviour referred to as 'doxing' (a person's real-life identity, address or contact details are made publicly available (Karimi et al. 2022)), a practice that is now *prima facie* illegal under most privacy legislation (Kukul 2023). Of course, the generalisation that privacy will always be an issue in the conduct of ACD can be countered by specific jurisdictional idiosyncrasies, e.g. in the United States, the Supreme Court has ruled that a person does not have a right to privacy when engaging in illegal activities, like hacking into a network or system (Simonato 2014).

In Australia, the *Privacy Act 1988* (Commonwealth of Australia) prohibits 'serious and repeated infringements with privacy' (s 13G), including repeated or sustained conduct which breaches the Australian Privacy Principles (APP) (section 13). These principles include, for example, the need to communicate clearly and transparently the reasons and mechanisms of data collection, processing, use, disclosure and storage (APP1.3 and 1.4) as well as dealing with 'unsolicited' information (APP4) which may arise from the use of ACD. Identification of a cyber-attacker's personal identity, physical or virtual location in cyber-threat intelligence shared with other bodies or entities may also breach APPs if the sharing is not with law enforcement agencies (APP6.1 and 6.3).

4.4 Consumer protection law

The third and final domain within which ACD may cause thorny legal challenges relates to commercial and consumer protection laws. This is because many jurisdictions adopt legislative standards to protect consumers of various goods and services from the predations of those making false or misleading claims as to efficacy, standard, utility or numerous other benefits of their products (Pengilley 2007; Cooper and Shepherd 2016; Willis 2020). Therefore, a private corporation which, while otherwise providing its goods or services as an entity 'in trade or commerce', deploys a deception network or honey objects, may fall foul of those misleading conduct provisions.

The devil is clearly in the detail, and the whole domain itself is woefully under-explored. For example, under the United Kingdom's *Consumer Protection from Unfair Trading Regulations 2008* (sections 5(2) and 5(3)) a business will behave unlawfully if it engages in a 'commercial practice' that 'contains false information' about a product such that it would 'cause the average consumer to take a transactional decision he would not have taken otherwise'. Clearly, an 'average consumer' is never likely to be exposed to an ACD operation unless that consumer is themselves doing something illegal, i.e. breaking into the corporation's network. That position can be contrasted with the US, where section 5(a) of the *Federal Trade Commission Act* (15 USC section 45) prohibits 'unfair or deceptive acts or practices in or affecting commerce'. As the US legislation does not rely on an 'average consumer' standard, there is arguably more room for it to potentially apply to private operators employing ACD.

In Australia, the Australian Consumer Law (ACL) operates as a schedule to the *Competition and Consumer Act 2010* (Commonwealth of Australia). Under the ACL, a bald prohibition exists (section 18) to a person engaging in conduct during 'trade or commerce' that is deceptive or misleading. These provisions clearly apply to 'computer software' and 'any component part of, or accessory to' that software. Conduct is deceptive or misleading if it 'induces or is capable of inducing error' (van Wyk 2015). As in the continental US, a private corporation that engages in ACD – even one entirely ancillary to, and protecting the underlying rationale for, its core business – may breach these provisions if its ACD program incorporates elements of deception.

5. Recommendations

To overcome legal ambiguities and facilitate responsible ACD adoption, the following amendments to legislation are recommended (an Annex is attached that demonstrates how these changes could be achieved in the context of Australian law):

5.1 Recommendations for the Commonwealth

- Ensure that corporations law, privacy law and crimes/criminal code legislation is amended to clarify that digital information, digitally stored data and information on a computer or network are considered an intangible form of property. This will ensure that private entities can use ACD while availing themselves of the 'self-defence' doctrines present in numerous Commonwealth jurisdictions.
- Ensure that, if private parties are authorised to conduct ACD, they do so within strict boundaries only and that they adhere to all guidelines issued by the national government. This will ensure Commonwealth nations have strong control over where and how private entities can engage in ACD.
- Closely monitor international developments in cybercrime and ACD legality to ensure that national laws do not breach international legal obligations.

5.2 Clarify self-defence, emergency and provocation defences

- The criminal statutes relating to criminal responsibility, excuses and defences (especially computer crimes) could otherwise be amended such that private organisations can take action (i.e. ACD) to protect their proprietary or commercial data, or the data of third parties for which they owe a statutory or common law duty of care, i.e. the personal information of customers.
- Alternately, specific computer crime offences (such as those enacted by parties to the Budapest Convention) need to be redrafted to exclude conduct of ACD by private organisations in response to a cyber-attack or cyber incident. This could

be by the creation of an exclusionary provision or a broader defence of 'acting in good faith'. In any event, private organisations should have the confidence that their position in utilising ACD is legally defensible.

- Alternately, computer crime offences could be subject to a limited defence of either emergency or provocation. In such situations, offence provisions should not apply to the conduct of ACD by persons in a private organisation either because of emergency, i.e. a reasonable and appropriate response to protect information for which the entity has responsibility; or because they are responding to a 'provocation', i.e. a cyber-attack or cyber incident against some asset for which those persons have some responsibility.

5.3 Safeguards

- **Privacy:** The use of ACD (especially tracing) will have serious consequences for privacy law, as it may enable the collection, use and dissemination of information on persons who are not cyber-attackers. There should be strong safeguards that limit the use of information gathered during ACD practices to protect individual privacy rights under both international and domestic law.
- **Anti-consumer practices:** Companies that deploy ACD (especially tracing) should be prohibited from using that information to engage in behaviour which offends consumer protection laws, i.e. by using tracing technology for advertising or marketing. Consumer laws should clearly define prohibited uses of information collected during ACD to prevent collection of excessive data or conduct invasive surveillance that infringes consumer privacy.
- **Oversight and transparency:** If these measures are adopted, judges could be permitted to immunise conduct of ACD by private entities. Relevant safeguards need to be included such as regular audits and public reporting by a competent and independent authority on the issuance and outcomes of such activities.
- **Unintended effects on legitimate users and scams:** While these provisions could empower businesses to combat cyber threats more effectively, there is a risk of collateral damage to innocent parties if compromised systems are mistakenly targeted. Clear safeguards and limitations on the scope of actions permissible under these amendments could help mitigate this risk.
- **Clarity on data usage limitations:** To prevent excessive or unjustified data collection, guidelines should clearly define the limits of what constitutes 'relevant' data that can be collected by ACD actions and how the data should be managed.

6. Conclusion

This paper has examined current ACD measures and the legal defences that may be invoked by individuals or organisations using ACD measures to protect their networks and data from cyber-attacks. It has explained the concepts of intervening conduct or event, sudden or extraordinary emergency, and duress, and how they relate to the use of ACD measures. It has also discussed the limitations and challenges of applying these defences in the context of ACD, such as the uncertainty of the law, the proportionality of the response, the attribution of the attacker and the potential harm to third parties. The paper concludes that the use of ACD measures requires careful assessment of the legal risks and consequences, and that more clarity and guidance from government authorities and the courts are needed to ensure the legitimacy and effectiveness of such measures.

Implementing and receiving the full value of ACD requires legal clarity. The amendments suggested in this paper would remove the current legal ambiguity to businesses, providing legal certainty so they can build and defend their organisations while operating within the bounds of the law. Without such clarity, businesses may inadvertently operate in legal grey areas, compromising their ability to protect themselves and their clients effectively.

In the Australian context, to meet its vision of being a world leader in cybersecurity by 2030, the Australian government needs to promote the use of ACD technologies and techniques to improve understanding of the actions and intent of cyber-attackers and, therefore, of the threats to Australian organisations and citizens. Globally, before we can encourage the use of ACD technologies and techniques, there needs to be legal clarity about the use of ACD. Therefore, this paper should serve as a call to action for legislators, especially in Australia, to make the changes that will remove the legal grey areas and allow private organisations to contribute to their respective jurisdictions' constructions of cybersecurity as part of the Australian government's call for a whole-of-nation effort of shared responsibility across the wider community.

Annex: Proposed Amendments to Commonwealth Criminal Laws

1 Insert:

Self-defence of data, data security or information systems

(1) A person is not criminally responsible for an offence if:

(a) the person believes that the conduct constituting the offence is necessary to defend data, data security or information systems that belong to the person or another person from unlawful injury; and

(b) the conduct is a reasonable response in the circumstances as the person perceives them.

(2) In determining whether the conduct is a reasonable response, regard must be had to:

(a) the nature and extent of the injury to data, data security or information systems that is threatened or inflicted;

(b) the potential or actual consequences of the injury to data, data security or information systems for the person, another person, or the public interest;

(c) the proportionality of the force used to the injury to data, data security or information systems that is threatened or inflicted;

(d) the availability and feasibility of any alternative means of preventing or mitigating the injury to data, data security or information systems;

(e) any relevant laws, policies, standards or codes of conduct that regulate or govern the use, protection or management of data, data security or information systems;

(f) any other relevant factors.

(3) For the purposes of this section:

(a) data means any information that is stored, processed, transmitted, or communicated by any means, whether electronically, digitally, optically, magnetically or otherwise;

(b) data security means the protection of data from unauthorised access, use, disclosure, modification, deletion or destruction;

(c) information system means any system, device, network or infrastructure that is used for the creation, storage, processing, transmission or communication of data;

(d) injury to data, data security or information systems means any act or omission that causes or is likely to cause damage, loss, impairment, disruption, interference or degradation to data, data security or information systems;

(e) unlawful injury means injury to data, data security or information systems that is contrary to law, or that exceeds or violates any lawful authority, consent or permission.

2 Insert:

Liability for certain acts – tracing and information gathering

A person is not subject to civil or criminal liability inside or outside [STATE] if the person causes any unauthorised access to data held in a computer or any compromise of the security system protecting the data held on a computer, if:

(a) the person is, or acts on behalf of, the owner of a computer system that has been subject to unauthorised access or exfiltration of data by another person;

(b) the person deploys software or hardware on the computer system of the other person for the purpose of gathering information about the unauthorised access or exfiltration of data;

(c) the person does not use or disclose any information collected by the software or hardware that is not reasonably considered relevant to identifying the person or system responsible for the unauthorised access or the defence of the person's system; and

(d) the person does not intentionally cause any damage, loss, or harm to the computer system or data of the other person, or any other person, as a result of the deployment of the software or hardware.

Liability for certain acts – damage or impairment to the computer of an attacker

A person is not subject to any civil or criminal liability for engaging in conduct inside or outside [STATE] that causes or is intended to cause computerrelated act, event, circumstance or result on the computer of another person (target computer) if:

(a) the person is, or acts on behalf of, the owner of a computer system that has been subject to unauthorised access or exfiltration of data by another person; and

(b) the person is reasonably satisfied that the target computer is the source of the attack; and

(c) the person is reasonably satisfied that the owner or operator of the target computer caused or permitted the attack to take place; and

(d) the conduct is likely to:

  (i) delete, damage or erase data present on the target computer without authorisation; and/or

  (ii) prevent or disrupt cybercrime; and

(e) the computer related act, event, circumstance or result is authorised by an active defence authority.

Active defence authorities

(1) A person may apply to a judge for an active defence authority.

(2) The application must include the evidence of each of the matters required by above.

(3) An application for an active defence authority must be dealt with in the absence of the public but is otherwise to be dealt with in such manner as is decided by the judge to whom the application is made.

(4) A judge must not issue an active defence authority unless the judge is satisfied that the application for the authority shows that reasonable grounds exist to justify its issue.

(5) When determining whether there are reasonable grounds to issue an active defence authority, a judge must have regard to the seriousness of the unlawful activity with which the application is concerned and the potential benefits of the conduct that would be authorised.

References

Ackerman, B (2003), 'The emergency constitution', *Yale Law Journal,* 113(5), 1029-1092.

Albakri A, Boiten EA and Lemos, RD (2019), 'Sharing cyber threat intelligence under the General Data Protection Regulation', in Naldi, M, Italiano, GF, Rannenberg, K, Medina, M and Bourka, A (Eds.), *Privacy technologies and policy*, Springer, Verlag, 28–41.

Al Qudat, MM (2009), 'Corporate criminal liability under the criminal laws of Jordan and Australia: A comparative analysis', *Journal Sharia and Law,* 37(8), 27-88.

Ashworth, AJ (2009), 'The doctrine of provocation', *Cambridge Law Journal,* 35(2), 292-320.

Ajayi, EFG (2016), 'Challenges to enforcement of cyber-crimes laws and policy', *Journal of Internet and Information Systems,* 6(1), 1-12.

Ball, D and Waters, G (2013), 'Cyber defence and warfare', *Security Challenges,* 9(2), 91-98.

Basu, A and Hickok, E (2020), 'Conceptualizing an international framework for active private cyber defence', *Indian Journal of Law & Technology,* 16(1), 16-47.

Berghel, H (2017), 'On the problem of (cyber) attribution', *Computer,* 50(3), 84-89.

Boerding, A, Culik, N, Doepke, C, Hoeren, T, Juelicher, T, Roettgen, C and Schoenfeld, MV (2018), 'Data ownership: A property rights approach from a European perspective', *Journal of Civil Law Studies,* 11(2), 323-370.

Broeders, D (2021), 'Private active cyber defense and (international) cyber security: Pushing the line?', *Journal of Cybersecurity,* 7(1), tyab010.

Bushby, A (2019), 'How deception can change cyber security defences', *Computer Fraud & Security,* 2019(1), 12-14.

Cameron, D (2015), *National security strategy and strategic defence and security review 2015: A secure and prosperous United Kingdom*, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478936/52309_Cm_9161_NSS_SD_Review_PRINT_only.pdf

Center for Cyber and Homeland Security (2016), *Into the gray zone: The private sector and active defense against cyber threats*, Washington, George Washington University.

Cook, C (2018), 'Cross-border data access and active cyber defense: Assessing legislative options for a new international cyber security rulebook', *Stanford Law & Policy Review,* 29, 205-236.

Cooper, JC and Shepherd, J (2016), 'State unfair and deceptive trade practices laws: An economic and empirical analysis', *Antitrust Law Journal,* 81(3), 947-980.

Corn, G and Jensen, E (2018), 'The use of force and cyber countermeasures', *Temple International & Comparative Law Journal,* 32(2), 127-134.

Creado, Y and Ramteke, V 2020, 'Active cyber defence strategies and techniques for banks and financial institutions', *Journal of Financial Crime,* 27(3), 771-780.

Crusto, MF (2015), 'State of emergency: An emergency constitution revisited', *Loyola Law Review,* 61(3), 471-524.

Curry, J (2012), 'Active defence', *ITNOW,* 54(4), 26–27, https://doi.org/10.1093/itnow/bws103

Department of Home Affairs (2023), *2023–2030 Australian cyber security strategy,* available at: https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

Department of Home Affairs (2024), *Cyber security legislative reforms engagement*, available at: https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/cyber-security-legislative-reforms

Dewar, RS (2014), 'The triptych of cyber security: A classification of active cyber defence', in Brangetto, P, Maybaum, M and Stinissen, J (Eds.), *Proceedings of the 2014 6th international conference on cyber conflict*, Tallinn, CCDCOE, 7-21.

Easterly, J and Fanning, T (2023), *The attack on colonial pipeline: What we've learned & what we've done over the past two Years*, available at: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

Gallagher, H (2022), 'Recognising a right to hack back: Tom and Jerry in cyberspace?', *Trinity College Law Review,* 25, 56-82.

Gerke, K (2021), 'Canadian hack-back?: A consideration of the Canadian legal framework for private-sector active cyber defence', *Alberta Law Review,* 59(1), 171-200.

Global Commission on the Stability of Cyberspace (2019), *Advancing cyberstability*, available at: https://cyberstability.org/assets/images/report/GCSC-Advancing-Cyberstability.pdf

Government of Canada (2017), *Defence policy: Strong, secure, engaged*, available at: https://www.canada.ca/en/department-national-defence/corporate/reports-publications/transition-materials/transition-assoc-dm/defence-policy-sse.html

Grimmelman, J and Mulligan, C (2023), 'Data property', *American University Law Review,* 72(3), 829-884.

Gruber, A (2015), 'A provocative defense', *California Law Review,* 103(2), 273-334.

Halberstam, M (2013), 'Hacking back: Re-evaluating the legality of retaliatory cyberattacks', *George Washington International Law Review*, 46(1), 199-238.

Han, X, Kheir, N and Balzarotti, D (2018), 'Deception techniques in computer security: A research perspective', *ACM Computing Surveys (CSUR),* 51(4), 1-36.

Hanson, F and Uren, T (2018), *Australia's offensive cyber capability*, available at: https://www.aspi.org.au/report/australias-offensive-cyber-capability

Harknett, RJ and Smeets, M (2022), 'Cyber campaigns and strategic outcomes', *Journal of Strategic Studies,* 45(4), 534-567.

Hoffman, W and Nyikos, S (2018), *Governing private sector self-help in cyberspace: Analogies from the physical world*, available at: https://carnegieendowment.org/research/2018/12/governing-private-sector-self-help-in-cyberspace-analogies-from-the-physical-world?lang=en

Housen-Couriel, D (2021), 'Hacking back under international law: Toward effective remedies against cyberattacks for non-state actors', in Siboni, G and Ezioni, L (Eds.), *Cybersecurity and Legal-Regulatory Aspects*, World Scientific, New York, 103-133.

Irving, L (2013), *Active cyber defense: A framework for policymakers*, available at: https://www.cnas.org/publications/reports/active-cyber-defense-a-framework-for-policymakers

Jakab, A 2006, 'German constitutional law and doctrine on state of emergency: Paradigms and dilemmas of a traditional (continental) discourse', *German Law Journal,* 7(5), 453-477.

Juels, A and Rivest, RL (2013), 'Honeywords: Making password-cracking detectable', *Proceedings of the 2013 ACM SIGSAC conference on computer & communications security.*

Juels, A and Ristenpart, T (2014), 'Honey encryption: Security beyond the brute-force bound', *Annual international conference on the theory and applications of cryptographic techniques*.

Jun, O (2023), 'Direction of Japan's new cybersecurity policy', *Asia-Pacific Review,* 30(3), 63-78, https://doi.org/10.1080/13439006.2023.2295707

Karimi, Y, Squicciarini, A and Wilson, S (2022), 'Automated detection of doxing on Twitter', *Association for Computing Machinery,* 6(3).

Kukul, B (2023), 'Personal data and personal safety: Re-examining the limits of public data in the context of doxing', *International Data Privacy Law,* 13(3), 182-192.

Lawrence, DE (2007), 'It really is just a game: The impracticability of common law property rights in virtual property', *Washburn Law Journal,* 47(1), 505-550.

Lin, HS (2010), 'Offensive cyber operations and the use of force', *Journal of National Security Law & Policy,* 4, 63-86.

Lin, P (2016), *Ethics of hacking back*, U.S. National Science Foundation, San Luis Obispo, CA.

McGee, S, Sabett, RV and Shah, A (2013), 'Adequate attribution: A framework for developing a national policy for private sector use of active defense', *Journal of Business & Technology Law,* 8(1), 206.

Miraglia, A and Casenove, M (2016), 'Fight fire with fire: The ultimate active defence', *Information & Computer Security,* 24(3), 288-296.

Montasari, R (2023), 'Cyber threats and the security risks they pose to national security: An assessment of cybersecurity policy in the United Kingdom', in Montasari, R (Ed.), *Countering cyberterrorism: The confluence of artificial intelligence, cyber forensics and digital policing in US and UK national cybersecurity,* Springer, Verlag, 7-25.

National Institute of Standards and Technology [NIST], (2024), *Computer Security Resource Center, Glossary*, available at: https://csrc.nist.gov/glossary/term/active_cyber_defense

Pengilley, W (2007), 'Fair trading, misleading or deceptive conduct', *University of Queensland Law Journal,* 26(1), 215-218.

Powell, J and Dolan, A (2021), *Active cyber defence tips the scales back in favour of the enterprise*, available at: https://purple.telstra.com.au/insights/thought-leadership/active-cyber-defence-tips

Powell, J (2021), *Deception in the essential eight*, available at: **https://acda.group/articles/**

Ramsey, CB (2010), 'Provoking change: Comparative insights on feminist homicide law reform', *Journal of Criminal Law & Criminology,* 100(1), 33-108.

Rid, T and Buchanan, B (2015), 'Attributing cyber attacks', *Journal of Strategic Studies,* 38(1–2), 4–37.

Rosenzweig, P (2013), 'International law and private actor active cyber defensive measures', *Stanford Journal of International Law,* 47(1), 1-15.

Rosenzweig, P (2014), 'International law and private actor active cyber defensive measures'. *Stanford Journal of International Law,* 50(1), 103-118.

Rudolph, A (2021), *Canada's active cyber defence is anything but active*, available at: https://www.cgai.ca/canadas_active_cyber_defence_is_anything_but_active

Sexton, M (2016), 'U.K. cybersecurity strategy and active cyber defence: Issues and risks', *Journal of Cyber Policy,* 1(2), 222-242.

Shackelford, SJ, Charoen, D, Waite, T and Zhang, N (2019), 'Rethinking active defense: Comparative analysis of proactive cybersecurity policymaking', *University of Pennsylvania Journal of International Law,* 41(2), 377-428.

Simonato, M, (2014), 'Defence rights and the use of information technology in criminal procedure', *Revue Internationale de Droit Penal,* 85(1), 261-310.

Steingartner, W, Galinec, D and Kozina, A (2021), 'Threat defense: Cyber deception approach and education for resilience in hybrid threats model', *Symmetry,* 13(4), 597-622.

Stevens, S (2020), 'A framework for ethical cyber-defence for companies', in Christen, M, Gordijn, B and Loi, M (Eds.), *The ethics of cybersecurity*, Springer, Cham, 317-330.

The Commonwealth (2018), *Commonwealth cyber declaration*, available at: https://thecommonwealth.org/commonwealth-cyber-declaration-2018

Thinyane, M and Christine, D (2020), *Cyber-resilience in the Asia Pacific: A review of national cybersecurity strategies*, available at: https://collections.unu.edu/eserv/UNU:7760/n2020_Cyber_Resilience_in_Asia-Pacific.pdf

Tran, D (2018), 'The law of attribution: Rules for attribution the source of a cyber-attack', *Yale Journal of Law & Technology,* 20, 376-441.

United States Department of Defense (2011), *Department of Defense strategy for operating in cyberspace*, available at: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

Van Dine, A (2019), 'When is cyber defense a crime? Evaluating active cyber defense measures under the Budapest Convention', *Chicago Journal of International Law,* 20(2), 530-564.

van Wyk, W (2015), 'Deception by omission: A warning about lawyers' duty to the court', *Bulletin (Law Society of South Australia),* 37(5), 37.

Walker-Munro, B, Mount, D and Ioannou, R (2022), 'The hacker strikes back: Examining the lawfulness of "offensive cyber" under the laws of Australia', *Computers & Law,* 94, 5.

Walker-Munro, B and Dov Bachmann, S-D (2024), *When cyber defence involves attack: Issues for Australia*, available at: https://www.lowyinstitute.org/the-interpreter/when-cyber-defence-involves-attack-issues-australia

Walters, R (2023), *Cybersecurity and data laws of the Commonwealth: International trade, investment and arbitration*, Springer, Cham.

Wanner, B and Ghernaouti, S (2019), 'Conceptualizing active cyber defence in cyber operations', *St Antony's International Law Review,* 15(1), 58-82.

Waxman, MC (2011), 'Cyber-attacks and the use of force: Back to the future of article 2(4)', *Yale Journal of International Law,* 36, 421-460.

Willis, LE (2020), 'Deception by design', *Harvard Journal of Law & Technology,* 34(1), 115-190.

Zhang, L and Thing, VL (2021), 'Three decades of deception techniques in active cyber defense: Retrospect and outlook', *Computers & Security* 106, 102288-102307.

About the authors

Dr Brendan Walker-Munro (lead author) is Senior Lecturer (Law) with the Faculty of Business, Law & the Arts at Australia's Southern Cross University. Brendan's focus is on "research security", the use of law and policy to protect university research from national security threats such as espionage, foreign interference, hacking, and technology transfer.

Andrew Cox is President of Australia's Active Cyber Defence Alliance Inc. and Principal Consultant at Avantgard, where he guides organisations in advancing from static to active cyber defence.

Grant Haroway is Managing Director, SiegeBrake Cyber Incident Readiness

Joe Otway is Cyber Security Architect, Australian Competition and Consumer Commission. Introduced to IT security in 1992, Joe has since operated in a range of information and cyber security roles in both Australia and overseas. He works with organisations that are critically dependent on secure information and IT.

Duncan Unwin is Practice Manager for Business Aspect, the consulting business of Data3. His cyber security work focuses on strategic threat intelligence in high risk and critical infrastructure environments.

Sascha Dov Bachmann is a Professor in Law at Canberra Law School, University of Canberra; Extraordinary Reader (Docent) in War Studies, Swedish Defence University (FHS), Stockholm; Fellow at NATO SHAPE, Hybrid War, and Lawfare Pacific and is working on various aspects of cyber operations and human security.

The Commonwealth

Commonwealth Cyber Journal \ 27
ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cyber-journal

Strengthening Nigeria's Cyber Frontier: Building Cybersecurity Resilience Through Legal Innovation

Iheanyi Samuel Nwankwo[1]

Abstract

Nigeria's digital environment faces significant cyberthreats, driven by the country's increasing reliance on information and communication technology across sectors, such as finance, telecommunications and public services. Despite foundational instruments like the Cybercrime Act and the National Cybersecurity Policy, the existing cybersecurity framework is inadequate to address the sophistication and dynamic nature of modern cyberthreats. The regulatory approach remains fragmented, outdated and poorly implemented in most cases.

This article addresses a critical gap in the current cybersecurity framework by proposing a novel legal framework to strengthen Nigeria's cybersecurity regulation. It moves beyond traditional, reactive approaches, arguing for a paradigm shift towards a proactive, resilience-focused regulation that intricately weaves cyber resilience principles – preparedness, adaptability and recovery – into the legislative fabric. Cyber-resilience promotes a holistic approach to security, emphasising proactive measures to anticipate, withstand and adapt to cyber disruptions, ensuring continuity in the face of cyberthreats.

The article uniquely presents a comprehensive blueprint for strengthening Nigeria's cybersecurity posture. It outlines key components of this cyber-resilient regulatory framework, including cyber safeguard legislation mandating risk assessments and 'security by design,' robust incident response mechanisms and strengthened reactive measures. This research offers concrete legal innovations to bolster Nigeria's cybersecurity ecosystem, aiming to reduce vulnerabilities, enhance readiness and foster resilience against dynamic cyberthreats, contributing a distinctly legal perspective to the discourse on cybersecurity in developing nations.

1 Institute for Legal Informatics, Leibniz Universität, Hannover, Germany.
Email: nwankwo@iri.uni-hannover.de

1. Introduction

In today's interconnected and digitally driven world, cybersecurity has become a global concern, particularly for rapidly developing nations like Nigeria. With the increasing reliance on digital technologies for everyday activities, data protection, whether personal or not, and safeguarding the digital infrastructure have never been more crucial. Consequently, cybersecurity has emerged as a vital component of modern data governance, requiring multifaceted measures to protect digital assets and mitigate risks to the infrastructure.

Against this backdrop, Nigeria's current cybersecurity landscape is evaluated to assess its readiness to tackle emerging cyberthreats. This assessment is crucial because, as a regional economic powerhouse with an emerging hub for technological innovation, Nigeria is attractive to cybercriminals seeking to exploit vulnerabilities in such a digital ecosystem. While Nigeria recognises the importance of cybersecurity and has established foundational instruments like the Cybercrime Act 2015, the current legal framework is demonstrably inadequate to address the sophistication and dynamic nature of modern cyberthreats.

Nigeria's cybersecurity framework is characterised by a mix of regulatory, organisational and technological measures, as well as educational initiatives to create awareness at various levels in the digital ecosystem (Global Cyber Security Capacity Centre, 2018). They are, however, marked by isolated, often obsolete, instruments that provide limited coverage amid the evolving threat landscape. This calls for a new formulation of laws and regulations that consider the complex social, technical and environmental factors that shape the modern cybersecurity threat and mitigation strategy alongside an enforcement mechanism that trickles to the lowest level of IT governance.

The gap created by the current state of affairs is significant and exposes the country to various cyber risks. Reports from reputable organisations consistently highlight the numerous threats and challenges that pose significant risks to national security, businesses and individuals (CSEAN, 2023; Cybervergent, 2024; Deloitte, 2024). These reports indicate a continuous rise in cyber incidents, including ransomware attacks, data breaches across various sectors, widespread financial fraud, the proliferation of phishing scams and insider threats.

In a recent assessment of global cybercrime indices, Nigeria's ranking was alarmingly low (Bruce and Lusthaus, 2024). Several factors contribute to this. For example, since 2015, when the Cybercrime Act was enacted, no other general application law has addressed other aspects of cybersecurity in Nigeria. Moreover, many of the provisions of this Act are yet to be implemented. It took almost a decade for the designation of national critical infrastructure to be published, signalling a very slow pace of implementation (Federal Republic of Nigeria Official Gazette, 2024).[2]

2 This is provided for in the Cybercrime Act, Section 3.

This lack of legislative updates and horizontal instruments to systematically address network and device security across various sectors, mandate cybersecurity risk management and promote the adoption of security by design principles throughout the lifecycle of digital products and services, as well as encourage or require the standardisation and certification of certain digital technologies, is significant and threatens the whole cyber ecosystem in Nigeria.

Unlike many cybersecurity policy studies that focus on technical or organisational solutions, this article addresses a critical gap by exploring legal innovation as the key to building cybersecurity resilience in Nigeria. We argue for a paradigm shift from traditional, reactive and prohibition-focused measures towards a proactive, resilience-focused regulatory approach (Talmi, 2023). The article uniquely proposes integrating core cyber resilience principles into Nigeria's legal framework. By outlining a comprehensive blueprint for a cyber-resilient legal framework, this research offers distinctly legal and actionable solutions for strengthening Nigeria's cyber frontier and safeguarding its digital economy.

The proposed approach aims to support Nigerian legislators and regulatory agencies in their cybersecurity decisions and to ensure Nigerian laws and policies are strategic, relevant and adaptive in the face of ongoing threats. This flexibility will allow the regulatory framework to withstand any shock occasioned by emerging threats and adjust to the desired state. Nigeria stands the chance of learning significant lessons from global best practices.

This article is structured as follows: following this introduction, Section 2 contains the methodology. Section 3 examines the critical importance of legal inputs in cybersecurity. Section 4 analyses Nigeria's current cybersecurity regulatory landscape. Section 5 discusses the paradigm shift towards embracing resilience in cybersecurity. Section 6 explores cyber resilience as a regulatory strategy. Section 7 provides a blueprint for strengthening Nigeria's cybersecurity legislation. Section 8 addresses the implementation challenges, and Section 9 concludes.

2. Methodology

This article employs a qualitative research methodology based on document analysis to examine Nigeria's cybersecurity legal framework and propose a resilience-based blueprint for its enhancement. The research follows a doctrinal approach combined with critical policy analysis, aiming to identify gaps and weaknesses in the existing regulatory landscape and develop evidence-based recommendations for improvement. The 'resilience-based blueprint' proposed is grounded in the concept of cyber resilience, focusing on the ability of Nigeria's legal framework to not only prevent cyber incidents but also prepare for, adapt to and rapidly recover from them. This will encompass preventative measures, incident response mechanisms, recovery protocols and adaptive governance structures.

The doctrinal approach provides a systematic exposition of the principles, rules and concepts governing a legal system (Smits, 2015). It examines the relationships between these elements to address gaps in the legal framework. This method involves identifying key legal principles related to cybersecurity within Nigerian law, tracing their evolution across legislative acts and regulations, and analysing judicial interpretations in relevant case law to understand their practical application and interrelation. This approach is used to identify, describe and analyse primary and secondary legal texts, including Acts of Parliament, regulations issued by government agencies and case law, to assess their implications for cybersecurity in Nigeria.

Critical policy analysis is suited for evaluating existing policies and frameworks, identifying shortcomings and proposing more effective alternatives (Robertson and Muirhead, 2022; O'Connor and Rudolph, 2023). This approach employs a framework that systematically deconstructs the existing cybersecurity policy framework, examining its goals, instruments, target groups and underlying assumptions. This deconstruction will facilitate the identification of legislative gaps (areas not covered by law) and implementation gaps (areas where policy enactment falls short of its intended goals). This involves deconstructing the current framework, highlighting legislative and implementation gaps, and developing a normative blueprint for a stronger legal structure.

This research relies exclusively on secondary data sources. Data collection involved an extensive review of legal and policy documents, international legal instruments, government and industry reports, and academic literature. The secondary data was analysed using qualitative content analysis and framework analysis. The findings from both the doctrinal approach and the critical policy analysis, particularly the identified gaps and weaknesses in the existing framework, directly inform the development of the resilience-based blueprint.

3. Cybersecurity: the strategic imperative of legal defence

According to the EU Cybersecurity Act, cybersecurity refers to 'the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats' (European Parliament and Council, 2019).[3] This definition highlights the broad scope of cybersecurity, encompassing not only the technological and data aspects but also the safeguarding of individuals and society. It underscores the importance of comprehensive measures to defend against various cyberthreats impacting multiple aspects of life, from personal privacy to national security.

3 Cybersecurity Act, Article 2.

Addressing cybersecurity challenges requires not only technological preparedness but also a comprehensive legal framework that can effectively respond to the evolving threat landscape. The crucial role of law in cybersecurity is widely acknowledged. Bozgeyik (2023) highlights the importance of legal protections for individuals, organisations and governments against various cyberthreats. These threats include privacy violations, intellectual property infringements, disruptions to international relations and cybercrimes. Similarly, Joshi (2024) highlights the urgent need for cybersecurity laws and regulations to adjust to emerging risks, stressing the importance of global co-operation and ongoing legislative evolution to keep up with rapid technological advancements. Solove and Hartzog (2022) advocate for a holistic approach to data security law, emphasising the importance of focusing on the entire data processing systems and holding all actors in the ecosystem accountable. Their aim is for the law to prioritise prevention and mitigation rather than reactive responses to data security.

In response to increasing cyberthreats, several nations and regional groups have enacted or updated cybersecurity laws.[4] These laws establish cybersecurity standards and requirements for organisations to protect data and systems. For example, the General Data Protection Regulation (GDPR) (European Parliament and Council, 2016) mandates appropriate technical and organisational security measures for personal data protection.[5] By requiring safeguards for information assets and penalising non-compliance, these laws ensure a baseline level of protection and incentivise robust cybersecurity practices. They also define and criminalise cyber offences like hacking, unauthorised access and cyber fraud,[6] deterring cybercriminals and providing a legal basis for prosecution.

While some nations have been proactive in enacting and updating laws to address cybersecurity issues, others have fallen behind. Nigeria falls into the latter category; despite a thriving digital economy, its cybersecurity laws have not kept up with advancements. Although Nigeria's current cybersecurity framework includes, the Cybercrime Act 2015, the National Cybersecurity Policy and Strategy 2021, the Nigeria Data Protection Act (NDPA) 2023 and snippets of cybersecurity-related provisions scattered across sector-specific laws and regulations,[7] significant gaps remain in both the scope of these laws and their implementation. This gap owes mainly to the lack of a cohesive legislative strategy. Therefore, revamping the regulatory framework and adopting a holistic, law-guided approach to fortifying the country's cyber defence is necessary.

4 For example, the EU has enacted the Network and Information Security Directive (NIS2) and the Cybersecurity Act, and the US has adopted the Cybersecurity Infrastructure Security Agency (CISA) Act. CISA has issued numerous guidelines and directives to enhance cybersecurity practices across critical infrastructure sectors.

5 See GDPR, Articles 25 and 32.

6 See, for example, the Convention on Cybercrime 2001.

7 For example, the Central Bank of Nigeria (CBN) Regulation on Risk-Based Cybersecurity Framework, and Guidelines for Deposit Money Banks (DMBs) and Payment Service Providers (PSPs) 2024, the Nigerian Communications Commission (NCC) Consumer Code of Practice Regulation 2024 and the Internet Code of Practice 2019.

4. A dive into Nigeria's cybersecurity regulatory landscape

A closer examination of Nigeria's cybersecurity legal framework reveals a mixed picture. While efforts have been made to bring cybersecurity issues to light, the outcomes of these are sometimes outdated and lack the sophistication needed to address the dynamic and ever-evolving nature of cyberthreats. The earliest attempt to regulate cybersecurity in Nigeria saw the setting up of a Presidential Committee on Illegal Online Activities in 2003, in response to the increasing rate of cyber-related crimes (Ikuero, 2022). This initiative led to establishment of the National Cybersecurity Initiative (NCI). In 2004, the Federal Government formed the Nigeria Cybercrime Working Group (NCWG) to sustain the objectives of the NCI. The NCWG assisted in drafting the Computer Security and Critical Information Infrastructure Bill in 2005, which was not passed into law (IISS, 2023). In 2006, a Directorate of Cybersecurity was created under the Office of the National Security Adviser to continue the work of the NCWG.

About a decade later, in 2014, the National Cybersecurity Policy and Strategy was published, with updates in 2021 (KPMG, 2017; Ekekwe, 2021). These publications exist alongside a National Security Strategy that considers cybersecurity to be part of the national threats. Although these documents set out the government's strategic intent in addressing the country's cyber risk exposure, their lofty ideals are yet to be realised.

In 2015, a more binding legislative instrument was passed in the form of the Cybercrime Act. This Act created a prohibitive framework, proscribing certain activities that threaten cybersecurity, such as unlawful access to a computer, system interference, unlawful interception and cyberterrorism, among others. It also aimed to protect critical infrastructure in Nigeria. It envisaged that the president may designate certain computer systems, networks and information infrastructure as 'critical national information infrastructure,' which is vital to national security or Nigeria's economic and social well-being. In June 2024, the designation order was finally gazetted, nine years after the Act's enactment, signalling a very slow pace of implementation. The Cybercrime Act was amended in February 2024 to correct typographical errors, address some issues in the original document and ensure compliance with the Economic Community of West African States Court's ruling that Section 24 violated the African Charter on Human and Peoples' Rights.[8]

It is important to note that Nigeria acceded to the Council of Europe's Cybercrime Convention in July 2022. However, this will have no local effect until it is domesticated per Section 12 of the Nigerian Constitution. Unfortunately, Nigeria has not signed the African Union (AU) Convention on Cyber Security and Personal Data Protection, which was adopted by the AU in 2014 and came into force in 2023 (Ayalew, 2023).

8 Paradigm Initiative v. FRN. ECW/CCJ/JUD/16/20.

It is equally notable that other criminal laws in Nigeria, such as the Criminal Code, the Advance Fee Fraud and Other Fraud Related Offences Act 2006, the Economic and Financial Crime Commission (EFCC) Act 2004, the Terrorism (Prevention) Act 2011 and the Money Laundering Prohibition Act 2022, have aspects relating to or that could be interpreted to cover cybercrime.

However, these laws need significant reforms to cater to the complexity and sophistication of modern cybercrimes and cybersecurity. For example, the offences addressed by the Cybercrime Act were common at the time of its enactment, but new cybercrimes have emerged, and others continue to evolve. While some provisions of the Act could be extended to cover new methods of cybercrime, it is doubtful whether the Act is flexible and adaptive enough to adequately address emerging threats such as revenge porn, disinformation, deepfakes and ransomware (Nwafor et al., 2021; Ajayi, 2023). Clarity in the definition of offences is crucial in criminal law, and ambiguities that arise from stretching existing definitions could impede justice.

Moreover, the penalties specified in the Cybercrimes Act are not sufficiently dissuasive to prevent these crimes. Many of its fines are significantly lower than the potential damage inflicted on information systems and individuals by cybercrime (Sibe, 2024). For example, it is an offence for a government or private employee to intentionally withhold or keep electronic mail, messages or payment card information (credit/debit) that was received in error and should have been delivered to someone else. Conviction carries a penalty of up to one year imprisonment, a fine of ₦250,000 or both.[9] At today's value, this amounts to less than US$150 and is too low in our view to deter such crime.

In 2019, the National Information Technology Development Agency (NITDA) issued the Nigeria Data Protection Regulation (NDPR) to address personal data protection issues. Subsequently, the Nigeria Data Protection Act (NDPA) 2023 was enacted as a federal law dedicated to privacy and personal data protection with an aspect focusing on data security. It requires data controllers and processors to implement appropriate technical and organisational measures to ensure personal data security,[10] and to notify relevant actors of data breaches.[11] It is, however, notable that the NDPA applies only where personal data is processed. Industrial operational data,[12] for example, is outside the scope of the NDPA unless such data relates to an identified or identifiable person.

Beyond the personal data protection law, some sector-specific instruments address cybersecurity in different contexts. These include the Nigeria Communications Commission (NCC) Consumer Code of Practice Regulation 2024 (NCC Regulation 2024) and the NCC Internet Code of Practice 2019 (NCC Code 2019), as well as the Central

9 Cybercrime Act, Section 12 (3).
10 See the NDPA, Section 39.
11 See the NDPA, Section 40.
12 Industrial operational data is data generated by industrial processes and equipment, such as sensors, control systems and Internet of Things (IoT) devices. This data provides valuable insights for optimising operations, predicting equipment failures, ensuring quality control and enhancing safety and security.

Bank of Nigeria (CBN) Risk-Based Cybersecurity Frameworks and Guidelines for Deposit Money Banks (DMBs) and Payment Service Providers (PSPs) 2024 (CBN Regulation 2024). It is equally notable that the Nigerian Code of Corporate Governance 2018, developed according to the Financial Reporting Council of Nigeria Act 2011, has some relevance to cybersecurity risk management. Principle 11 of the Code recommends that the 'Board delegates some of its functions, duties and responsibilities to well-structured committees, without abdicating its responsibilities.' One such committee is the Committee Responsible for Risk Management,[13] and it is expected to include cybersecurity risks in its framework.

Consequently, the extensive list of instruments highlighted above means several agencies play different roles in enforcing cybersecurity in Nigeria. These include:

- Office of the National Security Advisor (ONSA)
- Attorney General of the Federation
- Law enforcement agencies (police, EFCC, Independent Corrupt Practices Commission, etc.)
- Nigerian Computer Emergency Response Team (ngCERT)
- NITDA
- Cybercrime Advisory Council
- Nigerian Data Protection Commission
- NCC
- CBN, etc.

In the hierarchy, ONSA is responsible for cybersecurity co-ordination efforts in Nigeria. ngCERT, domiciled in ONSA, is the apex office responsible for managing cybersecurity activities in Nigeria and co-ordinates the operation of sector-based Computer Security Incidents Response Teams (CSIRTS) hosted in NITDA, NCC and the Defence Space Administration (ONSA, 2017). However, the country faces significant challenges in enforcing and co-ordinating cybersecurity affairs. For example, ONSA, which is responsible for both traditional and cyber-related national security, appears ill-prepared to confront the complexities of contemporary cyberthreats. There is limited evidence of ONSA's technical, legal and organisational capabilities to respond to cybersecurity challenges across all levels of cyber governance in Nigeria.[14]

13 Nigerian Code of Corporate Governance 2018, Principle 11.5.

14 At the time of writing, no website for ONSA and the Cybercrime Advisory Council relating to their cybersecurity roles could be found.

These enforcement gaps create an environment where cyberattacks are often concealed. Organisations are hesitant to report breaches, weakening data breach notification systems through denial and counter-accusations. A notable example is the ongoing National Identity Management Commission data breach controversy, where the Commission has repeatedly denied breaches, despite revelations of unauthorised third-party access to the National Identity Number database (Okamgba, 2024; Okonji and Ekebuike, 2024; Paradigm Initiative, 2024).

Resource constraints and a significant cybersecurity skills gap also impede Nigeria's ability to develop an effective cybersecurity regulatory framework. Many sectors face financial, technological and human resource shortages needed to build and maintain robust cybersecurity infrastructures. Small and medium-sized enterprises (SMEs) and government institutions, in particular, struggle to allocate sufficient budgets for advanced cybersecurity tools, continuous training and the recruitment of skilled personnel. These limitations leave Nigerian organisations and government institutions highly vulnerable to cyberattacks, exposing them to financial, reputational and operational risks. This calls for urgent action and co-ordination in revamping the country's regulatory framework through a resilient and multifaceted approach, combining legal reform, technical capacity-building and collaboration among domestic and global stakeholders.

5. A paradigm shift: embracing a resilience approach in cybersecurity

The concept of resilience has evolved over the years[15] and is embraced in many disciplines and fields, although the notion lacks a uniform definition (Florin and Linkov, 2016; Trump et al., 2018; Rogers, 2020; Smith, 2023; Araujo et al., 2024). In the domain of cybersecurity, it is widely acknowledged as a holistic approach to security that emphasises an organisation's ability to proactively prepare for, detect, respond to, mitigate and recover from a cyber incident to minimise the impact on its systems and services (Cisco, nd; IBM, nd). It encompasses a multifaceted approach to maintaining operational continuity in the face of cyberthreats, extending beyond the traditional focus on protection and defence, to include a broader strategy that integrates preparedness, adaptability and recovery (AL-Hawamleh, 2024).

Cyber resilience, as defined by leading cybersecurity bodies, emphasises the ability to anticipate, withstand, recover from and adapt to cyber incidents. Ross et al. (2021, p.1) define it as, 'The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.' Similarly, Goldman et al. (2021) view it as the capability to deliver and

15 The word 'resilience' comes to English from the French résilier and the Latin resilire and means jumping back, recoiling, springing back or resuming an original position.

sustain an adequate level of service despite faults and disruptions to regular operations, and Smith (2023, p.38) highlights the 'ability of a cyber system to recover from stress that causes a reduction of performance' as a core feature of cyber resilience.

These definitions converge on the core pillars of cyber resilience: the ability to anticipate, prevent, detect, respond to and recover from cyber incidents. Together, these components form a comprehensive approach aimed not only at defending against threats but also at ensuring an organisation can maintain operations during an attack and swiftly recover from such disruptions. Anticipation involves identifying potential risks before they materialise, allowing organisations to take pre-emptive action, while prevention focuses on implementing security measures that reduce the likelihood of a successful cyberattack. Detection emphasises the need for real-time monitoring systems capable of identifying malicious activity as soon as it occurs. Response involves immediate action to contain the impact of an attack, while recovery ensures operations are promptly restored to normal, minimising downtime and financial losses (Akinsanya et al., 2024).

In practice, cyber resilience involves developing detailed playbooks for managing cyber incidents and ensuring a co-ordinated response during and after attacks. Regular cybersecurity drills and simulations are crucial for assessing readiness, practising high-pressure scenarios and improving co-ordination. Consistently testing incident response procedures helps identify gaps, updates outdated processes and prepares both systems and personnel for various cyberthreats. These proactive measures enhance an organisation's ability to withstand cyberattacks with minimal disruption.

Some commentators have critiqued the growing trend of conflating cybersecurity with cyber resilience. Bygrave (2022), for instance, challenges the idea that cyber resilience should supplant the traditional concept of cybersecurity, arguing that the two serve distinct but complementary roles. It is essential to clarify that this article does not advocate for replacing cybersecurity with cyber resilience. Instead, the aim is to leverage the principles and components of cyber resilience to strengthen and enhance cybersecurity reforms. Cyber resilience is not meant to undermine the importance of traditional cybersecurity measures but to provide a more adaptive and comprehensive framework that addresses both the prevention and the recovery aspects of cybersecurity.

In this context, we propose a legal framework for cybersecurity developed through the lens of cyber resilience. The role of cyber resilience is to provide a foundational perspective – a skeleton – through which regulatory policies and strategic initiatives can be advanced more holistically. By incorporating resilience into the legal architecture, policy-makers can ensure regulations are flexible and adaptable, capable of evolving with the changing threat landscape. This approach aligns with Bygrave's conclusion that resilience-focused ideals can be adapted when reforming security rules, providing an enhanced model that better addresses the complexities of modern cyberthreats. The

incorporation of resilience thus becomes a tool for refining cybersecurity rules, ensuring they are not only proactive in preventing breaches but also robust in responding to and recovering from them.

Unpacking the components of cyber resilience and its role in cybersecurity regulatory governance is essential, given the inevitability of cyber incidents. A cyber resilience framework thus encourages proactive organisational preparedness, ranging from identifying critical assets and understanding their vulnerabilities to developing robust policies, procedures and controls to mitigate risks. This approach aligns with Björck et al.'s (2015, p.5) observation that 'the concept of resilience essentially treats adverse cyber events as part of normal operations.' Embracing this mindset enables regulators integrate countermeasures and contingency plans into the fabric of cyber safeguard laws.

6. Cyber resilience as a strategy in a regulatory framework

Several works have highlighted the importance of robust regulatory frameworks in effectively addressing cybersecurity (OECD, 2012; Björck et al., 2015; Bygrave, 2024). These works have suggested varying approaches to achieving an effective framework, including a risk-based approach. This article adds to this discussion by highlighting the components of cyber resilience as a skeleton for modelling cybersecurity regulatory frameworks for a developing nation like Nigeria.

When viewed through this lens, a cyber-resilient regulation integrates technical, organisational and operational safeguards to ensure systems can withstand and adapt to cyber disruptions through legislation. Essentially, it establishes obligations for key stakeholders, requiring them to ensure their systems are not only prepared to prevent cyberattacks but also proactively equipped to anticipate incidents, respond effectively and recover from them when disruptions occur. This approach is structured around several key components, including mandatory ex-ante risk assessments, security audits, vulnerability management, recovery planning, continuous monitoring and adherence to evolving cybersecurity standards and data protection protocols, while penalising non-compliance. Entities managing critical information infrastructure may face more stringent measures as a result of their criticality systems.

A cyber-resilient regulatory framework also accommodates reactive measures such as ex-post risk assessment, breach notification and vulnerability disclosure, to warn affected entities and giving them time to implement protective measures. Another key aspect of resilience is fostering collaboration and engagement of various stakeholders, including government agencies, private sector entities and civil society, to ensure comprehensive cybersecurity across sectors. Regulatory policies should encourage or require sharing of threat intelligence and best practices, enhancing the collective ability to respond to cyber incidents. Together, these elements foster an environment where cyber resilience is not

merely a technical goal but also a regulatory mandate, ensuring affected stakeholders operate with both proactive and reactive strategies to maintain operational integrity throughout the system lifecycle.

The EU provides an example of legislative initiatives on cybersecurity framed around resilience. This is reflected right from the titles of the legislative instruments, such as the Directive on the Resilience of Critical Entities (European Parliament and Council, 2022) and the just adopted Cyber Resilience Act (CRA) (European Parliament and Council, 2024). The CRA, for instance, introduces horizontal cybersecurity requirements by establishing EU-wide cybersecurity standards for manufacturers and developers of products with digital elements, encompassing both hardware and software.[16] The Act provides two sets of essential requirements in Annex 1 – namely, product cybersecurity requirements and vulnerability handling process requirements, designed to enhance product security by requiring manufacturers to incorporate essential cybersecurity measures from the design phase throughout the entire product lifecycle.

As can be deduced from this discussion, cyber-resilient legislation and policy frameworks are multifaceted and implemented through laws, standards, guidelines and best practices. In this regard, laws must adapt to evolving cyberthreats, allowing updates that reflect new risks and technologies. They should also be robustly enforced to motivate compliance and enhance necessary safeguards. As Kosseff (2018) notes, a focus on resilience requires cybersecurity law to be forward-looking, considering both incident prevention and recovery. This necessitates proactive laws and policies providing the procedural and substantive rules to enhance cybersecurity at all organisational levels, from boardrooms to operational management (Marchant, 2016). This ensures resilience is a core component of organisational strategy, not an afterthought.

7. A blueprint for strengthening Nigeria's cybersecurity regulation

The analysis in Section 4 revealed a cybersecurity legal landscape in Nigeria struggling to keep pace with evolving threats. Key weaknesses identified include the increasingly outdated nature of the Cybercrime Act, its reactive rather than proactive orientation and insufficiently dissuasive penalties. Furthermore, the current regulatory environment suffers from fragmentation and a lack of cohesive, overarching legislation, leading to enforcement and implementation difficulties. Existing laws also exhibit limited scope and coverage, failing to adequately address cybersecurity holistically across all sectors and neglecting the crucial aspect of cyber resilience. Finally, resource and skills gaps impede effective development and implementation.

16 "Products with digital elements" refers to any software or hardware product, including their remote data processing solutions and components, whether sold together or separately.

Recognising these critical shortcomings, this section outlines a blueprint for strengthening Nigeria's cybersecurity regulation. This proposed framework is deliberately structured to directly address each of these identified gaps, offering concrete and actionable measures to build a more robust and resilient cybersecurity ecosystem in Nigeria. The framework strengthens cybersecurity governance through a multifaceted strategy emphasising proactive measures, robust incident response and recovery, reactive requirements and accountability, and collaborative enforcement tools to address evolving threats and vulnerabilities. It includes key components designed to improve Nigeria's overall cybersecurity ecosystem.

7.1 Proactive cybersecurity measures

Nigeria needs cybersecurity legislation that prioritises proactive measures. Recognising the inevitability of cyber incidents, this legislation should prepare stakeholders to anticipate, prevent (where possible) and mitigate the impact of such incidents. Specifically, it should require the following actions from relevant stakeholders:

- **Mandatory risk assessments**

Introducing mandatory, regular and comprehensive ex-ante cyber risk assessments across sectors is a fundamental pillar of proactive cybersecurity legislation. This will be particularly crucial for industries classified as critical infrastructure, such as energy, telecommunications, finance, healthcare, the public sector and transportation, among others.[17] Legislation must require these sectors to conduct periodic systematic risk assessments to identify existing vulnerabilities, evaluate emerging threats and prioritise risk mitigation strategies. Such assessments are essential to ensure these organisations remain vigilant and adaptive in the face of evolving cyberthreats.

This requirement should be elevated to a board-level responsibility of the organisation to enhance accountability and ensure strict adherence. By integrating cyber risk management into the governance structure, senior leadership is made directly accountable for compliance, aligning cybersecurity with the broader organisational goals.

If implemented effectively across sectors, it can create a uniform standard of preparedness, foster resilience and minimise the potential impact of cyberattacks. By institutionalising regular assessments as a legal obligation, the legal system would ensure the critical sectors are continuously equipped to manage and mitigate the growing complexities of cyberthreats.

17 See Designation and Protection of Critical National Information Infrastructure Order 2024. The Schedule contains a list of identified computer systems, networks, assets and communications systems designated as critical national information infrastructure.

- Threat intelligence-sharing

A vital component of the proposed regulation is establishing robust, real-time threat intelligence-sharing platforms among relevant stakeholders. Effective cybersecurity governance hinges on the seamless exchange of actionable intelligence between key actors, including government agencies, private sector entities and international partners. In the Nigerian context, this will fill the gap in current cybersecurity efforts, which are severely hampered by the lack of a co-ordinated and systematic approach to threat intelligence-sharing.

Therefore, legislation should require the establishment of secure, centralised or decentralised platforms or networks that allow stakeholders to share timely and relevant threat information. These platforms would facilitate a more agile and co-ordinated response to cyberthreats, promoting a proactive rather than a reactive security approach. Additionally, enabling real-time intelligence exchanges would strengthen Nigeria's overall ability to effectively detect, respond to and mitigate cyber incidents, positioning the country as a significant player in international cybersecurity efforts.

- Security by design

Nigerian laws must actively promote the development of secure software and systems across all sectors. This approach, known as 'security by design,' entails embedding cybersecurity considerations at every stage of the digital technologies' lifecycle, from design and development to deployment. This strategy will make cybersecurity a foundational element rather than an afterthought in system design, potentially mitigating vulnerabilities and significantly reducing cyber risks by proactively addressing security concerns from the outset.

Likewise, legislation should promote the development of vulnerability disclosure programmes (VDPs) to improve the ability to identify and address potential threats before they can be exploited by malicious actors. These programmes offer a structured and collaborative method for security researchers, ethical hackers and other stakeholders to responsibly report security vulnerabilities. Additionally, legislative frameworks should mandate that system developers provide a Software Bill of Materials (SBOM) for their products. The SBOM serves as a comprehensive inventory of all software components, libraries and dependencies, ensuring transparency and traceability across the supply chain. This measure would not only help manage security risks related to third-party components but also encourage accountability in software development.

- Consistent system auditing and testing

In addition to ex-ante risk assessments, Nigerian cybersecurity regulations should require regular security audits and tests for critical infrastructure and high-risk organisations. These measures are vital for identifying vulnerabilities, testing the effectiveness of

security controls and confirming the efficacy of current cybersecurity measures. Regular audits ensure organisations comply with legal and regulatory requirements while continuously improving their cybersecurity protocols to address emerging threats.

For instance, penetration testing surpasses auditing by actively simulating real-world cyberattacks to assess an organisation's capacity to resist hacking attempts. By mimicking the tactics and strategies employed by malicious actors, penetration tests enable organisations to discover exploitable vulnerabilities in their systems, networks and applications before attackers can exploit them. This acts as a thorough assessment of an organisation's security defences, providing a proactive method to verify whether the implemented security measures are genuinely effective under pressure. Incorporating regular security audits and penetration testing into the legislative framework would strengthen a culture of continuous improvement in cybersecurity, encouraging organisations to stay vigilant and adaptable to the evolving threat landscape.

- **Cybersecurity awareness programmes**

Educating the public, employees and businesses about cyberthreats and best practices is essential for creating a cyber-resilient society. With the growing reliance on digital technologies, the threat landscape has become increasingly complex and widespread. To address these risks, legislation must actively contribute to cultivating a cybersecurity-aware population. This can be accomplished through policies that support and fund the development and implementation of comprehensive cybersecurity awareness and skill-building initiatives, including incorporating cybersecurity education in school curriculum.

Furthermore, fostering a culture of cybersecurity within organisations is equally critical. Legislation should mandate and promote awareness, encouraging organisations to integrate cybersecurity practices into their daily operations. This may include mandatory employee training programmes and regular cybersecurity drills.

7.2 Robust response and recovery mechanisms

While proactive strategies are crucial for mitigating cyberthreats, the inevitability of cyber incidents necessitates the inclusion of robust response and recovery mechanisms within a resilience-focused legislative framework. Legislation should mandate that all sectors, particularly the critical sectors, develop and maintain comprehensive incident response plans that outline clear, actionable steps for managing and mitigating the impact of cyberattacks. These plans must include regular drills and simulations, along with disaster recovery and business continuity solutions designed to minimise operational downtime and disruption.

- **Cyber incident response plan**

To address the rise in cyberattacks, Nigerian legislation should require structured cyber incident response frameworks for organisations. As Nigeria's digital economy expands, businesses encounter heightened risks such as data breaches and ransomware. An effective response plan facilitates prompt detection, analysis, and reaction to

security breaches, minimising damage to data and operations. Implementing these plans enhances national cybersecurity, fosters trust, and strengthens the country's digital landscape.

- Business continuity planning

Nigerian legislation should require organisations, especially those in critical sectors, to create and regularly test business continuity plans (BCPs). These plans should clearly describe the procedures for maintaining essential operations and ensuring service continuity during and after a cyber incident. By preparing for various scenarios, organisations can minimise downtime, lessen the impact of disruptions and continue providing essential services even during cyber crises. Regular testing of these plans through simulations and real-time exercises will ensure their effectiveness and preparedness during cybersecurity challenges.

- Data backup and recovery

To further strengthen resilience, legislation should mandate robust data backup and recovery mechanisms to protect against data breaches, ransomware attacks and other types of cyber intrusion. These requirements should encompass regular, encrypted data backups and secure storage practices. Moreover, organisations should create reliable recovery processes to swiftly restore systems and data after an attack. Well-maintained backup and recovery systems are crucial in minimising the impact of cyber incidents, enabling organisations to resume operations without significant data loss or prolonged downtime.

- Disaster recovery procedures

Comprehensive disaster recovery procedures should be mandated by law, requiring organisations to establish clear strategies for restoring IT infrastructure, systems and business operations after a cyberattack or natural disaster. These procedures should align with broader BCPs. Furthermore, disaster recovery strategies should be customised to address the unique risks facing each sector, ensuring critical systems are prioritised during the recovery process.

7.3 Reactive requirements and accountability

Nigeria's cybersecurity framework should establish reactive obligations across sectors to mitigate the impact of breaches and ensure organisations are accountable for cybersecurity failures. These measures should include mandatory breach notifications, post-incident analysis and a requirement to co-operate with relevant authorities during cybersecurity investigations. Such a framework would foster a culture of accountability and transparency, encouraging organisations to prioritise cybersecurity as a vital component of their operations.

- **Data breach notification and incident reporting**

Enacting a horizonal data breach notification law that requires organisations to notify relevant stakeholders in the event of a data breach is crucial to mitigating the harm victims may encounter afterwards. Drawing inspiration from the NDPA, prompt and transparent data breach notifications in various sectors of the economy, including where non-personal data is crucial, such as the industrial sector, can help lessen the impact of data breaches. The law should require measures such as credit monitoring for victims of a data breach. Organisations should be required to report security breaches, data leaks, ransomware attacks and other cybersecurity incidents to designated authorities to facilitate a co-ordinated response and learning lessons.

- **Post-incident analysis and integration of lessons learned**

Alongside response and recovery mechanisms, legislation should mandate that organisations perform comprehensive post-incident analyses after a cyber breach. This process should entail investigating the incident's root cause, evaluating the effectiveness of the response and pinpointing areas for improvement. The insights from these analyses must be incorporated into future risk management and incident response plans, ensuring organisations constantly enhance their cybersecurity practices.

- **Obligation to co-operate with cybersecurity investigations**

The obligation to co-operate with regulatory authorities during cybersecurity investigations is a critical component of a well-functioning cybersecurity regulatory framework. Organisations that experience cyberattacks or data breaches often possess valuable information that can help identify the source and extent of the attack while preventing future incidents. Therefore, both public and private sector entities should be required to collaborate with law enforcement agencies and cybersecurity authorities during investigations.

7.4 Strengthening the ecosystem through strong enforcement mechanisms and collaborations

Implementing robust enforcement mechanisms and encouraging collaboration among various stakeholders is crucial for building a resilient cybersecurity ecosystem in Nigeria. A comprehensive approach must focus not only on enforcing laws but also on promoting partnerships, research and the continuous development of best practices to ensure cybersecurity remains robust against evolving threats. The legal system should entail the following measures:

- **Strong enforcement mechanisms**

Reformed cybersecurity laws in Nigeria must have clear and enforceable provisions to ensure compliance. Penalties for violations, such as fines, sanctions and legal actions, should be stringent enough to dissuade individuals and organisations from engaging in cybercrime or failing to comply with established cybersecurity regulations. Enforcement

mechanisms must be backed by a competent and well-resourced regulatory body capable of investigating breaches, enforcing penalties, driving accountability and issuing clear guidance where necessary. However, this framework should remain adaptable and include a review mechanism that aligns with the rapidly changing cyberthreat landscape, allowing the regulatory environment to keep pace with innovations.

- Certification programmes and Standards

Adopting standardised certification programmes and industry benchmarks is crucial for enhancing Nigeria's cybersecurity posture. Certification frameworks such as International Organization for Standards (ISO) 27001 and the National Institute of Standards and Technology Cybersecurity Framework offer organisations structured guidelines for managing information security and reducing cyber risks. Establishing national standards that align with these international best practices can significantly strengthen the cybersecurity defences of both public and private institutions. The Standards Organisation of Nigeria (SON) has a crucial role to play in this respect. Certification programmes not only ensure compliance with best practices but also foster a culture of security awareness and continuous improvement within organisations. This should be promoted by law.

- Fostering collaborations

Public–private partnerships are essential for building a resilient cybersecurity ecosystem. Collaborations between government entities and private sector organisations facilitate the sharing of threat intelligence, enabling quicker identification of emerging cyberthreats and promoting collective responses. These partnerships allow for the pooling of expertise and resources, fostering co-ordinated efforts in mitigating cyber risks and managing incidents. Such collaboration also ensures both sectors are aligned in their cybersecurity governance approaches, thereby strengthening the nation's overall cybersecurity posture. Moreover, encouraging active international co-operation is crucial, as cyberthreats often transcend borders. By engaging with global partners at various levels, Nigeria can enhance its capacity to combat transnational cyberthreats, access valuable insights from international experiences and contribute to the global effort to establish stronger cybersecurity norms.

- Research and development

Investing in R&D is crucial for staying ahead of the rapidly evolving cyberthreat landscape. Innovation in cybersecurity technologies, methodologies and tools is essential for detecting, preventing and mitigating sophisticated cyberattacks. By supporting R&D initiatives through legislative measures, Nigeria can cultivate homegrown solutions that address unique national threats while contributing to global cybersecurity advancements. Government funding, academic involvement and private sector investment in

cybersecurity research will be vital in building advanced security infrastructure. Moreover, fostering a culture of innovation ensures Nigeria remains competitive and capable of responding to the challenges posed by new technologies.

8. Implementation considerations and addressing potential challenges

While a strong case has been made for integrating cyber resilience as a foundational element of Nigeria's national cybersecurity regulatory framework, potential challenges in implementation must also be acknowledged. Addressing these requires careful consideration in designing the framework, as outlined below.

8.1 Balancing technological neutrality with prescriptive legislation and the financial burden on SMEs

A key challenge is striking a balance between establishing a robust cybersecurity framework and ensuring technological neutrality while avoiding overly prescriptive legislation. Although this article advocates for embedding cyber resilience principles into law, it does not propose rigid mandates that could stifle innovation or impose excessive financial burdens, particularly on SMEs. Instead, the recommended framework follows a principles-based approach, setting clear cybersecurity objectives and outcomes while allowing organisations flexibility in selecting the technologies and methods to achieve them. The goal is to require essential cybersecurity capabilities – such as risk assessment, incident response and business continuity – without dictating specific technical solutions.

To mitigate the potential financial burden on SMEs, a tiered implementation approach is recommended. This could involve differentiated guidelines and expectations based on organisational size, sector criticality and risk profile. Additionally, the government could explore incentive programmes to support SMEs in adopting essential cybersecurity measures, such as subsidised training, access to affordable cybersecurity tools or tax incentives for cybersecurity investments. This balanced approach ensures the legal framework effectively raises the cybersecurity baseline across all sectors without disproportionately hindering the growth and innovation of smaller businesses.

8.2 Resource constraints, implementation and the need for a dedicated national cybersecurity agency

The effectiveness of any cybersecurity legal framework, regardless of its robustness, ultimately depends on adequate resources and effective implementation. As previously noted, resource constraints – both technical and financial – pose significant challenges to cybersecurity in Nigeria. Therefore, it is essential that the proposed framework is supported by a strong commitment to resource allocation and the establishment of a dedicated and empowered national cybersecurity agency.

The integration of cyber resilience principles into legislation should be explicitly linked to a clear mandate for a dedicated national cybersecurity agency. This agency would play a critical role in implementing the framework and providing support across all sectors. Its responsibilities should include publishing detailed, sector-specific guidelines for cyber resilience by design; developing and delivering comprehensive cybersecurity training programmes; facilitating international cooperation for knowledge-sharing and enforcement; collaborating with the national CSIRT on vulnerability management and penetration testing initiatives; and, critically, ensuring the continuous review and updating of the legal framework and associated guidelines in response to the evolving cyberthreat landscape. Without such a dedicated and well-resourced agency to champion and operationalise these obligations, even the most robust legislation risks remaining largely aspirational.

8.3 Reconciliation with existing laws

The implementation of certain mechanisms within the proposed blueprint – such as threat intelligence-sharing – requires careful alignment with existing legal provisions, particularly the NDPA and the Lawful Interception of Communications Regulations 2019. These regulations govern privacy and lawful interception, which are inherently intertwined with cybersecurity practices.

To ensure compliance, the design and implementation of threat intelligence platforms and protocols must be conducted with full cognisance of these existing legal frameworks. A comprehensive legal review should be incorporated into the implementation process to establish clear protocols that balance effective threat intelligence-sharing with fundamental rights, including privacy and data protection. This legal reconciliation is critical in building a secure, transparent and ethically responsible cybersecurity ecosystem in Nigeria.

8.4 Security by design in procurement

To further embed security by design principles at a national level, cybersecurity considerations should be integrated into national procurement regulations governing the acquisition of information and communication technology (ICT) equipment, systems and software solutions. Given that government agencies and public institutions are among the largest procurers of technology, prioritising cybersecurity at the procurement stage can significantly enhance national security.

Procurement guidelines should be updated to mandate the inclusion of cybersecurity requirements in tender specifications and evaluation criteria. This proactive approach would incentivise vendors to offer more secure products and services, ultimately strengthening the security posture of the public sector and, by extension, the national

digital ecosystem. Embedding security by design into procurement practices is a critical step towards fostering a cybersecurity-conscious culture from the foundation of technology acquisition and deployment.

9. Conclusion

This article has demonstrated the inadequacy of Nigeria's current cybersecurity framework against evolving cyberthreats. We have identified critical gaps: a static Cybercrime Act, fragmented regulation, a reactive posture and enforcement challenges. To address these, we propose a novel, comprehensive blueprint centred on cyber resilience and legal innovation – a necessary but complex undertaking.

Distinct from technical or organisational cybersecurity studies, this article offers a legal and actionable framework. Our blueprint represents a paradigm shift to proactive, resilient cybersecurity, uniquely integrating cyber resilience principles into legislation. Moving beyond reactive prohibition, it emphasises preparedness, anticipation and recovery, directly addressing identified gaps through proactive measures, threat intelligence-sharing, uniform laws and robust enforcement. Its ultimate success, however, depends on nuanced and effective implementation in Nigeria's complex environment.

The transformative potential of this framework thus hinges on implementation. While it offers a pathway to bolster Nigeria's cyber defences, safeguard its digital economy and build trust through proactivity and resilience, significant challenges remain. Bridging resource gaps – financial, infrastructural and expertise-related – requires strategic investment. Beyond resource allocation, inter-agency co-ordination, particularly having a dedicated lead agency, is crucial. A truly resilient ecosystem demands a holistic, long-term approach integrating legal reform with investment in ICT infrastructure, capacity-building, cybersecurity awareness and public–private partnerships. We believe these challenges are surmountable through strategic planning, phased implementation, stakeholder engagement and unwavering national commitment to cybersecurity leadership.

In conclusion, this article offers a timely roadmap for strengthening Nigeria's cybersecurity. Adopting cyber resilience and implementing legal innovations provides a clear, though complex, path to a resilient, adaptive framework. This strategic shift is imperative for Nigeria to fully realise digital benefits while mitigating risks, ensuring a secure digital future. We urge Nigerian law-makers and policy-makers to consider this blueprint, recognising that legal innovation, sustained effort and resource commitment are foundational to a resilient cyber frontier.

References

Ajayi, J. (2023) 'Fake News on Steroids: The Urgent Need for Nigeria to Regulate Artificial Intelligence'. 15 December www.linkedin.com/pulse/fake-news-steroids-urgent-need-nigeria-regulate-artificial-john-ajayi-nnnke/

AL-Hawamleh, A. (2024) 'Cyber Resilience Framework: Strengthening Defenses and Enhancing Continuity in Business Security'. *International Journal of Computing and Digital Systems* 15(1): 1315–1331.

Araujo, M., Machado, B. and Passos, F. (2024) 'Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance'. *Applied Sciences*, 14. https://doi.org/10.3390/app14052116

Akinsanya, M., Ekechi, C. and Okeke, C. (2024) 'The Evolution of Cyber Resilience Frameworks in Network Security: A Conceptual Analysis'. *Computer Science & IT Research Journal* 5(4): 926–949.

Ayalew, Y. (2023) 'The African Union's Malabo Convention on Cyber Security and Personal Data Protection Enters into Force Nearly After a Decade. What Does It Mean for Data Privacy in Africa or Beyond?' EJIL, 15 June www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/

Björck, F., Henkel, M., Stirna, J. and Zdravkovic, J. (2015) 'Cyber Resilience – Fundamentals for a Definition'. In A. Rocha, A. Correia, S. Costanzo and L. Reis (eds) *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol. 353*. https://doi.org/10.1007/978-3-319-16486-1_31

Bozgeyik, H. (2023) 'Importance of Cyber Law'. *Uzbek Journal of Law and Digital Policy* 2(2). https://doi.org/10.59022/ujldp.104

Bruce, M. and Lusthaus, J. (2024) 'World-First Cybercrime Index Ranks Countries by Cybercrime Threat Level'. University of Oxford, 11 April. www.infosec.ox.ac.uk/article/world-first-cybercrime-index-ranks-countries-by-cybercrime-threat-level

Bygrave, L. (2022) 'Cyber Resilience Versus Cybersecurity as Legal Aspiration. In T. Jančárková, G. Visky and I. Winther (eds) *14th International Conference on Cyber Conflict: Keep Moving*. CCDCOE Publications.

Bygrave, L. (2024) 'The Emergence of EU Cybersecurity Law: A Tale of Lemons, Angst, Turf, Surf and Grey Boxes'. Faculty of Law Legal Studies Research Paper 2024-04. Oslo: University of Oslo.

Cisco (nd) 'What Is Cyber Resilience?' www.cisco.com/c/en/us/solutions/hybrid-work/what-is-cyber-resilience.html (accessed 26 November 2024).

CSEAN (Cyber Security Experts Association of Nigeria) (2023) 'National Cyber Threat Forecast 2024'. https://csean.org.ng/national-cyber-threat-forecast-2024/

Cybervergent (2024) 'Ransomware Attacks in Nigeria'. 16 May. www.cybervergent.com/articles/ransomware-attacks-in-nigeria-5025e

Deloitte (2024) 'Nigeria Cybersecurity Outlook 2024'. www.deloitte.com/ng/en/services/risk-advisory/perspectives/Nigeria-Cybersecurity-Outlook-2024.html

Ekekwe, N. (2021) 'The Updated Nigeria's National Cybersecurity Policy and Strategy'. Tekedia, 24 February. www.tekedia.com/the-updated-nigerias-national-cybersecurity-policy-and-strategy/

European Parliament and Council (2016) 'Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)'. OJ L 119, 4.5.2016, pp. 1–88.

European Parliament and Council (2019) 'Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) 526/2013 (Cybersecurity Act)'. OJ L 151, 7.6.2019, pp. 15–69.

European Parliament and Council (2022) 'Directive (EU) 2022/2557 of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC'.

European Parliament and Council (2024) 'Regulation (EU) 2024/2847 of 23 October 2024 on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulations (EU) 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)'. OJ L 2847 20.11.2024, p. 1.

Federal Republic of Nigeria Official Gazette (2024) 'Designation and Protection of Critical National Information Infrastructure Order'. 25 June. https://cert.gov.ng/ngcert/resources/cnii-gazette.pdf

Florin, M. and Linkov, I. (eds) (2016) *IRGC Resource Guide on Resilience*. Lausanne: EPFL International Risk Governance Center.

Global Cyber Security Capacity Centre (2018) 'Cybersecurity Capacity Review Nigeria'. Oxford: University of Oxford.

Goldman, H., McQuaid, R. and Picciotto, J. (2011) 'Cyber Resilience for Mission Assurance'. *IEEE International Conference on Technologies for Homeland Security (HST)*.

IBM (nd) 'What Is Cyber Resilience?' www.ibm.com/topics/cyber-resilience (accessed 25 November 2024).

IISS (International Institute for Strategic Studies) (2023) 'Cyber Capabilities and National Power'. Vol. 2. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/09/cyber-capabilities-and-national-power-vol-2/cyber-capabilities-and-national-power_volume-2.pdf

Ikuero, F. (2022) 'Preliminary Review of Cybersecurity Coordination in Nigeria'. *Nigerian Journal of Technology* 41(3): 521-526.

Joshi, A. (2024) 'Study of Cybersecurity Laws and Regulations'. *Indian Journal of Law* 2(3): 7-14.

Kosseff, J. (2018) 'Defining Cybersecurity Law'. *IOWA Law Review* 103: 985-1031.

KPMG (2017) 'Building Cyber Security & Resilience in a Digital Africa'. May. https://assets.kpmg.com/content/dam/kpmg/ng/pdf/advisory/ng_building_cyber_security_resilience.pdf

Marchant, G. (2016) 'Advancing Resilience through Law'. In M. Florin and I. Linkov (eds) *IRGC Resource Guide on Resilience*. Lausanne: EPFL International Risk Governance Center.

Nwafor, I, Nwafor, N. and Alozie, J. (2021) 'Revenge Pornography in Nigeria: A Call for Legal Response and Cyber-Censorship of Content by Internet Service Providers'. *African Journal of Legal Studies* 13(2): 1-27.

O'Connor, K. and Rudolph, S. (2023) 'Critical Policy Analysis in Education'. Oxford Research Encyclopedia of Education, 22 March. https://oxfordre.com/education/education/display/10.1093/acrefore/9780190264093.001.0001/acrefore-9780190264093-e-1831

OECD (Organisation for Economic Co-operation and Development) (2012) 'Cybersecurity Policy Making at a Turning Point: Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy'. Digital Economy Paper 211. Paris: OECD.

Okamgba, J. (2024) 'NIMC Facing Multiple Unauthorized Accesses to NIN Data – Stakeholders'. Punch, 25 June. https://punchng.com/nimc-facing-multiple-unauthorised-accesses-to-nin-data-stakeholders/

Okonji, E. and Ekebuike, A. (2024) 'Again, NIMC Denies Data Breach, Assures Nigerians of Database Security'. This Day, 4 July. www.thisdaylive.com/index.php/2024/07/04/again-nimc-denies-data-breach-assures-nigerians-of-database-security/

ONSA (Office of the National Security Advisor) (2017) 'Action Plan for Implementation of the National Cybersecurity Strategy'. Draft. https://cert.gov.ng/ngcert/resources/draft-action-plan-ncss.pdf

Paradigm Initiative (2024) 'Major Data Breach: Sensitive Government Data of Nigerian Citizens Available Online for Just 100 Naira'. Press Statement, 20 June. https://paradigmhq.org/major-data-breach-sensitive-government-data-of-nigerian-citizens-available-online-for-just-100-naira/

Rogers, P. (2020) 'The Evolution of Resilience'. *Connections Quarterly Journal* 19(3): 13–32.

Robertson, L. and Muirhead, B. (2022) 'Critical Policy Analysis', in *Digital Privacy: Leadership and Policy*. Ontario Tech University. https://ecampusontario.pressbooks.pub/digitalprivacyleadershipandpolicy/chapter/critical-policy-analysis/

Ross, R., Pillitteri, V., Graubart, R. et al. (2021) *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. NIST Special Publication 800-160, Vol. 2, Rev. 1. https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final

Sibe, R. (2024) 'Cybercrime and the Challenge of Static Legislations in Nigeria'. Forbes, 29 April. www.forbes.com/councils/forbestechcouncil/2024/04/29/cybercrime-and-the-challenge-of-static-legislations-in-nigeria/

Smith, S. (2023) 'Towards a Scientific Definition of Cyber Resilience'. *Proceedings of the 18th International Conference on Cyber Warfare and Security.*

Smits, J. (2015) 'What Is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research'. Working Paper. 2015/06. Maastricht: Maastricht European Private Law Institute.

Solove, D. and Hertzog, W. (2022) *Breached! Why Data Security Law Fails and How to Improve It*. New York: Oxford University Press.

Talmi, N. (2023) '10 Bold Suggestions for Creating a Cyber Resilience Framework'. https://cybeready.com/guide-to-cyber-resilience/creating-a-cyber-resilience-framework

Trump, B., Florin, M. and Linkov, I. (eds) (2018) *IRGC Resource Guide on Resilience (vol. 2): Domains of Resilience for Complex Interconnected Systems*. Lausanne: EPFL International Risk Governance Center.

About the author

Iheanyi Samuel Nwankwo LLB, BL, LLM, PhD, is a senior research associate at the Institute for Legal Informatics at Leibniz Universität Hannover, Germany. His research focuses on data protection law, cybersecurity law, and emerging technologies, with a particular interest in systematising data protection impact assessments.

The Commonwealth

Commonwealth Cyber Journal \ 53
Print ISSN 2959-3018, online ISSN 2959-3026
thecommonwealth.org/cyber-journal

Cybersecurity Threats to Critical Energy Infrastructure in India: Challenges, Opportunities and Insights for Developing Nations

Rohini Haridas[1,2], Satish Sharma[2], Rohit Bhakar[2] and Chenghong Gu[1]

Abstract

The integration of information and communication technology into traditional power grids, transitioning them into smart grids, represents a significant step towards improved efficiency, reliability and sustainability. However, as these systems become more digitally dependent, they also become increasingly susceptible to cyberthreats, posing serious risks to national security, economic stability and public safety. Smart grids as a core component of critical energy infrastructure do not operate in isolation but are interconnected with other critical infrastructures such as water, telecommunications, transportation systems, etc. This interdependence increases the risk of cyberattacks, whereby disruptions in one sector can affect others, leading to widespread consequences. Thus, ensuring security is of the utmost importance. Cyberattacks on smart grids are no longer a theoretical concept. Rather, the question is, how prepared are countries to defend their smart grids from these sophisticated and rapidly evolving global threats? This paper explores the global issue of cybersecurity in smart grids, as it affects both developed and developing countries but with a particular focus on developing countries like India, where rapid digitisation combined with limited resources and expertise creates a unique set of challenges. By assessing India's current cyber security maturity level, this paper identifies key technical, operational and policy gaps that need to be addressed. Additionally, this paper highlights the potential of artificial intelligence and digital twin technology to significantly enhance the cybersecurity of smart grids, making them more resilient to emerging threats.

1 Department of Electronic and Electrical Engineering, University of Bath, UK
2 Department of Electrical Engineering, Malaviya National Institute of Technology, Jaipur, India

1. Introduction

The integration of digital technologies has transformed traditional power systems into interconnected, data-driven smart grids (SGs), promising improved efficiency, reliability and sustainability (Fardanesh et al., 2020). However, this digital transformation is a double-edged sword: while it optimises energy distribution and management, it also expands the attack surface, exposing SGs to sophisticated cyberthreats (Pengfei Zhao et al., 2024).

These risks are no longer hypothetical. Cyberattacks targeting SGs have already demonstrated their potential to disrupt national security, public safety and economic stability (Haridas et al., 2023). For example, the 2015 Ukraine power grid attack disrupted electricity supply to 225,000 customers during winter (CISA, 2021). The attackers used spear phishing emails to gain access to the system and deployed the BlackEnergy malware to manipulate Supervisory Control and Data Acquisition (SCADA) systems, resulting in the disconnection of multiple substations (Lee et al., 2016).

Similarly, the 2021 ransomware attack on the Colonial Pipeline in the US caused widespread fuel shortages, leading to economic losses and operational challenges (Goodell and Corbet, 2022). In India, the 2019 cyber-intrusion at the Kudankulam nuclear power plant exposed vulnerabilities in critical energy infrastructure (Campbell and Singh, 2019). Nuclear facilities are particularly attractive targets given their strategic importance and potential for large-scale environmental disasters (Poornima, 2022). It is estimated that the economic loss from a cyberattack on the US smart power grid is approximately US$1 trillion, eight times the cost of mitigating the Fukushima nuclear disaster (Tiscareno, 2019).

Cyberattacks on SGs have become more frequent and sophisticated. Such attacks are often driven by motives beyond financial gain, serving as a new weapon in state-sponsored actions, geopolitical tensions and deliberate efforts to destabilise national economies (Aljohani, 2024). Recent data indicates that the energy system as a whole accounts for 11.1 per cent of global cyberattacks (IBM, 2024).

This trend shows the need for domain-specific frameworks to enhance the resilience of such a critical infrastructure. This need becomes even more pressing given the rapid growth of SG adoption worldwide. The SG technology market, valued at US$50 billion in 2022, is projected to reach $130 billion by 2028 (Statista, 2023). India's power sector is undergoing rapid modernisation, with initiatives such as the installation of over 4.8 million smart meters in 2024 (Ministry of Power, 2024a). This reflects progress in digitisation but also expands the potential attack surface for cyberthreats. The 2020 Uttar Pradesh smart meter outage, which affected 158,000 households, showed operational vulnerabilities in Advanced Metering Infrastructure (Aggarwal et al., 2023).

SGs are also becoming increasingly interconnected with other critical infrastructure, such as gas and water systems, and face increased risks as a result of interdependencies, whereby disruptions in one domain can cascade across others, causing widespread disruptions. The cascading risks arising from such interdependencies highlight the need for robust and targeted cybersecurity measures designed to address the specific vulnerabilities of SGs.

Acknowledging this urgency, this paper explores the global issue of cybersecurity in SGs with a particular focus on developing countries like India, where rapid digitisation combined with limited resources and expertise creates unique challenges. It begins by defining critical infrastructure, acknowledging its varied definitions across countries based on unique priorities. It provides an overview of cyberattacks on critical infrastructure and their impacts. The paper evaluates India's cybersecurity maturity level and discusses global practices in securing SGs. It explores the potential of emerging technologies such as artificial intelligence (AI) and digital twins (DTs) to enhance the cybersecurity posture of SGs. Additionally, it addresses the technical and non-technical challenges facing developing countries, particularly India. The paper concludes by emphasising the importance of social responsibility, integrating cybersecurity into education and encouraging collaborative efforts among governments, industries and academia.

2. Definitions of critical infrastructure and its significance

Critical infrastructure refers to the assets, systems and networks that are essential for the functioning of a society and its economy (IBM, nd). These infrastructures are foundational for ensuring national security, public health and safety, economic stability and the well-being of a nation's citizens. Different countries define critical infrastructure based on their unique priorities and vulnerabilities.

In the US, critical infrastructure is defined as the assets, systems and networks, whether physical or virtual, so vital to the nation that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety or any combination thereof (CISA, nda). Similarly, the EU, under its European Programme for Critical Infrastructure Protection, defines critical infrastructure as an asset, system or part thereof located on EU territory that is 'essential for the maintenance of vital societal functions, health, safety, security, economic or wellbeing of people, and the disruption or destruction of which would have a significant impact on at least two member countries, as result of the failure to maintain those functions' (European Parliament, 2008). The UK defines critical infrastructure through the National Protective Security Authority as those essential services the loss or compromise of which could result in severe economic or social consequences or loss of life (NPSA, 2023). In India, critical infrastructure is defined by the National Critical Information

Infrastructure Protection Centre (NCIIPC) under the Information Technology Act 2000 as those computer resources the incapacitation or destruction of which shall have a debilitating impact on national security, economy, public health or safety (Drishti, 2022). The energy system, particularly power grids, is identified as a core component given its role in supporting economic growth and societal stability (Sadoian, 2025).

These definitions reflect each country's unique needs and challenges. The US focuses on systems vital to its resilience. The EU emphasises cross-border impacts, reflecting the interdependence of the bloc. The UK highlights essential services, while India prioritises the protection of digital systems, reflecting their critical role in its rapidly growing and technologically evolving infrastructure.

3. Cyberattack types and impacts

Cybersecurity is critical to maintaining the secure and reliable operation of SGs. It has three fundamental objectives: confidentiality, integrity and availability (the CIA triad: Fortinet, nd). Confidentiality ensures sensitive information is accessible only to authorised users; integrity guarantees the accuracy and trustworthiness of data; and availability ensures systems and services are accessible when required (Pillitteri and Brewer, 2014). While all three are essential, availability is the most critical aspect of the triad, as even brief periods of downtime can have severe consequences (Krause et al., 2021). Cyberattacks on SGs exploit vulnerabilities in systems, infrastructure and human behaviour (Ding, 2022). These attacks are diverse and can often be categorised based on their intent to compromise one or more aspects of the CIA triad. While no single classification captures every type of attack uniquely, they ultimately fall into categories based on their methods and targets. Also, regardless of their classification, the ultimate objective of these cyberattacks remains the same: to disturb national security, economy, public health or safety.

Common attacks include Denial of Service and Distributed Denial of Service attacks, which overload communication networks and disrupt grid operations (Huseinović et al., 2020). Attackers can launch eavesdropping and traffic analysis attacks to intercept and analyse network traffic to gain unauthorised access to sensitive information by exploiting vulnerabilities in encryption protocols or unsecured communication channels (Zibaeirad et al., 2024). As SGs expand, the increased interconnectivity creates a larger surface for such attacks. Phishing attacks exploit human vulnerabilities through deceptive emails or messages and rely on social engineering techniques (Mohamed, 2013). These attacks can compromise login credentials, enabling unauthorised access to critical systems and disrupting grid operations (Infosys BPM, nd).

Additionally, phishing is often used as an entry point to deploy malware or ransomware – significant threats to critical infrastructure, including SGs. Malware disrupts or damages systems through unauthorised access while ransomware encrypts files and demands payment to restore access (NCSC, nd). According to one report, the energy and utilities

sector experienced the highest number of ransomware vulnerabilities in 2024 (Sophos, 2024). This survey revealed that compromised credentials were the second most common root cause of ransomware attacks, preceded by malicious emails. Also, in 2023, 73 per cent of companies worldwide paid a ransom to recover data (CyberEdge, 2024). These findings apply to critical infrastructures as a whole.

Real-world examples include the 2015 Ukraine power grid attack where BlackEnergy malware was used to compromise SCADA systems, causing a power outage that affected 230,000 consumers (Lee et al., 2016). Similarly, in the 2021 Colonial Pipeline ransomware attack, attackers locked critical systems, disrupting fuel supply across the US East Coast (Young, 2024).

Man in the Middle attacks intercept communications to manipulate commands or steal sensitive information (Lindemulder and Kosinski, 2024). False Data Injection Attacks in SGs pose significant threats to both power system operations and electricity markets. These attacks can bypass bad data detection mechanisms in SCADA systems, potentially causing cascading failures through branch overloads and manipulating locational marginal prices (Yuan et al., 2012). Advanced Persistent Threats (APTs), often state-sponsored, are among the most sophisticated, and pose significant security risks.

Critical infrastructure is often targeted in cyberattacks, many of which are state-sponsored and motivated by geopolitical tensions. In 2024, a total of 178 politically driven cyberattacks were reported globally against the US, with 106 specifically targeting critical energy infrastructure (SWP, 2024). The primary motives behind such attacks align with their impacts targeting national security, economic stability and public safety (SMPnet, 2024). Beyond these primary impacts, other consequences include damage to reputation, regulatory penalties, data theft and loss of customer trust (Keeper Security, 2022).

4. Cybersecurity maturity level, with a focus on India

Cybersecurity maturity levels represent the extent of an organisation's capability to implement and sustain effective cybersecurity measures. As per one survey report (Sophos, 2022), these levels range from 'no plan' – where no cybersecurity framework exists – to 'optimised' – the highest stage, where continuous improvement cycles and adaptability to change are emphasised. Between these extremes are stages such as 'initial,' which reflects uncoordinated efforts; 'managed,' characterised by basic strategies ensuring planned activities with minimal performance tracking; 'defined,' where capabilities are proactive and co-ordinated across the organisation; and 'quantitatively managed,' which focuses on metrics-based objectives aligned with strategic goals.

Based on this analysis, which applies to all sectors, only 21 per cent of Indian organisations reported reaching 'optimised' level in 2022. This share falls behind that of Australia, where 28 per cent of companies have achieved this stage, reflecting a more advanced approach

to cybersecurity readiness. The gap widens at intermediate stages like 'quantitatively managed,' with only 18 per cent of Indian organisations aligning cybersecurity performance with measurable objectives compared with 26 per cent in Australia and even higher proportions in Singapore and Japan. Also, as per the Cisco Cybersecurity Readiness Index 2024, only 4 per cent of businesses and organisations in India are in the mature stage of cybersecurity readiness (Cisco Systems, 2024). Meanwhile, over 50 per cent are still in the formative phase of readiness, which is similar to the global trend.

4.1 Cybersecurity in India's power sector

Within India's power sector, cybersecurity maturity levels vary significantly across utilities. While some utilities demonstrate advanced readiness, incorporating modern infrastructure and proactive monitoring, others struggle, with limited resources, out-dated systems and fragmented policies. The Indian government has launched several initiatives to enhance cybersecurity maturity across the power sector (Ministry of Power, 2024b). Agencies like the Indian Computer Emergency Response Team (CERT-In), NCIIPC and the sector-specific Computer Security Incident Response Team (CSIRT Power) are central to these efforts, providing a co-ordinated response to threats. Security Operation Centres have been set up in POWERGRID for 24X7 monitoring of critical assets. Regular training and awareness programmes are being organised to upskill power sector employees. Initiatives like Cyber Jaagrukta Diwas, held monthly, raise awareness among employees about cybersecurity best practices. Employees are also encouraged to undergo certification programmes and training offered by institutions such as the National Power Training Institute and Rashtriya Raksha University, equipping them with the knowledge to tackle emerging cyberthreats. Despite these efforts, challenges remain, particularly in achieving uniform cybersecurity maturity levels across all utilities. While some State Load Dispatch Centres have achieved ISO27001 certification, others are still in the process of upgrading their systems. The integration of advanced technologies like SCADA and modern firewalls is ongoing in many states.

4.2 India's cybersecurity investments

India's cybersecurity market currently makes up approximately 3 per cent of the global market, projected to grow to 5 per cent by 2028 (DSCI, 2023). This growth is supported by a vibrant tech startup ecosystem, with around 27,000 startups as of March 2023. The allocated budget over three fiscal years, from FY2021/22 to FY2023/24, includes INR 1,010.51 crore dedicated to cybersecurity projects including the National Cyber Coordination Centre (NCCC) and other initiatives. Additionally, CERT-In has been allocated INR 633.6 crore during this period (Ministry of Electronics and IT, 2023) to strengthen capabilities in monitoring, responding to and managing cyber-incidents effectively. This financial backing is part of a broader initiative to expand the Digital India campaign, notably with a significant allocation of INR 14,903 crore aimed at developing cybersecurity tools and integrating the NCCC with 200 sites (Cabinet, 2023).

The India Union Budget 2024 highlights a transformative focus on enhancing the country's cybersecurity and technology sectors (Jain, 2024). With increased allocations directed towards upgrading cybersecurity infrastructure, the budget aims to fortify defences against sophisticated cyberthreats targeting critical infrastructure including SGs. Key areas of investment include advanced threat detection systems, intrusion prevention mechanisms and robust network architectures. The budget's emphasis on emerging technologies such as AI, machine learning and quantum computing marks a significant step forward. The budget also prioritises investment in cybersecurity education through funding for programmes, certifications and workshops designed to close the skills gap and build a workforce adept at managing cybersecurity concerns. Partnerships with educational institutions are emphasised to develop specialised cybersecurity courses that will generate a consistent output of qualified professionals.

Furthermore, the budget encourages public–private partnerships and the establishment of collaborative cybersecurity initiatives between government bodies, private sector entities and academic institutions. The budget also supports research and development through innovation grants and government-led research programmes focusing on emerging technologies and cybersecurity challenges. Public awareness and business training programmes receive increased attention to educate the public and businesses on cybersecurity best practices and risk management. Additionally, the budget supports innovation in the cybersecurity sector through the establishment of innovation hubs and incubators that provide funding, mentorship and resources to startups. Competitive grants are also available to fuel projects that tackle specific cybersecurity challenges or advance technological innovation. An important aspect of the budget is the enhancement of information-sharing platforms to facilitate the exchange of cyberthreat intelligence among various stakeholders, improving collective defence capabilities. The anticipated outcomes include strengthened national security, economic growth through job creation and increased public trust.

5. Global practices in securing smart grids

Securing the SG from cyberthreats has become a global priority as digital transformation and connectivity increase the vulnerability of critical infrastructure. Countries worldwide face sophisticated threats that target operational systems, disrupting essential services and endangering public safety. This section examines how selected developed countries and blocs like the US and the EU, along with Commonwealth developing country such as India has developed strategies and technologies to protect their power grids.

5.1 The United States

The US employs a comprehensive and multi-faceted approach to secure its electricity infrastructure. The North American Electric Reliability Corporation Critical Infrastructure Protection standards mandate cybersecurity requirements, focusing on risk assessment,

incident response and recovery (Erika, 2024). Complementing these standards, the Cyber Security Capability Maturity Model enables utilities to assess their readiness and identify security gaps (US Department of Energy, nd). These initiatives operate within the broader framework of the National Infrastructure Protection Plan (CISA, ndb) and are supported by the Cyber Security & Infrastructure Security Agency (CISA), which oversees cross-sector collaboration and preparedness. Public–private partnerships such as those facilitated by the Electricity Subsector Coordinating Council (ESCC, 2024) and the Electricity Information Sharing and Analysis Center (E-ISAC, 2024) enable real-time intelligence sharing between federal agencies and private sector operators. Legislative and executive actions further strengthen these efforts. For example, Executive Order 14028 on Improving the Nation's Cybersecurity prioritises zero trust architecture, secure software development and supply chain security (The White House, 2021).

5.2 The European Union

The EU regulates critical infrastructure through the Network and Information Security (NIS) directives and its updated NIS2 directive requiring member states to implement strict cybersecurity measures for operators of essential services including energy, water and transportation (European Parliament, 2023). The EU promotes collaboration through platforms such as the European Energy – Information Sharing & Analysis Centre. This facilitates a trusted network where private utilities, solution providers and public institutions collaborate to share real-time security data, incident reports and technical experiences. This initiative enables stakeholders to establish long-term relationships, learn from past incidents and proactively address future cybersecurity challenges. By promoting the exchange of information and best practices, it strengthens the resilience of Europe's energy system and contributes significantly to the broader EU cybersecurity framework.

5.3 India

The Cyber Security in Power Sector Guidelines (2021) issued by the Central Electricity Authority (CEA, 2021) outline key principles to enhance the cybersecurity framework of India's SGs. These guidelines mandate compliance from all stakeholders, including renewable energy generation utilities and aggregators. With the increasing complexity and frequency of cyberthreats, the framework is designed to evolve continuously to address emerging challenges in areas such as cyber-policy development, risk assessment, mitigation strategies, training for chief information security officers (CISOs), supply chain risk management, incident reporting, sabotage response mechanisms and cybersecurity audits.

To strengthen resilience across the sector, the Ministry of Power has established six sector-specific CERTs, covering thermal, hydro, transmission, grid operations, renewables and distribution. These teams are aligned with the National Cyber Security Policy and work in co-ordination with the Cyber Swachhta Kendra (Botnet Cleaning and Malware

Analysis Centre), encouraging power sector utilities to adopt robust malware prevention measures. The Information Sharing and Analysis Centre for Power (ISAC-Power) serves as a centralised platform for the six CERTs, facilitating efficient information-sharing and acting as a central repository for cybersecurity-related data. NCIIPC, operating under the National Technical Research Organisation, plays a pivotal role in safeguarding critical infrastructure as outlined by the Information Technology Act 2000 (amended in 2008).

The CEA (Cyber Security in Power Sector) Regulations 2024 represent a transformative step in fortifying India's power sector against cyberthreats (CEA, 2024). Enacted under Section 177 of the Electricity Act 2003, these regulations mandate stringent cyber security measures for all entities, including generating firms, transmission and distribution licensees and renewable energy operators. A cornerstone is the establishment of CSIRT Power, tasked with developing cybersecurity frameworks, co-ordinating responses to incidents and collaborating with national agencies like CERT-In and NCIIPC.

The regulations require every organisation to appoint a CISO and an alternate, ensuring senior-level oversight of cybersecurity strategies. Organisations also implement Cyber Crisis Management Plans to facilitate rapid detection, mitigation and recovery from cyber-incidents. Additionally, advanced security technologies such as firewalls, intrusion detection systems and intrusion prevention systems are mandated, alongside regular training for personnel managing IT and operational technologies. The regulations introduce a Trusted Vendor System ensuring all information and communication technology-based equipment and services are procured from verified suppliers to mitigate supply chain risks. Along with addressing technical requirements, the regulations also recognise the need to facilitate and promote research and development in the cybersecurity domain through collaboration with research institutes and academia. With provisions for regular audits, public consultations, a structured timeline for enforcement of the regulations and research collaboration, they reflect a proactive approach to addressing the increasing frequency and sophistication of cyberattacks targeting critical infrastructure.

6. Role of emerging technologies

In the context of SG cybersecurity, several emerging technologies are shaping the landscape, including blockchain for secure transactions (Mollah et al., 2019), quantum cryptography for advanced encryption (Kong, 2022), zero trust architecture for enhanced access control (Leadvent, 2024) and edge computing for real-time threat management (Zeng et al., 2023). However, this paper focuses on artificial intelligence (AI) and digital twins (DTs). given their transformative potential in predicting, detecting and mitigating cyberthreats within the complex and dynamic environment of SGs.

6.1 Artificial intelligence

Traditional cybersecurity solutions in SGs have primarily relied on perimeter defences, firewalls, intrusion detection systems and other reactive mechanisms. While these measures provide a foundational layer of security, they often fall short in detecting sophisticated attacks that exploit the grid's dynamic nature and interconnectedness (Radoglou-Grammatikis and Sarigiannidis, 2019). Furthermore, static cybersecurity frameworks struggle to adapt to evolving threat landscapes (Chehri et al., 2021), leaving critical systems vulnerable to new and increasingly complex cyberthreats.

AI has emerged as a transformative technology in addressing the complex and evolving challenges in cybersecurity. Its applications span critical areas, including monitoring network traffic, predicting breaches, automating incident response and analysing user behaviour (Cybersecurity Insiders, 2023a). AI techniques like natural language processing are enabling advanced phishing detection (Salloum et al., 2022), while deep learning is proving effective in detecting malware even in encrypted traffic (Yang and Lim, 2021). Transfer learning and reinforcement learning allow for rapid adaptation (Zhu et al., 2020) to evolving threats and dynamic policy management, ensuring cybersecurity systems remain resilient in an ever-changing landscape. Additionally, quantum-enhanced AI algorithms offer promising solutions for advancing cryptographic defences, while generative adversarial networks are enabling organisations to proactively simulate and address potential cyberthreats (Shi et al., 2024).

These emerging technologies ensure cybersecurity approaches are not only reactive but also proactive in identifying and mitigating potential threats. In one survey (Cybersecurity Insiders, 2023b), respondents reported significant improvements in several areas. The most notable was in threat detection, with 58 per cent of respondents highlighting its enhancement. Following closely were improvements in vulnerability management, noted by 57 per cent of respondents, and accelerated incident response times, mentioned by 56 per cent. Other improvements included better defence at scale (48 per cent), enhanced global visibility (44 per cent) and a reduction in false positive security alerts (43 per cent). Additionally, 37 per cent of respondents acknowledged that automation helped ease the talent shortage.

The global AI cybersecurity market reflects the rising importance of AI in this domain. In 2023, the market was valued at US$24.3 billion and it is expected to reach $134 billion by 2030, with significant growth driven by the increasing digitisation of critical infrastructures (Techopedia, 2024). However, the adoption of AI is not without concerns. While AI offers defenders significant advantages, generative AI tools have also enhanced the capabilities of attackers, automating malicious activities such as phishing and ransomware deployment (WEF, 2024). Furthermore, bias in AI-driven cybersecurity systems presents another challenge (Akitra, 2024). The effectiveness of AI in identifying and mitigating threats relies on the quality and diversity of the training data. If AI models are trained on datasets that lack representative attack patterns or exhibit inherent biases, they may

generate inaccurate threat assessments, leading to both false positive and false negative results (Townsend, 2018). Also, adversarial machine learning techniques can exploit these vulnerabilities, manipulating AI models into misclassifying malicious activities and weakening overall cybersecurity defences. To mitigate the risk of bias, diverse and representative datasets need to be used when training AI models. Continuous monitoring and auditing of AI systems can also help identify and address biases (Haber, 2025).

6.2 Digital twins

DTs are emerging as valuable tools for enhancing cybersecurity in critical infrastructure, particularly in SGs and industrial control systems. By creating virtual replicas of physical assets, DTs enable proactive identification and mitigation of vulnerabilities before they can be exploited (Srivastava et al., 2024). By providing a parallel environment for deep inspection and analysis, DTs allow for thorough investigation without disrupting operational technology services (Eckhart et al., 2024). DTs can detect cyberattacks during controlled transient behaviour and distinguish them from expected anomalies (Balta et al., 2024). When combined with deep learning, they improve intrusion detection, outperforming traditional methods in accuracy and efficiency (Ji and Niu, 2024; Lv et al., 2024). This capability is particularly evident in vehicle-to-grid cyber physical systems where a smart DT framework utilising long short-term memory and deep reinforcement learning effectively detects and mitigates co-ordinated cyberattacks within seconds (Ali et al., 2023). Similarly, Internet of Things (IoT)-based DTs integrated with control systems enhance resiliency against co-ordinated cyberattacks in networked microgrids (Sousa et al., 2021). They can be integrated into cybersecurity playbooks to support multidisciplinary teams in responding to incidents, thereby increasing system resilience (Allison et al., 2023).

However, several technical barriers constrain the implementation of DT. One of the most significant challenges is achieving interoperability and standardisation (Lei et al., 2023) across legacy and modern systems, where inconsistent communication protocols hinder seam less integration (Piroumian, 2021). Ensuring real-time data accuracy and synchronisation is critical but challenging, given the complexity of managing large-scale, heterogeneous data streams from different sources (Omrany et al., 2023). The high costs associated with sensors, IT infrastructure and their ongoing maintenance pose significant challenges, particularly in large systems (Sifat et al., 2024). Developing comprehensive software platforms to model complex grid dynamics and facilitate real-time interactions requires advanced computational capabilities, which remain difficult to achieve in practical deployments. Moreover, the bidirectional communication between physical and virtual systems significantly increases the risk of cyberattacks (Alcaraz and Lopez, 2022). Thus, these technical challenges are essential to utilise the full potential of DTs for enhancing the cybersecurity of SGs.

The adoption of DT technology also faces non-technical challenges, primarily organisational and economic in nature. Resistance to technological change within organisations is a major issue, often resulting from a lack of skilled personnel trained in DT technologies and their applications (Opoku et al., 2023). Addressing this skills gap requires significant investment in education, training and workforce development (Hazrat et al., 2023). The high costs of implementation also represent a significant barrier, especially in medium- or small-scale industries (Waqar et al., 2023). Moreover, the absence of clear value propositions for DTs (Tripathi et al., 2024) in some use cases complicates decision-making for stakeholders, who may find it difficult to justify the financial investment without well-defined outcomes. Regulatory requirements, including compliance with data governance (Pervez et al., 2023) and cybersecurity standards, add additional complexity, particularly in regions with stringent regulations that vary globally. Thus, there is a need for structured policy frameworks and strategic planning to facilitate the adoption of DT technologies in the energy system.

7. Cybersecurity challenges in developing countries

Developing countries face unique cybersecurity challenges, owing to systemic limitations, rapid digital transformation and socio-economic constraints. These challenges are particularly critical in the context of energy infrastructure, where vulnerabilities can have far-reaching consequences. This section outlines the key challenges faced by developing countries.

7.1 Technical challenges

In developing countries including India, energy infrastructure relies heavily on legacy systems that were not originally designed with cyberthreats in mind (EIS Council, nd). As these systems are integrated with modern IoT-enabled smart grids, they become potential entry points for cyberattacks (Zsuchy, 2023). Globally, around 57 per cent of such devices were identified as susceptible to medium to high severity threats (Rock, 2020). The complexity of securing the vast, distributed network of interconnected devices poses additional challenges. With components spread across large geographic areas, monitoring and ensuring the security of each entry point becomes increasingly difficult (Abu et al., 2021). Interoperability is another major challenge (Ma et al., 2013), as these systems often involve equipment from multiple vendors. The lack of uniform security standards across different systems increases the likelihood of security gaps providing opportunities for attackers to exploit weaknesses in the system.

The integration of electric vehicles (EVs) presents other significant technical challenges, as a result of the bidirectional nature of energy flows, which must be securely managed to prevent exploitation by attackers. Key areas of concern include charging station security, information privacy, software security, connected vehicle security and autonomous driving security (Shirvani et al., 2024). EV charging stations serve as critical infrastructure

yet remain vulnerable to tampering and unauthorised access. Vulnerabilities in EV charging stations raise concerns for both the grid and consumers, necessitating robust security measures (Pourmirza and Walker, 2021). The Open Charge Point Protocol and International Organization for Standardization standard 15118, which facilitate communication between charging stations and energy management systems, are susceptible to various attacks, including resource reservation interference and energy theft (Alcaraz et al., 2017). Also, attacks targeting EV communication protocols or exploiting weak authentication mechanisms can compromise charging schedules, disrupt grid stability, etc. (ElHussini et al., 2021).

Furthermore, the unpredictability of EV charging patterns complicates load balancing, which, if manipulated, could lead to localised overloads or cascading failures (Sayed et al., 2021). As the adoption of EVs increases, the growing number of charging points and their integration with home energy systems create additional decentralised entry points for cyberthreats (van den Brink and Broos, 2022). Similarly, increased integration of distributed energy resources (DERs) into SGs introduces new dimensions of cybersecurity challenges. DERs are often owned and operated by third parties, leading to inconsistent security implementations that increase the risk of exploitation (Zografopoulos et al., 2020). The secure synchronisation of DERs with the main grid is critical for maintaining grid stability, as desynchronisation caused by cyberattacks can result in grid instability (Culler, 2021). Also, wireless communication systems in SGs are vulnerable to various security threats, including jamming attacks, which can disrupt critical information exchange (Wang and Yi, 2011; Su et al., 2012).

The scalability of cybersecurity measures is also an issue, as securing a rapidly expanding infrastructure with numerous connected devices requires continuous upgrades and adjustments (Mishra and Pandya, 2021). Data privacy is also a growing concern, as SGs collect and process large amounts of personal energy consumption data. Without proper security controls, this data could be exposed to unauthorised access or misuse, violating individual privacy (Hu and Vasilakos, 2016). Also, the rise of APTs adds another layer of complexity. These highly sophisticated and prolonged attacks require advanced detection systems and strategies to mitigate (Akbar et al.,2023).

7.2 Non-technical challenges

7.2.1 Economic and demographic challenges

The interplay between economic constraints and demographic factors significantly influences the nation's capacity to implement robust cybersecurity measures. Financial instability remains a persistent issue, with state-run distribution companies burdened by massive losses, amounting €74.4 billion by 2023 (Raizada, 2024). These constraints force many utilities to prioritise basic infrastructure and service delivery over cybersecurity investments, perpetuating outdated systems vulnerable to sophisticated attacks. The rapid integration of renewable energy sources and IoT-enabled devices further expands the potential attack surface, while necessary cybersecurity upgrades often remain

deprioritised. Demographic disparities further highlight the uneven preparedness across regions. Rural and remote areas are often managed by state-run distribution companies operating under tight financial constraints, and lack the communication and monitoring infrastructure essential for real-time threat detection and response. These areas also experience a lack of training for operators and limited awareness among end users regarding cybersecurity risks, amplifying their exposure to threats.

7.2.2 Specialised workforce gap

The global cybersecurity workforce gap, which reached approximately .47 million professionals in 2024 (ISC2, 2024), reflects the growing challenges faced by both developed and developing nations. The Asia Pacific region alone required 3.37 million IT security experts, with China experiencing the largest shortfall, of 1.72 million professionals, and India a deficit of nearly 800,000 (ISC2, 2023). This shortage stems from a combination of rapidly increasing demand, migration of skilled professionals and systemic limitations in education and workforce development. Retaining skilled professionals is particularly challenging for developing nations, as many are drawn to developed countries offering higher salaries and better career prospects (Okafor and Chimereze, 2020).

Another significant challenge is the interdisciplinary skill set (Pirta-Dreimane et al., 2024) required for SG cybersecurity, which further widens workforce gap. Securing SGs requires expertise in both cybersecurity and power systems. This requirement significantly narrows the pool of qualified candidates as most existing education programmes focus on one domain without addressing the overlap. This issue is further aggravated by the disconnect between academic curricula and industry requirements (ibid.). India has made some progress in bridging this gap through industry-led initiatives, but these efforts remain insufficient to meet the scale of demand (ISC2, 2023). Additionally, the high cost of cyber security certifications acts as a significant barrier in developing countries (Catota et al., 2019). In addition to systemic challenges, societal policies aimed at promoting inclusivity can also affect workforce development. This also leads to further brain drain, reducing human capacity in the country (Gupta, 2022).

7.2.3 Lack of cybersecurity awareness

The lack of cybersecurity awareness among utility personnel and consumers is the significant challenge. According to a 2024 survey, 66 per cent of CISOs in the US identified human error as the most significant cyber security vulnerability (Proofpoint, 2024). Thus, its essential to provide targeted training to address human factors. In most of the cases, utility employees tend to perceive cybersecurity as a hypothetical issue rather than a tangible threat (TSC, 2023). Existing training programmes, conducted primarily by IT professionals, fail to effectively bridge this gap as they often lack contextual relevance to SG operations. These programmes rarely demonstrate the direct operational impacts of cyberattacks, limiting their effectiveness in convincing employees of the critical need

for robust security measures. Tailoring training modules to simulate real-world scenarios and highlight the cascading effects of cyberattacks on grid reliability can help align these programmes with practical needs and enhance their impact. On the consumer side, the rapid deployment of smart metering systems has not been matched by efforts to educate users about secure practices. In many regions, particularly in rural areas, low levels of digital literacy increase the risk of phishing attacks and unauthorised access to devices (Bajwa, 2023). Such consumer-side vulnerabilities weaken the overall security of SGs.

7.2.4 Corruption

Unfortunately, many developing countries struggle with a severe and unacceptable level of corruption, which creates significant barriers to implementing effective frameworks and policies (Otuoze et al., 2019). Misallocation of funds, favouritism in awarding contracts and lack of accountability weaken the overall governance and implementation frameworks (Hui et al., 2011). Investments in advanced technologies, skilled personnel and regulatory enforcement are often necessary for progress. However, in corruption-prone environments, resources allocated for essential upgrades are frequently diverted or misused, leading to delays and substandard outcomes (Adam and Fazekas, 2023). It Is evident that, in some developing nations, contracts are awarded based on political affiliations or personal interests rather than technical competence (Musanzikwa, 2013). India, despite making significant strides in digitiSation, has not been immune to these challenges (Transparency International, 2024). While the country continues to address corruption through various reforms, systemic issues persist. Without addressing this systemic issue, even the most advanced technological solutions are unlikely to achieve their full potential.

8. Bridging gaps in education and capacity-building

Addressing cybersecurity challenges in SGs requires a multifaceted approach that bridges current gaps in research, education and societal awareness. While strides have been made, particularly in policy and infrastructure upgrades, significant challenges remain, particularly in the context of developing nations like India.

The main issue is that most undergraduate curricula are outdated, with limited flexibility to make necessary changes, especially for university-affiliated private institutions. As a result, students often learn things that fail to address current industry challenges. The question remains whether the lack of such integration owes to regulatory barriers, institutional inertia or a lack of resources. Integrating SG cybersecurity into undergraduate curricula ensures students are aware of its importance early, enabling them to develop the skills and mindset needed to address future challenges effectively. The National Education Policy 2020 of India aligns well with addressing these issues (Ministry of Education (India), 2020). By advocating for interdisciplinary collaboration and emphasising

practical, application-based learning over traditional rote methods, the Policy fits with the goals of creating industry-relevant and forward-looking educational programmes. Also, financial constraints often hinder the development of advanced research infrastructure in educational institutions and research centres. Bridging financial and infrastructural gaps is therefore essential to equip institutions with the necessary resources to conduct meaningful research and training. Considering the interdisciplinary nature of SG cybersecurity, collaborative research between electrical engineering, computer science and policy-making departments must be encouraged. which can lead to holistic solutions that address the specific needs of SGs.

Another challenge lies in the limited accessibility of internationally recognised certifications in cyber security, which remain expensive and out of reach for many students and early career professionals. Governments could consider subsidising these certifications or developing regionally tailored alternatives that maintain global relevance. Making such qualifications more accessible would strengthen local talent pools and address skill shortages in cybersecurity.

Finally, the limitation of the current exam-driven educational system, which often prioritises grades and rote learning over practical application, underscores the need for reform. This gap presents an opportunity to redefine the role of students for cultivating a sense of responsibility towards addressing pressing societal challenges. Despite significant government efforts such as cybersecurity awareness campaigns and digital literacy initiatives, the vast population and geographic diversity create barriers to effective implementation. This gap can be bridged by integrating community-driven assignments into academic curricula where students engage in spreading awareness and educating underprivileged communities.

9. The Commonwealth's role in cybersecurity enhancement

The Commonwealth has played a crucial role in advancing cybersecurity through the Commonwealth Cyber Declaration (2018), which promotes a secure, inclusive and resilient digital environment to support economic and social development (The Commonwealth, 2018). By emphasising open markets, free data flow and innovation, the Commonwealth aims to create a trusted cyberspace that fosters investment, trade and technological advancements while upholding fundamental rights and security.

1. Cyberspace that supports economic and social development and rights online

- Encourages open markets and global digital trade, ensuring businesses and individuals benefit from cross-border economic opportunities;

- Supports global technical standards to enhance cybersecurity, data protection and trust in online services;
- Ensures online rights align with offline rights, with strong commitments to digital inclusion, cybersecurity awareness and protection against cybercrime;
- Advocates for tolerance, respect and diversity in digital spaces, reinforcing the role of the internet in promoting democratic values and human rights.

2. Building national cybersecurity capabilities

- Stresses the importance of national cybersecurity strategies, legal frameworks and enforcement mechanisms to protect critical infrastructure;
- Calls for businesses and organisations to adopt cybersecurity best practices, securing their digital operations and customer data;
- Encourages investment in cybersecurity skills development, particularly for women and girls, to close the cybersecurity skills gap;
- Promotes collaboration in cyberthreat intelligence-sharing, enhancing collective cybersecurity resilience across Commonwealth member countries;
- Recognises the unique cybersecurity challenges facing developing nations and small island states and commits to capacity-building efforts, including education, skills training and knowledge transfer.

3. Promoting stability in cyberspace through international co-operation

- Supports the development of domestic cybercrime and cybersecurity policies aligned with existing international laws and agreements;
- Advocates for cross-border co-operation in cybercrime investigation and digital evidence-sharing, ensuring effective law enforcement collaboration;
- Promotes harmonised legal approaches to cybersecurity and cybercrime to enhance interoperability across member countries;
- Encourages the establishment of voluntary norms of responsible state behaviour in cyberspace, preventing cyber conflicts and fostering trust;
- Strengthens efforts to define the application of international law including the United Nations Charter, in cyberspace governance, ensuring a secure and rule-based digital environment.

10. Conclusion

This paper has examined the technical and systemic challenges associated with SGs, particularly in developing countries like India. It has also explored the role of emerging technologies such as AI and DTs in enhancing the cybersecurity of SGs. However, fundamental questions remain: How can advanced technologies be leveraged securely without introducing additional risks? Are current regulatory and technical frameworks sufficiently dynamic to address the evolving threat landscape? As SGs become increasingly interconnected with other critical infrastructures, is achieving a truly secure and resilient system feasible without co-ordinated global efforts?

These considerations underscore the pressing need for continuous innovation, interdisciplinary collaboration and the development of adaptive, scalable cybersecurity frameworks. They emphasise the importance of integrating technical, socio-economic and geopolitical strategies to ensure a secure and sustainable smart grid.

References

Abu, S., Anwar, A., Choi, J. et al. (2021) 'IoT-Enabled Smart Energy Grid: Applications and Challenges'. *IEEE Access* 9: 50961–50981.

Adam, I. and Fazekas, M. (2023) 'Overview of Corruption and Anti-Corruption in Infrastructure Development'. Bergen: U4 Anti-Corruption Resource Centre.

Aggarwal, D., Kalra, S. and Agrawal, S. (2023) 'Making India's Advanced Metering Infrastructure Resilient Analysis from a Cyber Security Perspective'. CEEW Issue Brief, March. https://www.ceew.in/sites/default/files/electricity-power-grid-cyber-security-making-advanced-metering-infrastructure-resilient.pdf

Akbar, K., Wang, Y., Ayoade, G. et al. (2023) 'Advanced Persistent Threat Detection Using Data Provenance and Metric Learning'. *IEEE Transactions on Dependable and Secure Computing* 20: 3957–3969. https://ieeexplore.ieee.org/document/9947295

Akitra (2024) 'The Ethical Considerations of AI in Cybersecurity: Balancing Security Needs with Algorithmic Bias and Transparency'. Medium, 16 September. https://medium.com/@akitrablog/the-ethical-considerations-of-ai-in-cybersecurity-balancing-security-needs-with-algorithmic-bias-3b083488ba23

Alcaraz, C. and Lopez, J. (2022) 'Digital Twin: A Comprehensive Survey of Security Threats'. *IEEE Communications Surveys Tutorials* 24(3): 1475–1503.

Alcaraz, A., López, J. and Wolthusen, S. (2017) 'OCPP Protocol: Security Threats and Challenges'. *IEEE Transactions on Smart Grid* 8: 2452–2459.

Ali, M., Kaddoum, G., Li, W.-T. et al. (2023) 'A Smart Digital Twin Enabled Security Framework for Vehicle-to-Grid Cyber-Physical Systems'. *IEEE Transactions on Information Forensics and Security* 18: 5258–5271

Aljohani, T.M. (2024) 'Cyberattacks on Energy Infrastructures as Modern War Weapons-Part II: Gaps, Standardization, and Mitigation'. *IEEE Technology and Society Magazine* 43: 70–77.

Allison, D., Smith, P. and Mclaughlin, K. (2023) 'Digital Twin-Enhanced Incident Response for Cyber-Physical Systems'. Proceedings of the 18th International Conference on Availability, Reliability and Security 2023.

Bajwa, S. (2023) 'Challenges and Opportunities of Promoting Digital Media Literacy in Rural India'. *International Journal of Science and Research*. http://www.ijsr.net/archive/v12i7/SR23709181750.pdf

Balta, E.C., Pease, M., Moyne, J. et al. (2024) 'Digital Twin-Based Cyber-Attack Detection Framework for Cyber-Physical Manufacturing Systems'. *IEEE Transactions on Automation Science and Engineering* 21: 1695–1712.

Cabinet (2023) 'Union Cabinet Approves Expansion of the Digital India Programme with an Outlay of 14,903 Crore'. 16 August. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1949426

Campbell, A. and Singh, V. (2019) 'Lessons from the Cyberattack on India's Largest Nuclear Power Plant'. *The Bulletin*, 14 November. https://thebulletin.org/2019/11/lessons-from-the-cyberattack-on-indias-largest-nuclear-power-plant/

Catota, F., Granger Morgan, M. and Sicker, D. (2019) 'Cybersecurity Education in a Developing Nation: The Ecuadorian Environment'. *Journal of Cybersecurity* 5(1). https://academic.oup.com/cybersecurity/article/5/1/tyz001/5382610?login=false

CEA (Central Electricity Authority) (2021) 'CEA (Cyber Security in Power Sector) Guidelines 2021'. https://cea.nic.in/wp-content/uploads/notification/2021/10/Guidelines_on_Cyber_Security_in_Power_Sector_2021-2.pdf

CEA (Central Electricity Authority) (2024) 'Draft CEA (Cyber Security in Power Sector) Regulations 2024'. https://cea.nic.in/wp content/uploads/notification/2024/08/Draft_CEA_Cyber_Security_in_Power_Sectyor_Regulations_2024_English_Version.pdf

Chehri, A., Fofana, I. and Yang, X. (2021) 'Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence'. *Sustainability* 13(6). https://www.mdpi.com/2071-1050/13/6/3196

CISA (Cybersecurity & Infrastructure Security Agency) (2021) 'Cyber-Attack Against Ukrainian Critical Infrastructure'. 20 July. www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

CISA (nda) 'Critical Infrastructure Sectors'. www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors (accessed 21 February 2025).

CISA (ndb) 'National Infrastructure Protection Plan and Resources'. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/national-infrastructure-protection-plan-and-resources (accessed 21 February 2025).

Cisco Systems (2024) 'Degree of Cybersecurity Readiness Among Organizations in India in 2024'. India: cybersecurity readiness of organizations 2024 | Statista

Culler, M. (2021) 'Securing Distributed Energy Resource Integration'. Thesis, University of Illinois. https://www.ideals.illinois.edu/items/118364

CyberEdge (2024) 'Annual Share of Companies Worldwide That Paid Ransom and Recovered Data from 2018 to 2023'. Global ransom payers that recovered data 2023 | Statista

Cybersecurity Insiders (2023a) 'Which Emerging AI and ML Techniques Hold the Most Promise for Enhancing Cybersecurity Defenses? Top AI and ML techniques to improve cybersecurity 2023 | Statista

Cybersecurity Insiders (2023b) 'What Do You See as the Most Significant Benefits of Incorporating AI into Your Cybersecurity Operations?' Top benefits of integrating AI into cybersecurity 2023 | Statista

Ding, J., Qammar, A., Zhang, Z. et al. (2022) 'Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions'. https://api.semanticscholar.org/CorpusID:252388587

Drishti (2022) 'Critical Information Infrastructure' 22 June. https://www.drishtiias.com/daily-news-analysis/critical-information-infrastructure

DSCI (Data Security Council of India) (2023) 'India Cybersecurity Domestic Market Report 2023'. http://www.dsci.in/files/content/knowledge-centre/2023/India%20Cybersecurity%20Domestic%20Market%202023%20Report.pdf

Eckhart, A., Ekelhart, A. and Weippl, E. (2019) 'Enhancing Cyber Situational Awareness for Cyber-Physical Systems through Digital Twins'. 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA): 1222–1225.

EIS Council (nd) 'Cyber Resilience in the Energy Sector: Safeguarding the Grid from Digital Disruptions'. https://eiscouncil.org/building-cyber-resilience-in-the-energy-sector/ (accessed 21 February 2025).

E-ISAC (2024) 'About the E-ISAC'. https://www.eisac.com/s/about-the-eisac

E-ISAC (2024) 'About the E-ISAC'. https://www.eisac.com/s/about-the-eisac ElHussini, H., Assi, C., Moussa, B. et al. (2021) 'A Tale of Two Entities. Contextualizing the Security of Electric Vehicle Charging Stations on the Power Grid'. *ACM Transactions on Internet of Things* 2: 1–21.

Erika, B. (2024) 'Understanding NERC CIP Requirements for 2024'. *London Daily News*, 23 July. https://www.londondaily.news/understanding-nerc-cip-requirements-for-2024/

ESCC (2024) 'About the ESCC'. https://www.electricitysubsector.org/

European Parliament (2008) 'European Critical Infrastructure'. Revision of Directive 2008/114/EC. www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf

European Parliament (2023) 'The NIS2 Directive: A High Common Level of Cybersecurity in the EU'. Briefing, 8 February. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

Fardanesh, B., Shapiro, A., Saglimbeme, P. et al. (2020) 'A Digital Transformation at New York Power Authority: Using Innovative Technologies to Create a More Efficient Power System'. *IEEE Power and Energy Magazine* 18: 22–30.

Fortinet (nd) 'What Is the CIA Triad?' https://www.fortinet.com/resources/cyberglossary/cia-triad (accessed 21 February 2025).

Goodell, J.W. and Corbet, S. (2022) 'Commodity Market Exposure to Energy-Firm Distress: Evidence from the Colonial Pipeline Ransomware Attack'. *Finance Research Letters*, 1 September. https://api.semanticscholar.org/CorpusID:252288082

Gupta, R. (2022) 'False Polarity: On Reservation System'. *Times of India*, 2 October. https://timesofindia.indiatimes.com/readersblog/contemporary-addict/false-polarity-on-reservation-system-45388/

Haber, M. (2025) 'The Risks Of Implementing AI In Cybersecurity Defense'. Forbes, 6 February. https://www.forbes.com/councils/forbestechcouncil/2025/02/06/the-risks-of-implementing-ai-in-cybersecurity-defense/

Haridas, R., Sharma, S., Bhakar, R. and Mathuria, P. (2023) 'Evolution of Load Redistribution Attack in Cyber Physical Power System'. 2023 IEEE PES Conference on Innovative Smart Grid Technologies - Middle East: 1–5.

Hazrat, M., Hassan, N., Chowdhury, A. et al. (2023) 'Developing a Skilled Workforce for Future Industry Demand: The Potential of Digital Twin-Based Teaching and Learning Practices in Engineering Education'. *Sustainability* 15(23). https://www.mdpi.com/2071-1050/15/23/16433

Hu, J. and Vasilakos, A. (2016) 'Energy Big Data Analytics and Security: Challenges and Opportunities'. *IEEE Transactions on Smart Grid* 7: 2423–2436. https://ieeexplore.ieee.org/document/7466849

Hui, W.S., Othman, R., Omar, N. et al. (2011) 'Procurement Issues in Malaysia'. *International Journal of Public Sector Management*. https://www.emerald.com/insight/content/doi/10.1108/09513551111163666/full/html

Huseinović, A., Mrdović, S., Bikakci, K. and Uludag, S. (2020) 'A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid'. *IEEE Access* 8: 177447–177470.

IBM (2024) 'Distribution of Cyberattacks Across Worldwide Industries in 2023'. Global cyberattacks in industries 2023 | Statista

IBM (nd) 'What Is Critical Infrastructure'. https://www.ibm.com/think/topics/critical-infrastructure (accessed 21 February 2025).

Infosys BPM (nd) 'Smart Grid Security: Attacks and Defence Technique'. www.infosysbpm.com/blogs/business-transformation/smart-grid-security-attacks-and-defence-techniques.html (accessed 21 February 2025).

ISC2 (2023) 'Number of Cybersecurity Professionals Needed Worldwide in 2023, by Country'. Cybersecurity jobs gap by country 2023 | Statista

ISC2 (2024) 'Cybersecurity Workforce Gap Worldwide in 2024, by Region (in 1,000s)'. Cybersecurity workforce gap by region 2024 | Statista

Jain, S. (2024) 'India Budget 2024 Boosts Cybersecurity: AI, Talent, Innovation on the Agenda'. *The Cyber Express*, 24 July. https://thecyberexpress.com/india-budget-2024-boosts-cybersecurity/

Ji, C. and Niu, Y. (2024) 'A Hybrid Evolutionary and Machine Learning Approach for Smart City Planning: Digital Twin Approach'. Sustainable Energy Technologies and Assessments 2024.

Keeper Security (2022) 'US Cybersecurity Census Report'. 2022-US-Cybersecurity-Census.pdf

Sophos (2022) Self-assessed Cyber Security Maturity Level at Companies in the Asia-Pacific Region in 2022, by Country. https://www.statista.com/statistics/1368028/apac-cyber-security-maturity-level-at-companies-by-country/

Kong, P.Y. (2022) 'A Review of Quantum Key Distribution Protocols in the Perspective of Smart Grid Communication Security'. *IEEE Systems Journal* :141–54.

Krause, T., Ernst, R., Klaer, B. et al. (2021) 'Cybersecurity in Power Grids: Challenges and Opportunities'. Sensors 21(18): 6225.

Leadvent (2024) 'Zero Trust Architecture: A New Paradigm for Cyber Security in the Energy Sector'. 20 June. https://www.leadventgrp.com/blog/zero-trust-architecture-a-new-paradigm-for-cyber-security-in-the-energy-sector

Lee, M., Assante, M. and Conway, T. (2016) 'Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case, Protocol TLP: White E-ISAC'. https://www.sans.org/industrial-control-systems-security/

Lei, B., Janssen, P., Stoter, J. and Biljecki, F. (2023) 'Challenges of Urban Digital Twins: A Systematic Review and a Delphi Expert Survey'. *Automation in Construction* 147. https://www.sciencedirect.com/science/article/pii/S0926580522005866

Lindemulder, G. and Kosinski, M. (2024) 'What Is a Man-in-the-Middle (MITM) Attack?' IBM, 11 June. www.ibm.com/think/topics/man-in-the-middle

Lv, Z., Chen, D., Cao, B. et al. (2024) 'Secure Deep Learning in Defense in Deep-Learning-as-a-Service Computing Systems in Digital Twins'. *IEEE Transactions on Computers* 73: 656–668.

Ma, R., Chen, H.H. and Meng, W. (2013) 'Smart Grid Communication: Its Challenges and Opportunities'. *IEEE Transactions on Smart Grid* 4: 36–46.

Ministry of Education (India) (2020) 'National Education Policy 2020'. https://www.education.gov.in/sites/upload_files/mhrd/files/NEP_Final_English.pdf

Ministry of Electronics and IT (2023) 'Notes on Demands for Grants, 2023-2024'. http://www.indiabudget.gov.in/doc/eb/sbe27.pdf (accessed 12 December 2024).

Ministry of Power (India) (2024a) 'Smart Meters Installed in India from Financial Year 2020 to 2025 (in 1,000s)'. India: smart meters installed 2025 | Statista

Ministry of Power (India) (2024b) 'Cybersecurity of Power Grids'. 8 August. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2043154

Mishra, N. and Pandya, S. (2021) 'Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review'. *IEEE Access* 9: 59353–59377. https://ieeexplore.ieee.org/document/9405669

Mohamed, A. (2013) 'Phishing and Social Engineering Techniques'. Infosec, 18 April.

www.infosecinstitute.com/resources/hacking/phishing-and-social-engineering-techniques/

Mollah, M.B., Zhao, Z., Niyato, D. et al. (2019) 'Blockchain for Future Smart Grid: A Comprehensive Survey'. *IEEE Internet of Things Journal* 8: 18–43.

Musanzikwa, M. (2013) 'Public Procurement System Challenges in Developing Countries: The Case of Zimbabwe'. *International Journal of Economics, Finance and Management Sciences.* https://www.sciencepublishinggroup.com/article/10.11648/j.ijefm.20130102.18

NCSC (National Cyber Security Centre) (nd) 'A Guide to Ransomware'. https://www.ncsc.gov.uk/ransomware/home (accessed 21 February 2025).

NPSA (National Protective Security Authority) (2023) 'Critical National Security'. 26 April. www.npsa.gov.uk/critical-national-infrastructure-0

Okafor, C. and Chimereze, C. (2020) 'Brain Drain among Nigerian Nurses: Implications to the Migrating Nurse and the Home Country'. https://ideas.repec.org/a/bjc/journl/v7y2020i1p15-21.html

Omrany, H., Al-Obaidi, K., Husain, A. and Ghaffarianhoseini, A. (2023) 'Digital Twins in the Construction Industry: A Comprehensive Review of Current Implementations, Enabling Technologies, and Future Directions'. *Sustainability* 15(14): https://www.mdpi.com/2071-1050/15/14/10908

Opoku, D., Perera, S., Osei-Kyei, R. et al. (2023) 'Barriers to the Adoption of Digital Twin in the Construction Industry: A Literature Review'. *Informatics* 10. https://www.mdpi.com/2227-9709/10/1/14

Otuoze, A., Mustafa, M., Ibrahim, O. et al. (2019) 'Threats and Challenges of Smart Grids Deployments: A Developing Nations' Perspective'. *ELEKTRIKA- Journal of Electrical Engineering* 18: 33–43.

Pengfei Zhao, A., Li, S., Gu, S. et al. (2024) 'Cyber Vulnerabilities of Energy Systems'. *IEEE Journal of Emerging and Selected Topics in Industrial Electronics* 5(4): 1455–1469.

Pervez, Z., Khan, Z., Ghafoor, A. et al. (2023) 'SIGNED: Smart clty diGital twiN vErifiable Data Framework'. *IEEE Access* 11: 29430–29446. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10078428

Pillitteri, V. and Brewer, T.L. (2014) 'Guidelines for Smart Grid Cybersecurity'. https://api.semanticscholar.org/CorpusID:114196261

Piroumian, V. (2021) 'Digital Twins: Universal Interoperability for the Digital Age'. *Computer* 54: 61–69.

Pirta-Dreimane, R., Romanovs, A., Bikovska, J. et al. (2024) 'Enhancing Smart Grid Resilience: An Educational Approach to Smart Grid Cybersecurity Skill Gap Mitigation'. *Energies* 17(8). https://www.mdpi.com/1996-1073/17/8/1876

Poornima, B.G. (2022) 'Cyber Threats and Nuclear Security in India'. *Journal of Asian Security and International Affairs* 9: 183–206.

Pourmirza, Z. and Walker, S.L. (2021) 'Electric Vehicle Charging Station: Cyber Security Challenges and Perspective'. 2021 IEEE 9th International Conference on Smart Energy Grid Engineering: 111–116.

Proofpoint (2024) 'Share of CISOs in Companies in the United States in Agreement That Human Error is Their Organization's Biggest Cyber Vulnerability from 2021 to 2024'. U.S. CISO biggest cyber vulnerability is human error 2024 | Statista

Radoglou-Grammatikis, P. and Sarigiannidis, P. (2019) 'Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems'. *IEEE Access* 7: pp. 46595– 46620.

Raizada, A. (2024) 'India's Broken Power Economics Addressing DISCOM Challenges'. IFRI Memo, 15 October. https://www.ifri.org/sites/default/files/2024-10/ifri_raizada_india_broken_power_economy_2024_1.pdf

Rock, A. (2020) 'Report: 57% of IoT Devices Vulnerable to Severe Attack'. CEPro, 21 April. www.cepro.com/news/57-percent-iot-devices-vulnerable-attack/

Sadoian, L. (2024) 'NCIIPC Explained: Safeguarding India's Critical Infrastructure'. Upguard, 8 January. https://www.upguard.com/blog/nciipc-explained

Salloum, S., Gaber, T., Vadera, S. and Shaalan, K. (2022) 'A Systematic Literature Review on Phishing Email Detection Using Natural Language Processing Techniques'. *IEEE Access* 10(11). https://ieeexplore.ieee.org/document/9795286

Sayed, M., Atallah, R. and Debabbi, M. (2021) 'Electric Vehicle Attack Impact on Power Grid Operation'. https://api.semanticscholar.org/CorpusID:244477823

Shi, H., Chen, X., Gu, C. et al. (2024) 'Review of the Opportunities and Challenges to Accelerate Mass-Scale Application of Smart Grids with Large-Language Models'. *IET Smart Grid*, 6 November. https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/stg2.12191

Shirvani, S., Baseri, Y. and Ghorbani, A. (2024) 'Evaluation Framework for Electric Vehicle Security Risk Assessment'. *IEEE Transactions on Intelligent Transportation Systems* 25: 33–56.

Sifat, M., Das, S. and Choudhury, S. (2024) 'Design, Development, and Optimization of a Conceptual Framework of Digital Twin Electric Grid Using Systems Engineering Approach'. *Electric Power Systems Research* 26(1). https://linkinghub.elsevier.com/retrieve/pii/S0378779623008465

SMPnet (2024) 'From Grid to Nation: The Convergence of Cybersecurity, National Security, and Power Grids'. Techspace, 1 August. www.smpnet.tech/post/from-grid-to-nation-the-convergence-of-cybersecurity-national-security-and-power-grids

Sophos (2022) 'Self-Assessed Cyber Security Maturity Level at Companies in the Asia-Pacific Region in 2022, by Country'. APAC: cyber security maturity level at companies by country 2022 | Statista

Sophos (2024) 'Root Causes of Ransomware Attacks in Worldwide Organizations as of February 2024, by Industry, 2024'. Cause ransomware attacks worldwide by industry 2024 | Statista

Sousa, B., Ariero, M., Pereira, V. et al. (2021) 'ELEGANT: Security of Critical Infrastructures with Digital Twins'. *IEEE Access* 9: 107574–107588.

Srivastava, A., Liu, C.C., Stefanov, a. et al. (2024) 'Digital Twins Serving Cybersecurity: More Than a Model: Cybersecurity as a Future Benefit of Digital Twins 2'. *IEEE Power and Energy Magazine* 22: 61–71

Statista (2023) 'Smart Grid Technology Market Size Worldwide from 2022 to 2028 (in Billion U.S. Dollars), 2023'. Global smart grid market size 2022-2028 | Statista

Su, H., Qiu, M. and Wang, H. (2012) 'Secure Wireless Communication System for Smart Grid with Rechargeable Electric Vehicles'. *IEEE Communications Magazine* 50. https://ieeexplore.ieee.org/document/6257528

SWP (2024) 'Number of political cyberattacks launched against U.S. 2024, by attack characteristic'. U.S. targeted political cyberattacks 2024 | Statista

Techopedia (2024) 'Value of the Artificial Intelligence (AI) Cybersecurity Market Worldwide from 2023 to 2030 (in Billion U.S. Dollars)'. Global AI cybersecurity market size 2030 | Statista

The Commonwealth (2018) 'Commonwealth Cyber Declaration, 2018'. https://thecommonwealth.org/commonwealth-cyber-declaration-2018

The White House (2021) 'Improving the Nation's Cybersecurity'. Executive Order 14028, 5 May.

Tiscareno, K.K. (2019) 'The Growing Cyber-Risk to Our Electricity Grids - and What to Do About It'. WEF, 19 April. www.weforum.org/stories/2019/04/the-growing-risk-to-our-electricity-grids-and-what-to-do-about-it/

Townsend, K. (2018) 'The Malicious Use of Artificial Intelligence in Cybersecurity'. *Security Week*, 29 March. https://www.securityweek.com/malicious-use-artificial-intelligence-cybersecurity/

Transparency International (2024) 'Corruption Perceptions Index in the G20 Countries 2023'. Corruption perceptions index - G20 countries 2023 | Statista

Tripathi, N., Hietala, H., Xu, Y. and Liyanage, R. (2024) 'Stakeholders Collaborations, Challenges and Emerging Concepts in Digital Twin Ecosystems'. *Information and Software Technology* 169: 107424. https://www.sciencedirect.com/science/article/pii/S0950584924000296?via%3Dihub

TSC (2023) 'India's Poor Cyber Awareness: Lack of Board-Buy in and Digital Literacy Damaging Security Levels'. 16 March. https://thesecuritycompany.com/the-insider/indias-poor-cyber-awareness-lack-of-board-buy-in-and-digital-literacy-damaging-security-levels/

US Department of Energy (nd) 'Cybersecurity Capability Maturity Model (C2M2)'. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2 (accessed 21 February 2025).

Van den Brink, H. and Broos, P. (2022) 'Cyber Security Challenges in the Electric Vehicle Infrastructure'. CIRED Porto Workshop 2022: E-mobility and Power Distribution Systems 2022. https://api. semanticscholar.org/CorpusID:251123501

Waqar, A., Othman, I. Almujibah, H. et al. (2023) 'Factors Influencing Adoption of Digital Twin Advanced Technologies for Smart City Development: Evidence from Malaysia'. *Buildings* 13(3). https://www.mdpi.com/2075-5309/13/3/775

Wang, X. and Yi, P. (2011) 'Security Framework for Wireless Communications in Smart Distribution Grid'. *IEEE Transactions on Smart Grid* 2: 809–818. https://ieeexplore.ieee.org/document/6060942

WEF (World Economic Forum) (2024) 'What Are You Most Concerned about in Regards to Generative AI's Impact on Cyber?' Global concerns about GenAI's impact on cybersecurity 2024 | Statista

Yang, J. and Lim, H. (2021) 'Deep Learning Approach for Detecting Malicious Activities Over Encrypted Secure Channels'. *IEEE Access* 9: 39229–39244. https://ieeexplore.ieee.org/document/9373407

Young, K. (2024) 'Cyber Case Study: Colonial Pipeline Ransomware Attack'. Coverlink, 22 July. https://coverlink.com/case-study/cyber-case-study-colonial-pipeline-ransomware-attack/

Yuan, Y., Li, Z. and Ren, K. (2012)' False Data Injection Attacks in Smart Grid'. https://api.semanticscholar.org/CorpusID:108476110

Zeng, P., Liang, H., Zhang, N. and Song, C. (2023) 'Editorial: Recent Advances of Edge Computing for Smart Grid'. *Frontiers in Energy Research* 11. https://www.frontiersin.org/journals/energy-research/articles/10.3389/fenrg.2023.1229000/full

Zhu, Z., Lin, K., Jain, A. and Zhou, J. (2020) 'Transfer Learning in Deep Reinforcement Learning: A Survey'. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 45: 13344–13362. https://ieeexplore.ieee.org/document/10172347

Zibaeirad, A., Koleini, F., Bi, S. et al. (2024) 'A Comprehensive Survey on the Security of Smart Grid: Challenges, Mitigations, and Future Research Opportunities'. https://arxiv.org/abs/2407.07966

Zografopoulos, I., Ospina, J. and Konstantinou, C. (2020) 'Harness the Power of DERs for Secure Communications in Electric Energy Systems'. https://arxiv.org/abs/2009.06975

Zsuchy, D. (2023) 'Data Security Concerns of Smart Grids'. CEE Legal Matters, 19 July. https://ceelegalmatters.com/hungary/23960-data-security-concerns-of-smart-grids

About the authors

Rohini Haridas is currently a Commonwealth Split-Site Scholar at the University of Bath, UK, and a full-time PhD student of Electrical Engineering at Malaviya National Institute of Technology in Jaipur, India. She received her Bachelor's and Master's degrees in engineering from India, specialising in electrical power systems, in 2011 and 2013, respectively. Her research focuses on smart grid security, covering areas such as attack modelling, cascading failures, stealth enhancement and uncertainty modelling. She is a certified trainer at the National Power Training Institute, the apex body of the Ministry of Power of the Government of India, responsible for educating distribution company utility personnel across the country on smart grid cybersecurity.

Satish Sharma received his PhD from the Indian Institute of Technology, Delhi, India. He is an assistant professor with the Department of Electrical Engineering, Malaviya National Institute of Technology Jaipur, India. Previously, he was a Postdoctoral Fellow with the Intelligent and Autonomous System group at Centrum Wiskunde & Informatica, Amsterdam, Netherlands. He received the Power System Operation Corporation (a Government of India enterprise) Award in 2017, in recognition of innovative technical research excellence in power systems. His research interests include smart grid cybersecurity, power systems economics and multiagent systems.

Rohit Bhakar received his PhD degree from the Indian Institute of Technology, Roorkee, India. He was a Prize Fellow on Energy Demand Reduction at the Department of Electronic and Electrical Engineering, University of Bath, UK. He is currently a Professor with the Malaviya National Institute of Technology, Jaipur. He is a member of the State Advisory Committee of Rajasthan Electricity Regulatory Commission. He has held multiple research grants from Indian and international funding agencies, including two India–UK Consortium grants, in association with several Indian Institutes of Technology and UK universities. His research interests include smart grid cybersecurity, power system operation and economics, network pricing and electricity markets.

Chenghong Gu received his PhD degree from the University of Bath, UK. He is a professor with the Department of Electronic and Electrical Engineering in the University of Bath. Previously, he was an Engineering and Physical Sciences Research Council Research Fellow with the University of Bath. He was a member of Ofgem's Safety, Resilience & Reliability Working Group and the IEEE Working Group on Network Charging. He co-chairs the Markets and Regulation Working Group of the Supergen Energy Networks Hub. His primary research is concerned with planning and operating resilient smart multi-vector energy systems of electricity, natural gas, heating/cooling and transportation towards zero emissions by 2050 under dramatic climate change.

The Commonwealth

Commonwealth Cyber Journal \ 79
Print ISSN 2959-3018, online ISSN 2959-3026
thecommonwealth.org/Cyber-journal

Strengthening Cybersecurity and Data Protection Frameworks in Commonwealth Member Countries: Policy and Institutional Approaches

Otshepeng Mazibuko[1]

Abstract

In an increasingly interconnected world, cyber threats pose significant risks to the security and privacy of individuals, organisations and governments. As digital ecosystems expand, the legal, policy and institutional frameworks governing cybercrime and cybersecurity must evolve to ensure the protection of personal data and the privacy of users. This paper explores the current state of privacy and data protection mechanisms within Commonwealth countries, highlighting the disparities, challenges and opportunities in developing more effective frameworks. Drawing on recent trends, this paper examines the effectiveness of existing legislation, policy and initiatives designed to combat cybercrime and improve data protection. It also investigates how different Commonwealth countries address issues such as cross-border data sharing, cybersecurity capacity building and digital sovereignty. It gives special attention to the role of international co-operation and institutional development in mitigating emerging cyber threats and fostering a resilient cybersecurity environment across the Commonwealth. By assessing both successes and gaps, the paper proposes strategies for strengthening data protection laws, improving cybersecurity infrastructures and fostering multilateral partnerships that can promote a secure digital landscape. It aims to contribute to the ongoing discourse on privacy and cybercrime governance and offer policy recommendations that Commonwealth nations can implement to safeguard their digital future.

1 Research assistant at the University of Cape Town for a PUBGEM-Africa project, GeneMAP Research Center, and PhD candidate at the University of Pretoria.

1. Introduction

As the world is being digitalised, governments, organisations and individuals are concerned with critical issues of cybersecurity and data protection (Shackelford 2012). These concerns relate to the sensitive data generated, processed and stored together with the speed, complexity and volume of digitalisation (Clarke 2019). This technological development contributes to socio-economic growth, but the associated data breaches, cyber-attacks and privacy violations pose significant risks (Smith et al, 2020).

Challenges with cybersecurity and data protection persist. This relates to the variation in levels of economic development and technological adoption across the Commonwealth. This needs to be addressed by the Commonwealth (Commonwealth Secretariat, 2018). Some countries are struggling with resource constraints, fragmented regulatory frameworks and gaps in capacity. These prevent them from fulfilling their role in implementing data protection measures (Arora and Luthra 2021). However, cultural similarities, historical ties and collaboration bring opportunities for confronting the challenges – not in silos, but collectively (Weber 2020).

This paper examines differences in data protection procedures and cybersecurity preparedness in Commonwealth nations. It considers difficulties for countries in protecting privacy and personal information and suggests areas for co-operation, capacity building and policy harmonisation (Mistry 2022). It aims to add to continuing discussion on improving cybersecurity and data protection in the Commonwealth context by pointing out gaps and suggesting workable solutions.

2. The cybersecurity landscape in Commonwealth countries

Groups of nations that form the Commonwealth have undergone different levels of digital transformation. Advanced economies have enhanced their digital infrastructures and broadened coverage. (Commonwealth Telecommunications Organisation 2019). Although these advancements showcase the association's strengths and capabilities, they also highlight the challenges posed by cyber threats. This is evident in developed countries such as Canada and the United Kingdom through their well-designed cybersecurity frameworks (Johnson 2017).

The threats are significant because Commonwealth nations are diverse. Individuals and organisations face identity and intellectual property theft, which compromise them greatly (Sharma 2020). Hackers disguise themselves as sophisticated and state-sponsored to directly attack critical infrastructure including power grids, healthcare systems and financial institutions (Clarke 2019). Threats are compounded for member countries with inadequate resources to enforce regulations, or where there is less co-operation with others (Mistry 2022).

Privacy and data protection measures are essential for combatting cyber threats. Cybersecurity needs strengthened more broadly to protect individuals' data and to enhance trust in digital systems (Sharma 2020). Sensitive information must be protected through effective data protection measures to eliminate cyber-attacks (Weber 2020). Geopolitics and socio-economic disparities make it difficult for the Commonwealth to adopt uniform standards for data privacy (Arora and Luthra 2021).

3. Legal, policy and institutional frameworks

Commonwealth nations have differences and similarities, for example legislation, socio-economic contexts and technologies. These shape the associations' legal framework for governance in privacy and data protection (Commonwealth Secretariat, 2018a; Greenleaf 2021). Some of the developing and underdeveloped countries lack privacy legislation and the capacity to update legal frameworks as needed. In comparison, the UK has data protection laws that align with the European standards of the General Data Protection Regulation (GDPR) (ICO 2021).

The advantages of comprehensive legal protection are evident in nations with highly developed regulatory frameworks. Accountability and the rights of individuals, particularly the rights to access and to ensure the accuracy of their data, are embedded in the UK's Data Protection Act 2018, which assures personal data protection. Guidelines stipulated in Australia's Privacy Act 1988 place restrictions on cross-border data transfers and on the handling of personal information.

However, it is difficult for many developing Commonwealth nations to set up and implement comparable systems. The non-existence of comprehensive legal provisions makes them vulnerable to data misuse and cybercrime. Nevertheless, countries such as Kenya and Nigeria have enacted data protection laws consistent with global good practice, indicating progress (DataGuidance 2020; OAIC 2020). Data Protection Act principles such as data minimisation, consent-based processing and accountability, are reflected in the Kenyan framework, which aligns with global practice and standards.

Despite such developments there are challenges with the implementation process, and inconsistencies in the scope and enforcement of any legislation. This hinders effective partnership and cross-border data sharing across the Commonwealth (Commonwealth Secretariat ,2018b). Co-ordination and legal assistance are needed across Commonwealth member countries to improve transnational cyber threats.

Assessment of institutional frameworks for cybersecurity

Institutional frameworks need to be efficient to ensure the implementation and enforcement of established legal provisions. Such frameworks vary across the Commonwealth. Developed and resourced countries such as the UK and Singapore have established regulatory bodies such as the Information Commissioner's Office (ICO)

in the former and the Personal Data Protection Commission (PDPC) in the latter. This enables handling of intricate issues, including compliance campaigns, public education and awareness campaigns, and data breaches (ICO 2021; PDPC 2022).

Under-resourced countries lack the institutional capacity to implement and enforce privacy and cybersecurity laws effectively. It means that agencies struggle with fragmented governance, limited technical expertise, mandates that overlap and inadequate funding (Greenleaf 2021). For example, the enforcement of existing laws and public trust in digital systems are undermined by the non-existence of data protection authorities in some of the African Commonwealth nations.

Capacity-building initiatives and regional cooperation can help address this challenge. Programmes like the Commonwealth Cyber Programme offer training and technical assistance to member countries. Additionally, international organisations such as the International Telecommunication Union (ITU) can enhance the capabilities of under-resourced institutions (ITU 2021).

Gaps and inconsistencies in legal and policy measures across member countries

A coherent and integrated strategy for cybersecurity and data protection is made extremely difficult by the Commonwealth's disparate legal and policy frameworks. These disparities show themselves in several ways including:

1. Scope and coverage

The absence of comprehensive privacy laws and the reliance on sector-specific regulations mean that countries fail to confront the implications of data protection in the digital economy. Critical sectors such as healthcare and education are prone to cyber threats due to segmented approaches (UNCTAD 2021).

2. Enforcement mechanisms

For privacy and cybersecurity to be effective, adequate authority, resources and regulatory bodies are needed. Low compliance and limited-to-no accountability for violations in many Commonwealth countries result from weak or non-existent enforcement mechanisms (Greenleaf, 2021).

3. Cross-border data transfers

Complex international partnerships and inconsistent policies on cross-border data transfers create legal uncertainty for businesses operating across multiple jurisdictions (ICO 2021; OAIC 2020). While some countries lack a data protection framework, others, like Australia and the UK, have established clear guidelines

4. Public awareness and education

   Public education and education campaigns enable legal and policy measures to be effective. In many Commonwealth nations legislative efforts are weakened by their citizens' lack of knowledge about privacy and cybersecurity risks (PDPC 2022).

Confronting these gaps requires an organised approach that emphasises the harmonisation of laws; encourages and promotes public-private collaborations; and builds capacity. Challenges could be overcome by leveraging the expertise and resources of Commonwealth member countries and establishing a solid legal and institutional framework for data protection, including protection of personal data.

4. Challenges in cybersecurity and data protection

Cross-border data sharing: Issues and implications for privacy

Data needs to be able to flow across borders to enhance and develop the commercial, innovation and governance sectors. But there are challenges because of the different legal systems and data protection levels across Commonwealth countries (Daly 2020). Different privacy regulations and frameworks may lead to a lack of trust within shared digital ecosystems (Greenleaf, 2021).

There may be a lack of clarity about data ownership and jurisdiction. The individual responsible for safeguarding data, particularly in transnational systems prone to breaches, raises critical concerns about safety and security (ITU 2022). Moreover, unresolved issues related to surveillance and the misuse of personal information can hinder partnerships and the establishment of international collaboration. A coherent approach to respecting national laws and building trust in shared systems can help to overcome concerns (Commonwealth Secretariat 2018c).

Data localisation policies for ensuring that countries' data do not move beyond borders vary considerably. While such policies are supposed to protect data subjects or citizens in general, they can prevent economic integration and can lead to conflict (Greenleaf 2021). This hinders access to global markets and technological advancement.

Cybersecurity capacity building: Barriers to implementation in resource-constrained countries

Effective data protection and privacy requires sustained capacity building to strengthen cybersecurity. Under-resourced Commonwealth countries with a lack of transferable skills, policies and practical infrastructure to confront cyber threats, face barriers in ensuring regulation (ITU 2022).

Lack of finance is a major barrier to investing in training, adapting technology, and developing and maintaining concrete cybersecurity systems. For developing countries in the Commonwealth, immediate priorities, such as healthcare, education and poverty alleviation, must compete with such investment (Commonwealth Secretariat 2018b).

Lack of professional expertise is another obstacle. Mobility and migration of skilled personnel for career opportunities elsewhere, lead to a lack of qualified staff in the highly specialised field of cybersecurity in some countries. Low- and middle-income countries (LMICs) run the risk of being unable to detect and effectively respond to cyber threats because of the lack of local expertise (Daly 2020).

Capacity-building initiatives are delayed by institutional weakness. Commonwealth nations often lack committed cybersecurity agencies to drive national efforts through clear policy frameworks and regulations. In some instances, the intervention and involvement of politics and bureaucracy aggravates this, raising questions of sustainability (ITU 2022).

Digital sovereignty: Balancing national interests with global co-operation

As an association of member countries, the Commonwealth faces growing challenges in managing data governance, as this is perceived to undermine the digital sovereignty of individual member countries. This tension is contributing to resistance towards global collaboration on cybersecurity and data protection (Greenleaf 2021).

It can be difficult to find a balance. Controlling digital resources is important for protecting the privacy of citizens. Isolationist policies limit access to global expertise exposing countries to cyber threats that go beyond borders.

Some Commonwealth nations safeguard their sovereignty by implementing policies that restrict internet governance. This is to control internal cyberspace. However, this limits international partnerships and economic growth and suppresses innovation (Daly 2020). To address this tension and promote meaningful participation in global cybersecurity efforts, the frameworks enable countries to assert control over their digital sovereignty.

Community-based training programmes

To close the digital literacy gap, community-based training initiatives in some member countries, use the expertise of nearby NGOs and civic leaders. To make training inclusive and accessible, these initiatives provide interactive workshops in regional languages. By emphasising practical skills including smartphone use, online service access and basic troubleshooting, such training guarantees that participants acquire real-world digital competence. Influencers in the community can act as advocates for digital literacy, boosting long-term involvement and programme participation. Furthermore, modifying

the training to meet community needs – like expanding access to healthcare or putting farmers in touch with agricultural markets – guarantees that such training initiatives have a significant and long-lasting effect.

Educational and public-private partnerships

Collaborating with educational institutions provides a long-term strategy for promoting digital literacy from a young age. Consistent exposure to critical abilities is ensured by incorporating digital skills into the standard curriculum at all educational levels. In order to encourage students to use digital technologies to tackle real-world problems, educational institutions can also offer seminars, coding camps and hackathons. Programmes for training teachers are essential for giving them the skills they need to teach digital knowledge. Educational institutions can give students access to resources like computers, internet connectivity, internships and mentorship opportunities. Partnerships with the private sector may strengthen these initiatives and close the gap between education and real-world application.

Public awareness campaigns

Campaigns to raise public awareness are essential for advancing cybersecurity and digital literacy and for encouraging safer online conduct in all communities. Social media platforms can provide interesting content like infographics, videos and interactive posts that appeal especially to younger audiences. Important messages about internet safety can be amplified through partnerships with thought leaders, celebrities or local influencers. Town hall talks and digital literacy fairs are examples of community events that provide attendees with the chance to speak with professionals face-to-face and to learn about cybersecurity best practice. The significance of such campaigns is demonstrated by successful examples such as the 'Stay Safe Online' campaign- https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/s3fs-public/2024-05/cybercrime_laws_updf.pdf?utm_source=chatgpt.com, that raises awareness of phishing scams, data protection and secure password practice in effective and relatable ways.

5. Role of multilateral co-operation

Examination of existing Commonwealth-wide initiatives and partnerships

A multifaceted partnership is essential in addressing and combating challenges related to data protection and cybersecurity within the Commonwealth. This is to facilitate meaningful collaboration, capacity building and knowledge sharing among member countries.

An important milestone in promoting cybersecurity resilience is the adoption of the Commonwealth Cyber Declaration in 2018. It emphasises capacity building, the protection of critical infrastructure and the importance of international co-operation. It recommends that Commonwealth member countries integrate the framework to align effectively with global cybersecurity standards.

There are other programmes, such as those offered by the Commonwealth Telecommunications Organisation (CTO), aimed at supporting member countries to improve and confront information and communication technology (ICT) capabilities and cybersecurity challenges. These include workshops, training sessions and guidance through policy processes, essential for establishing and promoting best practice across the Commonwealth.

These programmes highlight the necessity for collective action and for adoption of stronger institutional mechanisms to enhance effectiveness. Member countries continue to face the challenges that these programmes aim to address. This emphasises the importance of sustained support and accountability.

Importance of international collaboration in combatting cybercrime

International collaboration is effective in addressing and combatting cybersecurity challenges globally. This is particularly important to Commonwealth member countries as they share vulnerabilities to cyber threats that are of significant concern.

The investigation and prosecution of cybercrime are key areas in which international collaboration can provide a collective response. Cyber hackers exploit regulatory loopholes and legal gaps to evade accountability. Mutual legal assistance treaties (MLATs) are collaborative frameworks that enable countries to share intelligence, pursue justice and co-ordinate investigations through joint taskforces.

Global partnership promotes the exchange of best practice and recommendations on technological advances. This enables member countries to enhance their access to cutting-edge solutions for combatting cyber threats through international forums and collaborative working groups. The joint approach fosters trust and solidarity in the collective response to emerging challenges.

Best practice from successful initiatives

Numerous approaches strengthen joint partnerships within the Commonwealth by providing valuable lessons. For example, the Malabo Convention is a formal regional framework of the African Union that co-ordinates cybersecurity and data protection initiatives. The regional model consistently demonstrates the ability of regional agreements to align policy and foster collective action.

The European Union's GDPR has paved the way for, and shaped, global privacy legislation. Compatibility and greater integration are key principles of GDPR that help Commonwealth member countries strengthen their respective data protection frameworks.

Platforms that promote knowledge transfer and skills development have proven to be effective in enhancing capacity and fostering innovation. For example, a balanced and resilient cybersecurity ecosystem could be achieved by pairing developed countries with under-resourced ones, effectively transferring skills and technologies.

6. Opportunities for strengthening frameworks

Recommendations for enhancing data protection laws and policies

Commonwealth nations should strengthen their respective data protection laws and policies while recognising the distinct legal and socio-economic contexts of each member state. Data protection must have an established baseline, drawing lessons from the GDPR (European Union 2016). Core principles such as data minimisation, transparency and accountability can serve as a framework for Commonwealth nations to adopt incremental approaches towards an equivalent system.

Commonwealth countries should prioritise establishing independent data protection authorities and commissioners, equipped with context-specific regulations and enforcement mechanisms to ensure compliance. Such authorities can provide guidance on best practice, investigate breaches and impose penalties.

Maintaining contextual relevance, along with stakeholder involvement and public engagement, can effectively facilitate the policymaking process. The practice of inclusivity can address concerns about the rights of marginalised communities in the context of emerging data-driven technologies, such as artificial intelligence (AI), and its effects on small businesses.

Strategies for building resilient cybersecurity infrastructures

Technology, policy and human resources must all be used in a complex strategy to create resilient cybersecurity infrastructures. Prioritising the creation of national cybersecurity policies that address regional risks and conform to international standards should be a top priority. Protecting critical infrastructure requires significant investment. Adopting cutting-edge technologies like multi-factor authentication, intrusion detection systems and zero-trust architectures is part of this. Since the private sector frequently controls sizeable portions of vital infrastructure, public-private partnerships can be extremely important.

Building capacity is equally important. To resolve the global scarcity of qualified cybersecurity specialists, governments must invest in education and training. Local talent pools can be developed with the aid of initiatives like public awareness campaigns,

specialised training programmes and scholarships. Mechanisms for incident response and recovery ought to be improved too. Establishing computer emergency response teams (CERTs) or security operations centres (SOCs) can enable nations to detect, respond to and mitigate cyber threats effectively.

Approaches to foster multilateral partnerships and knowledge sharing

Because cyber threats are transnational, multilateral collaborations are essential. The Commonwealth provides a special setting for encouraging these kinds of partnerships. Establishing regional centres for cybersecurity research and innovation is one strategy that uses the resources and experience of developed member countries to assist others. Knowledge-sharing platforms, like the programmes of the CTO, can help spread technical know-how, case studies and best practice. Regular workshops, online training courses and co-operative projects involving various stakeholders should all be added to these platforms.

Harmonising legal frameworks to facilitate smooth cross-border co-operation should be another goal. This entails establishing MLATs, co-ordinating data protection standards and developing procedures for co-operative cybercrime investigations. Commonwealth nations intending to improve their cybersecurity capabilities can benefit from additional resources and knowledge offered by international organisations such as the ITU and INTERPOL.

7. Case studies

Analysis of selected Commonwealth countries

Analysing the methods used by different Commonwealth nations indicates a range of approaches to and results from data protection and cybersecurity.

UK

With reputable frameworks like the Government Cyber Security Strategy, the UK is a leader in cybersecurity. Establishing the National Cyber Security Centre (NCSC) has improved the country's capacity to identify and address threats. Strong privacy rights are guaranteed under the UK's Data Protection Act 2018, which includes the GDPR. The significance of institutional leadership, consistent infrastructure investment and proactive co-operation with foreign partners are among the most important lessons from the UK (European Union 2016).

India

With a growing digital economy, India has serious cybersecurity issues. Despite implementation delays, the 2023 Digital Personal Data Protection Act creates a thorough framework for data protection. India's emphasis on protecting vital assets is exemplified by programmes like the National Critical Information Infrastructure Protection Centre (NCIIPC). Nonetheless, it faces difficulties because of limited capacity and a disjointed regulatory environment.

Botswana

Botswana has made strides in developing a national cybersecurity strategy focusing on building awareness and strengthening institutional capacity (Phahlamohlaka et al. 2022). Given its small size, Botswana deserves praise for its efforts to improve its cybersecurity infrastructure. The Cybercrime and Computer-Related Crimes Act, 2018 offers a legal foundation for dealing with cyberthreats, while the Botswana Communications Regulatory Authority (BOCRA) oversees ICT growth and security. To solve capacity shortages, Botswana is exemplary in using regional collaborations and customising tactics to local settings.

Singapore

With a developed ecosystem backed by the Cyber Security Agency (CSA), Singapore stands out as a global leader in cybersecurity. The country's cybersecurity strategy integrates international co-operation, business sector engagement and public awareness in a comprehensive approach. Singapore's achievements demonstrate the importance of a proactive, all-encompassing approach to cybersecurity. Singapore's emphasis on international co-operation is one of its distinguishing features. It actively contributes to improving cybersecurity internationally through bilateral agreements, partnerships with international organisations and involvement in regional forums such as the Association of Southeast Asian Nations (ASEAN) (Ee 2024).

Fiji

Fiji has introduced regional collaboration efforts to address cybersecurity threats, leveraging partnerships with larger nations and organisations (Tamanikaiwaimaro 2021). Fiji regularly interacts with institutions like the United Nations and regional initiatives like the Pacific Islands Forum to develop strong cybersecurity frameworks.

Eswatini

Eswatini's initiatives include public-private collaborations for ICT infrastructure development. Resource constraints and limited public awareness hinder progress (Nchake and Shuaibu 2022). Through various programmes, such as encouraging public-private partnerships targeted at improving ICT infrastructure, Eswatini has made

significant progress in developing its ICT sector. These partnerships have made it easier to roll out digital tools and increase internet access to boost economic growth and enhance service delivery in industries including agriculture, healthcare and education. Methods to address these issues include initiatives to raise funds to close resource shortages, efforts to advance ICT literacy, and capacity-building programmes to improve digital skills. Eswatini hopes to establish itself as a competitive participant in the global ICT scene and to foster a more inclusive digital economy by concentrating on these areas.

Lessons learned from successes and failures

Invest in leadership and institutions: Nations with specialised institutions, like Singapore's CSA or the UK's NCSC, are better equipped than others to handle cyber threats. Co-ordination and consistent focus among stakeholders are guaranteed by institutional leadership.

Adjust frameworks to local contexts: Although EU models such as the GDPR offer helpful standards, frameworks must be modified to consider regional legal, cultural and economic circumstances.

Fill the capacity gaps: Countries with limited resources frequently find it difficult to implement thorough cybersecurity safeguards. These gaps can be closed through focused collaboration, technology and educational initiatives.

Encourage regional and global co-operation: No nation can handle cyber threats on its own. Cyber threats are international. Successful examples that highlight the value of co-operation include Singapore's involvement in international forums.

Avoid fragmented approaches: Inconsistent policies and a lack of agency collaboration impede cybersecurity efforts. Better outcomes are obtained through integrated approaches as demonstrated in Singapore and the UK.

Raise public awareness: At local level, resilience is improved by educating people about cybersecurity threats and best practice.

Lack of political will, inadequate finance and an excessive dependence on outside solutions without local capacity building are frequent causes of failure. A long-term vision and consistent dedication are needed to address these problems.

8. Policy recommendations

To improve cybersecurity and privacy governance in the Commonwealth, effective policy suggestions must consider the diverse capacities of member countries while striking a balance between short-term demands and long-term objectives. This section presents customised implementation plans for both the short and long term, with a focus on methods that consider the difficulties faced by high-capacity and low-resource nations.

Short-term strategies

Adopting or revising cybersecurity and privacy laws to improve their legal and regulatory frameworks should be a top priority for member countries. As a starting point, low-resource nations should adopt adaptable baseline norms like the African Union Convention on Cyber Security and Data Protection (Malabo Convention). High-capacity nations ought to concentrate on improving current legislation to consider cutting-edge technology like the Internet of Things (IoT) and AI.

Create national cybersecurity plans. Creating a national cybersecurity plan offers a way of dealing with weaknesses. Plans for safeguarding vital infrastructure, capacity-building programmes and risk assessments should all be part of these.

Boost public awareness campaigns. Educating people about privacy and cyber hygiene is an affordable way of improving resilience on a personal level. Governments should work with the business sector and civic society to produce easily available instructional materials.

Establish regional support networks. To exchange resources and experience, Commonwealth countries should set up regional cybersecurity hubs. Smaller countries with fewer resources can particularly benefit from these hubs' ability to function as training, research and incident response facilities. One important short-term step is to increase incident response capacity by establishing CERTs in each member country. CERTs can facilitate information sharing among stakeholders, offer technical support and organise responses to cyber incidents.

Long-term strategies

Create strong institutional frameworks by fortifying national cybersecurity agencies and establishing independent data protection authorities (DPAs). These organisations ought to have the funding and legal standing necessary to compel adherence to regulations and to direct the creation of new ones.

Invest in education and workforce development. Member countries should place a high priority on developing a workforce with the necessary skills by funding professional training programmes and cybersecurity education. Scholarships, internships and certification can be funded, in part, through public-private partnerships.

Encourage regional and global harmonisation: Bringing cybersecurity and data protection standards into line throughout the Commonwealth will ease cross-border collaboration and lessen regulatory fragmentation. The goal of member countries should be to conform to international agreements like the Budapest Convention on Cybercrime.

Leverage emerging technologies. To improve data security and threat detection, governments should investigate the application of blockchain, AI and machine learning. Blockchain, for instance, can guarantee data integrity, while AI can examine significant volumes of data to detect threats early.

Promote sustainable funding models. Countries with limited resources can receive sustainable funding by creating cybersecurity trust funds or applying for international development assistance. High-capacity nations should provide financial and technical assistance for regional projects.

Tailored approaches for low-resource and high-capacity countries

Low-resource countries ought to concentrate on basic projects that require little funding but have a significant impact. These include focusing public awareness efforts, utilising regional hubs for knowledge and implementing baseline legal frameworks. Local resources can be enhanced through collaboration with private sector groups and foreign organisations.
High-capacity countries might set the standard by showcasing the usefulness of cutting-edge frameworks and technologies. Innovation, cross-border co-operation, and offering technical support to member countries with fewer resources should be their top priorities. High-capacity countries can contribute to strengthening the Commonwealth's overall cybersecurity resilience by serving as mentors.

9. Conclusion

This paper has covered important issues, opportunities and tactics for improving cybersecurity and data protection in the Commonwealth. The diversity of Commonwealth countries presents both opportunities and challenges for developing common cybersecurity standards. Diverse institutional and regulatory frameworks make it difficult to share data across borders and to work together to combat cyber threats. Many member countries face major obstacles due to a lack of resources and a lack of skilled workers, especially in low-income areas. Through the Commonwealth Cyber Declaration and the CTO's operations, for example, the Commonwealth has made progress in promoting collaboration despite these obstacles.

The paper also highlights successful national and regional initiatives including the significance of customised strategies that adhere to international standards while respecting local situations.

Reflections on fostering a safer and more secure digital environment

Three fundamental tenets – inclusion, innovation and international co-operation – are essential for a secure digital environment in the Commonwealth. Regardless of ability, inclusivity guarantees that all member countries have the resources and assistance required to safeguard their digital ecosystems. The creation of innovative solutions to counteract ever-changing cyber threats is fuelled by innovation. International co-operation makes it possible to pool resources, share knowledge and take co-ordinated action to address shared problems.

Strong public-private partnerships, ongoing governmental commitment, and the active participation of civil society are all necessary to achieve these objectives. Policymakers need to understand that data protection and cybersecurity are not merely technical problems. Rather, they are essential to social progress, economic growth and national security.

Call to action for policymakers, institutions and international bodies

Policymakers should make cybersecurity and data protection a top priority on national agendas and provide enough money and legislative backing. They should participate in multilateral discussions to align national policies with regional and international norms.

Institutions should enforce the law, control hazards, co-ordinate actions, strengthen institutions and establish new ones as needed. They should invest in research and development to keep ahead of new dangers.

International organisations should increase capacity-building programmes aimed at low-resource nations while guaranteeing fair access to financial support and technical assistance. They should encourage the exchange of case studies and best practice to foster innovation and knowledge transfer.

10. References

African Union (2014), African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), available at: https://au.int

Arora, R and Luthra, S (2021), 'Challenges in cybersecurity policy implementation: A Commonwealth perspective', *Journal of Cyber Policy*, 6(2), 123-145.

Bada, M and Nurse, JRC (2019), 'Cybersecurity education and awareness: A systematic review of research and trends', *Computers & Security, 88*, 101613, available at: https://doi.org/10.1016/j.cose.2019.101613

Clarke, R (2019), 'Understanding the complexities of data protection in the digital age', *Information Security Journal*, 28(3), 190-202.

Commonwealth Secretariat (2018a), 'Enhancing cybersecurity in the Commonwealth: Key strategies and initiatives', *Commonwealth Reports*, 45, 89-104.

Commonwealth Secretariat (2018b), *The Commonwealth Cyber Declaration*, available at: https://thecommonwealth.org

Commonwealth Secretariat (2018c), *Cybersecurity and the Commonwealth: Advancing National and Regional Approaches to Cybersecurity Policy*.

Commonwealth Telecommunications Organisation (2019), *The State of Digital Transformation in Commonwealth Countries*.

Cyber Security Agency of Singapore (CSA) (2021), Singapore Cybersecurity Strategy 2021, available at: https://www.csa.gov.sg

Daly, A (2020), *Privacy, Data Protection, and Cybersecurity in the Commonwealth*. Cambridge University Press.

DataGuidance (2020), *Kenya's Data Protection Act: An Overview*, available at: www.dataguidance.com

Ee, SKE (2024), US-Singapore cooperation on tech and security: Defense, cyber, and biotech, *arXiv preprint arXiv:2408.07946*.

European Union (2016), 'General Data Protection Regulation (GDPR)', *Official Journal of the European Union, L119, 1–88*, available at: https://eur-lex.europa.eu

Greenleaf, G (2021), *Global data privacy laws 2021: 145 national laws and many bills*, Privacy Laws & Business International Report.

Information Commissioner's Office (ICO) (2021), *Guide to the UK General Data Protection Regulation (UK GDPR)*, available at: www.ico.org.uk

International Telecommunication Union (ITU) (2021), *Global Cybersecurity Agenda*. Available at: www.itu.int

International Telecommunication Union (ITU) (2022), *Global Cybersecurity Index*. Available at: www.itu.int

Johnson, D (2017), 'Cybersecurity frameworks in advanced economies: Lessons from Canada and the UK', *Global Cybersecurity Review*, 10(1), 34-50.

Mistry, P (2022), 'Advancing cybersecurity collaboration in the Commonwealth', *Commonwealth Studies Quarterly*, 29(4), 67-81.

Nchake, MA and Shuaibu, M (2022), 'Investment in ICT infrastructure and inclusive growth in Africa', *Scientific African*, 17, 10.1016/j.sciaf.2022.e01293.

Office of the Australian Information Commissioner (OAIC) (2020), *Privacy Act 1988 Overview*, available at: www.oaic.gov.au

Personal Data Protection Commission (PDPC) (2022), *Personal Data Protection in Singapore: Guidelines and Resources*, available at: www.pdpc.gov.sg

Phahlamohlaka, J, Theron, J and Aschmann, MJ (2022), 'National cybersecurity implementation in South Africa: The conundrum question', *Journal of Information Warfare,* 21(1), 1-16.

Radu, R (2021), 'The harmonization of data protection policies across the Commonwealth: A pathway for innovation and governance', *Journal of International Policy, 14*(2), 223-244, available at: https://doi.org/10.1016/j.jip.2021.14.223

Shackelford, S (2012), 'Rethinking cybersecurity: Global perspectives', *American Journal of International Law*, 106(3), 569-607.

Sharma, N (2020), 'Emerging cyber threats and their implications for Commonwealth nations', *Digital Security Quarterly*, 15(3), 45-60.

Smith, J, Taylor, R and Green, H (2020), 'Data breaches and socio-economic impacts', *Cyber Studies Review*, 22(2), 210-229.

Tamanikaiwaimaro, S (2021), *Cybersecurity in the Republic of Fiji*, DiploFoundation, available at: https://www.diplomacy.edu/wp-content/uploads/2021/06/IGCBP2010_2011_Tamanikalwalmaro.pdf

United Kingdom Government (2018), Data Protection Act 2018, available at https://www.legislation.gov.uk/ukpga/2018/12/contents

United Nations Conference on Trade and Development (UNCTAD) (2021), *Data Protection Regulations and International Data Flows: Implications for Trade and Development*. United Nations.

Weber, M (2020), 'Collaborative approaches to data protection in international organizations', *International Journal of Cyber Studies*, 18(1), 75-92.

World Economic Forum (2020), *Cybersecurity and the Digital Economy: Lessons from Leading Nations*, *The Global Risks Report 2020*, available at: https://www.weforum.org

About the authors

Otshepeng Mazibuko PhD (c) is at the University of Pretoria and a researcher assistant on the Public Understanding of Big Data and Genomic Medicine in Africa project at the University of Cape Town. Her interdisciplinary work blends robust theoretical frameworks with practical expertise in research, project management, and policy advocacy, gained through roles such as Research Consultant at the Southern African Trust. Her doctoral research critically examines decentralisation processes in South Africa, aiming to influence governance and reverse systemic inequalities through innovative, impactful solutions.

The Commonwealth

Commonwealth Cyber Journal \ 97
ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cyber-journal

Child Protection in the Digital Age

International Standards and Middle East and North Africa Perspectives on Online Child Sexual Exploitation and Abuse

Mohamed Hemdani[1]

Abstract

Online child sexual exploitation (OCSE) has become a critical focus within the evolving frameworks for international cybercrime legislation. This article examines the current approach of the Budapest Convention and the UN Cybercrime Convention, particularly in their handling of OCSE, and provides a comparative analysis with legal frameworks in the Middle East and North Africa (MENA) region. It explores the complexities of harmonising international standards and addressing regional legal differences, with an emphasis on the gaps and opportunities in combating OCSE through both global and local efforts.

Article 9 of the Budapest Convention and Article 14 of the UN Cybercrime Convention aim to create a comprehensive legal framework for addressing cybercrime, including the transnational nature of OCSE. Specifically, they focus on improving the capacity of states to investigate, prosecute and prevent crimes related to OCSE. In contrast, many MENA countries approach cybercrime, including OCSE, through national-level legislation, often influenced by religious, cultural and socio-political factors. While some countries in the region have developed robust cybercrime laws, others face significant challenges in enforcement and legal consistency.

While efforts have been made to align cybercrime laws in the region with international norms, significant differences remain. Legal frameworks in many MENA countries focus more on content control and cybersecurity, often with a less targeted approach to protecting children from online exploitation.

1 Mohamed Hemdani is an Egyptian judge specialising in cybercrime, digital evidence, data protection and financial crimes. mohgameel2011@gmail.com

A more regionally tailored approach, complemented by stronger international co-operation, is essential to effectively combat OCSE. The comparative analysis reveals both promising advancements and critical areas needing reform, especially as the international community moves toward a more co-ordinated global response to cybercrime in general and OCSE specifically.

1. Introduction

Online child sexual exploitation (OCSE) is a global phenomenon associated with a range of negative outcomes that can be severe and longsuffering for victims (Brown, 2023). There is a lack of data to draw a clear picture of the gravity of the issue in some jurisdictions (Burton et al., 2016), as there is no international mandate requiring countries to maintain a national database identifying the frequency of child sexual abuse incidents (ECPAT and Interpol, 2018). However, it is evident that most countries have taken serious steps towards combating the phenomenon. Legislative and social measures include joining international treaties, enacting domestic laws combating OCSE or promoting the work of organisations that work in the field domestically or by joining international ones.

The societal and cultural dimensions are crucial to understanding and addressing the spread of OCSE. These factors significantly shape the nature of the problem and the response. Additionally, the religious context, particularly in the countries of the Middle East and North Africa (MENA) region, plays a pivotal role in influencing both the prevalence of OCSE and the legislative and social measures taken to combat it.

The harmonisation of legislation plays a pivotal role in combating any crime, especially those committed online. Cybercrime is transnational in nature, which adds a layer of complexity to its investigation and prosecution. Many jurisdictional issues arise, in addition to obstacles to acquiring relevant digital evidence. These result from a lack of criminalisation of some cybercrimes in certain jurisdictions, which creates cybercrime safe havens and hinders the exchange of evidence or the extradition of criminals through the absence of the dual criminality prerequisite.

This article starts by introducing definitions, including OCSE and its difference from online child sexual abuse (OCSA). It then delves into the international legal framework on the issue, including the Convention on the Rights of the Child (CRC), the Convention on Cybercrime (the Budapest Convention) and the UN Cybercrime Convention. It next compares the situation in some MENA countries – namely Egypt, Saudi Arabia and the United Arab Emirates (UAE) – with the UK and looks at how MENA legislation reflects cultural and religious aspects and how the dominant religion in each country shapes the response to OCSE.

2. Definitions

2.1 Child

According to Article 1 of the CRC, a child is defined as 'every human being below the age of eighteen years unless, under the law applicable to the child, majority is attained earlier.' Most legislation around the globe adopts this definition, and the countries in our studies are no different. In Egypt, Article 2 of Law No. 12 of 1996 (the Child Law) provides that, 'A child in the field of care stipulated in this law means anyone who has not exceeded the full eighteen years of age.' In Saudi Arabia, the Law on the Protection of the Child issued by Royal Decree No. 14 of 2014 provides in Article 1 that a child is 'any person under 18 years of age.' In the UAE, meanwhile, Federal Law No. 3 of 2016 on the Child Rights Law (Wadeema) defines a child in Article 1 as 'each and every human being born alive and below 18 years of age.' Note that the law of the UAE sets as a condition that the child is born alive; while this has no effect in the context of this article, it may have implications for the child's rights to inheritance (Al Sayed, 2004)[2]

In the UK, the Children Act of 1989, which makes provision for a number of orders relating to the welfare of children, defines a child as a person under the age of 18.

All the countries mentioned are signatories to the CRC, which gives us a clear view of the important role that international law plays in the harmonisation of legal standards.

2.2 Online child sexual exploitation vs online child sexual abuse

According to the World Health Organization (WHO, 1999: 15–16), child sexual abuse is:

> ... the involvement of a child in sexual activity that he or she does not fully comprehend, is unable to give informed consent to, or for which the child is not developmentally prepared and cannot give consent, or that violates the laws or social taboos of society. Child sexual abuse is evidenced by this activity between a child and an adult or another child who by age or development is in a relationship of responsibility, trust or power, the activity being intended to gratify or satisfy the needs of the other person. This may include, but is not limited to, the inducement or coercion of a child to engage in any unlawful sexual activity; the exploitative use of a child in prostitution or other unlawful sexual practices; the exploitative use of children in pornographic performance and materials.

The differentiation is clearer in the definitions adopted by the UN Refugee Agency (UNHCR, nd). UNHRC defines child sexual abuse as follows:

> ... the actual or threatened physical intrusion of a sexual nature, whether by force or under unequal or coercive conditions. Any sexual activity with children (persons under the age of 18 years) constitutes sexual abuse.

2 Alsayed Sabeq Al Banna, 2004 Fiqh Al Sunnah, Dar Al Hadeeth, Cairo: page 1115

It defines child sexual exploitation as:

> ... any actual or attempted abuse of a position of vulnerability, differential power, or trust, for sexual purposes, including, but not limited to, profiting monetarily, socially, or politically from the sexual exploitation of another. It includes but is not limited to exchanging money, employment, goods or services for sex. This includes transactional sex regardless of the legal status of sex work in the country. It also includes any situation where sex is coerced or demanded by withholding or threatening to withhold goods or services or by blackmailing.

Meanwhile, the Lanzarote Convention (criminalising sexual offences against children) mentions child sexual exploitation and child sexual abuse without actual differentiation. Article 3b provides that '"sexual exploitation and sexual abuse of children" shall include the behavior as referred to in Articles 18 to 23 of this Convention,' but these articles do not differentiate explicitly between exploitation and abuse. Article 18 (titled 'Sexual abuse') criminalises certain sexually related acts when committed on a child but, overall, a clear distinction is not evident. The convention lists offences such as child pornography, child prostitution, solicitation of a child for sexual purposes and the corruption of children, while utilising the terms 'abuse' and 'exploitation' throughout.

Article 34 of the CRC defines child sexual exploitation and abuse by describing certain acts that form such an offence, such as the inducement or coercion of a child to engage in any unlawful sexual activity, the exploitative use of children in prostitution or other unlawful sexual practices and the exploitative use of children in pornographic performances and materials.

3. International legal context of online child sexual exploitation and abuse

The online form of child sexual exploitation and abuse is often focused on the display of such exploitation or abuse, rather than on the actual offline act of exploitation, except in the case of solicitation and grooming of children online. This explains the use of the term 'material' in international texts dealing with OCSEA.

However, some modalities of the crime, such as sextortion and the online incitement of violent or coerced sexual acts (where the perpetrator goes online and orders certain sexual acts to be performed on a minor in real time), are not explicitly mentioned in cybercrime-focused international texts.

Online solicitation or grooming of children to sexual acts, despite involving an action by the online perpetrator, whereby the material element of the crime is committed online by inciting the victim to perform sexual acts, is mentioned in Article 15 of the UN Cybercrime Convention.

Since our focus in this paper is the online form of CSEA, we mention here the two most comprehensive international texts dealing with the matter.

3.1 The Budapest Convention

The Budapest Convention of 2001 does not mention OCSEA; rather, in Article 9, it lists conduct relevant to child pornography that should be criminalised, such as producing, offering, distributing and possessing child pornography. Child pornography is defined in the same article as 'material that visually depicts:

(a) a minor engaged in sexually explicit conduct;

(b) a person appearing to be a minor engaged in sexually explicit conduct;

(c) realistic images representing a minor engaged in sexually explicit conduct.'

3.2 The UN Cybercrime Convention

The UN Convention against Cybercrime defines OCSEA using a list of descriptions for abuse materials or exploitation materials. Article 14–2, provides that:

'The term "child sexual abuse or child sexual exploitation material" shall include visual material, and may include written or audio content, that depicts, describes or represents any person under 18 years of age:

(a) Engaging in real or simulated sexual activity;

(b) In the presence of a person engaging in any sexual activity;

(c) Whose sexual parts are displayed for primarily sexual purposes; or

(d) Subjected to torture or cruel, inhumane or degrading treatment or punishment and such material is sexual in nature.'

Article 14-1 contains a list of behaviour that should be criminalised in relation to CSA or CSE, such as producing, offering, selling, distributing, transmitting, broadcasting, displaying or publishing CSA or CSE through information and communication systems, and soliciting, procuring or accessing, possessing or controlling CSA or CSE material stored in an information and communication system.

Article 15 criminalises grooming or solicitation of a child into committing a sexual offence as defined in domestic law, including those listed in Article 14.

In conclusion, both terms, CSE and CSA, are employed in the international context as mutually complementary. The distinction will be purely legal in nature and will subsequently be reflected in descriptions of specific conduct, primarily in the domestic

context, to determine the appropriate penalty. Therefore, when adopting the UNHCR distinction, the criminalisation of the conduct will be of paramount importance, rather than the broader umbrella term under which such conduct is described.

For the purposes of this article, we use the umbrella term CSEA for reference to the genre of crime, with details according to each researched jurisdiction.

It is important to remember that, although OCSEA is a crime that is largely committed by the display of a certain conduct online, an actual crime is being committed in the offline world in order for the OCSEA to be committed.

Our research will show how jurisdictions deal with CSEA to reach the criminalisation of OCSEA, focusing on crime modalities covered in the Budapest and the UN conventions.

4. The religious aspect of CSEA in the MENA region

Religion in the MENA region, predominantly Islam, plays a pivotal role in shaping legislation, starting with the constitutions in most of the MENA countries, which draw on Islam as their main source (Ali, 2024).

Sharia law, or simply sharia, is the collection of rules set out in the Quran and the Sunnah (the Prophet Mohamed's sayings and doings), along with the opinions and research of Islam scholars.

Thus, *sharia*, *shar'*, *din* (religion) and *millah* (creed) carry one essential meaning: the divine rulings prescribed by Allah for His servants. However, these rulings are referred to as *sharia* in consideration of their establishment, clarity and precision; as *din* with respect to submission to them and obedience to Allah through them; and as *millah* in view of their being enjoined upon the people (Zaidan, 2005).

Allah, the Exalted, says:

> *Then we set you upon a clear path of the matter [i.e., Sharia], so follow it, and do not follow the desires of those who do not know.* (Surat Al Gathieya, 18).

Here, we point to the main provisions relevant to child protection in Islamic sharia, to shed light on the impact of such provisions on the domestic legislation of the studied jurisdictions.

Generally, Islamic sharia prohibits all forms of violation, physical and especially sexual. Violation is a term that implies the loss of the sanctity of something. Clearly, this is a crime that must be condemned; violators deserve to be punished. Islamic sharia forbids any attack on the human body; this is a general prohibition that includes attack by smacking or other forms of corporal harm, or sexual assault. The Prophet, Peace Be Upon Him, said (in Al Azhar University, 2005):

> *The whole of the Muslim is forbidden to another Muslim; his blood, his property and his honour.*

Preservation of honour is one of the objectives of Islamic sharia.

> *Indeed, those who like that immorality should be spread [or publicised] among those who have believed will have a painful punishment in this world and the Hereafter. And Allah knows, while you do not know.* (Surah An-Nur, 24: 19).

The Prophet, Peace Be Upon Him, prohibited the violation of others' honour (chastity) in his farewell sermon, saying:

> *Indeed, your blood, your properties, and your honour are sacred to one another like the sanctity of this day of yours, in this month of yours, in this town of yours*.

Islamic sharia has closed all avenues leading to the harassment of women. Allah has prohibited adultery, sodomy and slander, and has also forbidden the means leading to these acts. Thus, it prohibits unnecessary mixing, seclusion and immodesty, and commands the preservation of chastity, modesty, lowering the gaze and covering private parts. It encourages marriage and prescribes fasting for those who cannot control their desires. Furthermore, it imposes severe punishments to protect honour, aiming to build a pure and chaste Islamic society (Khaled, 2021).

Thus, Islamic sharia prohibits all sorts of harm to human beings, men, women or children, and also provides for the protection of chastity.

Since Islamic sharia is a main source for most of the legislation in the MENA region, societal expectations regarding the protection of children from online sexual abuse are shaped by a combination of cultural and religious values, legal frameworks and international commitments. Communities anticipate robust measures to safeguard children, reflecting a collective responsibility towards their well-being.

Furthermore, the UN Children's Fund (UNICEF) has been actively involved in addressing OCSEA in the MENA region. Its initiatives focus on strengthening child protection systems, promoting awareness and fostering collaboration among stakeholders. For instance, UNICEF supports co-ordinated national responses to protect children from sexual abuse and exploitation online, ensuring cases are investigated and prosecuted effectively (UNICEF, nd).

5. Comparing legislative frameworks of MENA countries and the UK

5.1 Egypt

5.1.1 Legislative framework for OCSEA

Egypt has ensured the protection of children from all sorts of abuse or maltreatment on several levels.

Constitution

Article 80 of the Constitution of 2014 (last amended in 2019) covers the safeguarding and protection of the child from all forms of violence, abuse, mistreatment, and sexual and commercial exploitation.

Penal Code

Article 178 of the Penal Code punishes anyone who publishes, produces, possesses, trades, distributes, rents, pastes, displays or sells obscene objects or pictures with imprisonment for two years or a fine of between EGP 5,000 and EGP 10,000.

Article 267 punishes whoever rapes a woman with execution or life imprisonment; such punishment is aggravated to only execution if the victim was under 18 years of age.

Article 268 provides that anyone who commits an indecent assault on a person by force or threat, or attempts to do so, shall be punished with hard labour imprisonment. If the age of the victim at the time of the offence was under 18, the punishment shall be not less than seven years.

Article 269 provides that whoever commits an indecent assault on a boy or girl under the age of 18 without force or threat shall be punished with imprisonment. If the victim is under 12 full calendar years, the punishment shall be hard labour imprisonment for not less than seven years.

In defining what constitutes indecent assault, the Egyptian Court of Cassation held that the offence of indecent assault is established when the perpetrator is aware that the physical acts committed violate the victim's decency.[3]

In a subsequent ruling, the court clarified that physical contact was not a prerequisite for establishing an offence. The mere exposing of the victim's private body part is sufficient to constitute an indecent assault.[4]

3 Cassation Case No. 80 of Judicial Year 22, hearing of 8 April 1952.
4 Cassation Case No. 1664 of Judicial Year 28, hearing of 12 January 1959.

Article 327, on the other hand, criminalises all sorts of extortion, including sextortion, whatever the means used in committing the crime. The article provides that anyone who threatens another in writing to commit a severe crime against this person or his or her property, or by disclosing matters or attributing matters that damage honour, where the threat is accompanied by a demand or the imposition of an order, shall be punished with imprisonment.

Confinement shall be imposed if the threat is not accompanied by a demand or the imposition of an order.

Similar verbal threats are also punishable by confinement whether direct or indirect.

Anti-Prostitution Law No. 10 of 1961

This comprehensive piece of legislation encompasses the criminalisation of various forms of prostitution involving women, and same-sex sexual acts regardless of sex. It also penalises individuals under the age of 21 who engage in such activities or provide support, including places or funding for these criminal endeavours.

The legislation also encompasses penalties for assisting individuals in leaving the country to commit such crimes abroad or facilitating their entry into the country for the same purpose.

Child Law No. 12 of 1996

This comprehensive legal framework governs all aspects of childcare, health, safety and education, encompassing the definition of a child as an individual under the age of 18, as per Article 2.

Article 116 provides that adults who induce children to commit misdemeanours face imprisonment not more than half of the minimum penalty of such crime, with increased penalties for coercion, threats or familial relationships. Felony-inducing adults face penalties similar to if they instigated such crimes.

Human Trafficking Law No. 46 of 2010

Article 2 provides that a person is considered guilty of human trafficking if they deal with a natural person (e.g., through selling, purchasing, employing, transporting or harbouring) using means such as force, threats, deception or exploitation of vulnerability, with the intent of exploitation. This includes **sexual exploitation of children**, whether through prostitution, pornography or any other form of abuse. The crime also encompasses actions aimed at exploiting children for sexual purposes under coercive or manipulative circumstances.

Cybercrime Law No. 175 of 2018

The law deals with both cyber-dependent crimes and many cyber-enabled ones, in addition to having very important provisions dealing with special investigatory powers in examining cybercrime cases and the rules of admissibility of digital evidence.

Article 25 punishes anyone who violates family values, invades privacy, sends unsolicited electronic messages, shares personal data for promotion without consent or publishes privacy-infringing content online – whether true or false – with imprisonment of at least six months, a fine of EGP 50,000 to EGP 100,000, or both penalties.

One of the most important articles of this law is Article 27, which provides that creating, managing or using a website or account to facilitate a crime punishable by any law results in at least two years' imprisonment, a fine of EGP 100,000 to EGP 300,000, or both.

This means that any crime, explicitly provided for in the Cybercrime Law or in any other law, falls under the Cybercrime Law whenever the means to its commission is a website or an account. The importance of this general article is that is enables investigators of such crimes to use the relatively wide powers granted by the Cybercrime Law in collecting digital evidence.

5.1.2 Egypt's membership in relevant international conventions

While Egypt is not party to the Budapest Convention, it was one of the earliest countries to ratify the CRC, in February 1990, and its Optional Protocol on the Sale of Children, Child Pornography and Prostitution, in 2007. Egypt ratified the Arab Convention on combating information technology crimes in 2010; this came into force in 2014 after it was ratified by seven member countries of the Arab League.[5] The Arab Convention has the purpose of strengthening co-operation between states within the League of Arab States to enable them to defend against and protect the states' property, people and interests from cybercrime.[6] As for the UN Cybercrime Convention, Egypt participated in the sessions for the draft, with some reservations on Articles 6,14, 24 and 40, mainly regarding human rights provisions and provisions on CSEA.

5 http://www.lasportal.org/ar/legalnetwork/Documents/اتفاقية%20عربية%20لمكافحة%20جرائم%20تقنية%20المعلومات.pdf

6 UNODC, 2022, Overview of existing instruments, recommendations and other documents on countering the use of information and communications technologies for criminal purposes. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/CRP10.pdf

Egypt's reservations on CSEA provisions reflect many cultural and religious aspects, such as the absence in some countries of a minimum age for consensual sex in favour of a minimum age for marriage and the prohibition of dissemination of images of an intimate nature, leading to a need to prioritise domestic law (Delegation of Egypt, 2024).[7]

5.1.3 Gap analysis of the Egyptian OCSEA legislative framework

Despite the lack of a specific definition of OCSEA in the Egyptian legislative framework, a comprehensive analysis of the laws and their judicial applications reveals the extent to which these provisions are designed to combat OCSEA, in line with the relevant international texts.

It is evident that such modalities are covered by both the Penal Code and the Cybercrime Law.

In deciding whether the Egyptian legislative framework is sufficient to address the problem, we examine types of OCSEA and see whether they are covered by the national legislation. In doing so, we adopt the approach taken by the Budapest Convention and the UN Cybercrime Convention in enumerating OCSEA modalities.

Furthermore, we touch on the effectiveness of the Egyptian system on the exchange of relevant digital evidence from third countries.

Child pornography

Article 9 of the Budapest Convention and Article 14 of the UN Cybercrime Convention deal with CSEA materials, Budapest through criminalising child pornography using the above-mentioned definition and associated criminal conduct, and the UN convention through the definition in Article 14-2 of what constitutes CSEA material and the criminal conduct in Article 14-1.

For this specific crime, the Egyptian Penal Code Article 178 covers all criminal conduct related to pornography. Furthermore, Articles 267, 268 and 269 criminalise all sexual conduct that could be the subject of such photos, which builds a comprehensive criminalisation system for all pornography-related conduct.

Coupled with the Anti-Prostitution Law and Articles 25 and 27 of the Cybercrime Law, all conduct related to child pornography as defined in Budapest and the UN convention are covered by Egyptian law covering offline and online relevant conduct.

7 Statement of the Delegation of Egypt, 2024, Concluding Session of the Ad-Hoc Committee on the Elaboration of a Draft Convention on the Use of Information and Communication Technologies for Criminal Purposes https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/MEMBER_STATES/Closing_Statement_final.pdf

Solicitation and grooming

The approach adopted by Article 15 of the UN convention makes communicating, soliciting, grooming or making any arrangement through an information and communication technology system for the purpose of committing a sexual offence against a child a criminalised act. Thus, the mere act, even if it does not result in an actual sexual offence committed by the child, is considered a crime meeting all the essential elements. Paragraph 2 of this article gives countries the possibility to require an act in furtherance of the conduct described in paragraph 1 of the article, which would be the actual occurrence of the sexual offence.

Article 116 of the Egyptian Child Law covers any sort of incitement of a child to commit any crime, with a gradual penalty escalation depending on the gravity of the offence incited. Article 2 of the Human Trafficking Law is applied in cases of solicitation and grooming of children as well. The courts have deemed the act of luring minors for money to perform sexual acts, exploiting their need for money or by coercion, to meet the definition of human trafficking as defined by Article 2;[8] furthermore, Article 3 of the law provides that consent has no effect in the fulfilment of the constitutive elements of the offence if the victim is a child, which makes all sorts of sexual abuse of children, whatever the means, punishable by the law.

Communicating with a child for the purpose of committing a sexual offence is, however, not provided for explicitly as a criminalised act. This may lead to judicial issues in applying the existing provisions for this specific form of criminal act.

Other forms of OCSEA

Budapest and the UN convention deal specifically with child pornography, online grooming and similar derivatives of OCSEA. Some other forms of the crime qualify as OCSEA yet are not specifically provided for in the conventions.

Online sextortion, for instance, despite not being provided for explicitly and individually as a crime, is being prosecuted by Egyptian courts using the existing provisions in the Penal Code and the Cybercrime Law.[9]

Another form of the crime is the coercion of a child to perform certain sexual acts at the demand of other person in real time. This is also covered by the provisions of the Penal Code and the Cybercrime Law, which impose adequate punishments through the penalisation of any form of sexual abuse of a child.

8 Court of Cassation ruling no. 12737 of the judicial year 91, hearing date 11-2-2023

9 Court of Cassation Case No. 19281 of Judicial Year 89, hearing on 19 September 2020. The court held that the Economic Court of Appeal had correctly applied the law in assuming jurisdiction over a case of a suspect coercing a female victim to send nude pictures of herself under threat of divulging pictures he had of her. The prosecution presented the case with a list of indictments using Article 327 of the Penal Code along with Article 27 of the Cybercrime Law.

Funding any of the criminal acts provided for in the conventions remains unregulated, with no specific legal provision punishing such a crime; however, general rules of aiding to commit a crime could apply in this regard. Article 43 of the Egyptian Penal Code punishes whoever aids the main perpetrator of a crime with the same punishment designated for committing such a crime.

Most OCSEA criminal modalities are fully covered by Egyptian law, even though specific crimes may not have the exact definition adopted by the international texts.

5.2 Saudi Arabia

5.2.1 Legislative framework for OCSEA

The legislative framework for protection from OCSEA in Saudi Arabia involves the Child Protection Law, the Anti-Trafficking law and the Cybercrime Law. We look at these laws in some detail for specific provisions applicable to OCSEA.

Child Protection Law of 2014

Article 1 on definitions defines sexual abuse as exposing a child to any type of sexual assault, harm or exploitation, Along with Articles 2 and 9, it asserts that sexually harassing a child or exposing him or her to sexual exploitation is a form of abuse.

Article 23(bis) provides for a penalty of imprisonment for a term not exceeding two years and a fine not exceeding 100,000 riyals, or by one of these penalties in case of committing any sort of abuse, to be doubled in case of recidivism.

Anti-Trafficking Law 2009

Article 2 provides that trafficking in persons is prohibited, including coercion, threats, fraud, deceit, abduction, abuse of position or power, taking advantage of vulnerability, paying or receiving benefits to control another person for sexual assault, forced labour, services, mendicancy, slavery or slavery-like practices, servitude, organ removal or medical experiments.

Article 4 aggravates the punishment provided for in Article 3 – which is imprisonment for a period not exceeding 15 years or a fine not exceeding 1,000,000 riyals, or both penalties – in case the victim is a child, without stating exactly how such aggravation would take place.

Cybercrime Law of 2007

Article 6 punishes the preparation, publication or promotion of material for pornographic networks or gambling activities, which violate public morals, with imprisonment for a period not exceeding five years and a fine not exceeding 3,000,000 riyals, or either penalty.

5.2.2 Saudi Arabia's membership in relevant international conventions

Saudi Arabia ratified the CRC in 1996, and actively took place in the discussions for the UN Cybercrime Convention, without depositing certain comments in the final session.[10]

Further, Saudi Arabia signed the Arab Convention in 2010;[11], however, it has not ratified the Convention as of the time of writing of this article.

5.2.3 Gap analysis of the Saudi OCSEA legislative framework

It is important to note, before delving into the crime modalities and how the law handles them, that Saudi Arabia has no unified penal code as of the time of writing. The judge relies on two main sources for punishments: Islamic sharia, whenever there are clear boundaries for a specific punishment for specific criminal conduct, or their own discretion in deciding the suitable punishment for a certain illegal act (Essa, 2024).

This could explain provisions such as Article 4 of the Anti-Trafficking Law, which does not outline a threshold for the aggravation of the punishment in case the crime is committed on a child.

Child pornography

Saudi law seems to tackle the issue of indecent photos in general, only through the Cybercrime Law. This means that, before 2007, Saudi Arabia did not have a specific provision for such crimes. When looking at punishment in the Cybercrime Law, we note that Article 6 makes no differentiation in case the victim is a child.

Furthermore, the wording of the article itself is not indicative of its applicability to the production of pornographic material; rather, it relates to the production of material pertaining to pornographic networks, which does not cover all modalities of child pornography provided for in Budapest and the UN convention.

For instance, it does not tackle the offering, selling, distributing, transmitting, broadcasting, displaying, publishing or otherwise making available of the pornographic material, which we consider a gap in the legislative framework that requires a legislative amendment.

Solicitation and grooming

For this type of crime, the Child Protection Law and the Anti-Trafficking Law provisions are most useful. However, some of the modalities involved in this crime, such as 'communicating,' are not covered. The wording used in the Anti-Trafficking Law includes 'coercion, threat, fraud, deceit' and that in the Child Protection Law includes 'abuse,' which

10 https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_reconvened_concluding_session/main accessed 1/12/2025

11 http://www.lasportal.org/ar/legalnetwork/Documents/%20%D8%A7%D8%AA%D9%81%D8%A7%D9%82%D9%8A%D8%A9%20%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A%D8%A9%20%D9%84%D9%85%D9%83%D8%A7%D9%81%D8%AD%D8%A9%20%D8%AC%D8%B1%D8%A7%D8%A6%D9%85%20%D8%AA%D9%82%D9%86%D9%8A%D8%A9%20%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA.pdf

excludes the act of the mere communication with a child for the purposes of committing a sexual offence. This narrow wording may lead to judicial issues in the application of the law to this specific way of committing the crime.

Furthermore, the acts mentioned in the Saudi law do not include the act of solicitation for money. In Arabic, 'fraud' and 'deceit' do not cover the act of convincing a child to commit or be the victim of a sexual offence, unlike the term 'incitement' used in the Egyptian Child Law for instance, which allows for wider application given its comprehensive linguistic meaning.

5.3 The United Arab Emirates

5.3.1 Legislative framework for OCSEA

Three relevant laws are found within the legislative framework of the UAE for combating OCSEA.

Federal Penal Code (Federal Law No. 3 of 1987, as amended)

While the Penal Code focuses primarily on offline crimes, it contains provisions relevant to protecting children from abuse and exploitation in general, and sexual abuse specifically.

Article 413 criminalises acts of harassment, including sexual harassment of minors, and imposes severe penalties for such offences.

Articles 414–443 cover indecent acts, including those involving minors, and impose penalties for solicitation or attempts to involve a child in sexual activities such as prostitution and debauchery.

Federal Law No. 3 of 2016 on Child Rights

This law ensures the protection of children from all forms of exploitation and abuse. Specifically, Articles 29 and 37 prohibit the exploitation, production, filming, possession and circulation of child pornographic materials. The law mandates immediate removal of such content from the internet; it also outlines penalties for violations, in Article 65, by imprisonment of not less than 10 years.

Federal Decree-Law No. 34 of 2021 on Countering Rumours and Cybercrimes

This law addresses cybercrimes, including those involving child pornography. It defines child pornography as any material depicting a child in a dishonourable situation in a sexual act or show, whether real, fictional or simulated. Articles 33–36 provide for imprisonment of at least six months or a fine ranging from AED 150,000 to AED 1,000,000 for criminal conducts including using children in prostitution, production of pornographic material and incitement of immoral acts, with Articles 35 and 36 specifically drafted to tackle criminal conduct where children are being victims.

5.3.2 UAE's membership in relevant international conventions

The UAE is party to the CRC and the Option Protocol. In addition, it has ratified the Arab Convention.

5.3.3 Gap analysis of the UAE OCSEA legislative framework

The UAE legal framework is closer to that of Egypt, in terms of the variety of offences and the existence of a proper penal code that covers the gaps existing in specialised laws such as the cybercrime law and the child protection law.

In determining specific legal characterisation of specific conducts, we use the categorisation adopted by Budapest and the UN convention as follows.

Child pornography

The child rights and cybercrime laws of the UAE draw a solid framework for combating child pornography with stringent punishments, especially the former.

The collective articles dealing with the matter encompass most of the criminal conduct related to child pornography as provided for in Budapest and the UN convention.

Funding any of the criminal acts provided for in the conventions remains unregulated, with no specific legal provision punishing such crime; however, general rules on aiding to commit a crime could apply in this regard. Article 48 of the Penal Code punishes whoever aids the main perpetrator of a crime with the same punishment as designated for such a crime.

Solicitation and grooming

'Incitement for immoral acts' as covered in Article 33 of the cybercrime act could encompass the criminal conduct provided for in Article 15 of the UN Cybercrime Convention.

The law does not explicitly provide for communicating with a child for the purpose of committing a sexual offence as a criminalised act. This may lead to judicial issues in applying the existing provisions to such a form of criminal act.

5.4 Legislative framework for OCSEA in the United Kingdom

The UK has developed an extensive legislative framework to combat OCSEA, combining both preventative and punitive measures. Furthermore, the UK has been a member of many international conventions dealing with child sexual abuse, facilitating international co-operation in the matter.

Protection of Children Act 1989

The law includes 'sexual abuse' in the definition of 'ill-treatment' of a child, meaning all offences provided for ill-treatment include sexual abuse.

In addition, it contains sections tackling caring for the child in a position of abuse, such as Sections 17, 47 and 31.

Sexual Offences Act 2003

This act provides a comprehensive range of offences concerning online child exploitation.

Sections 5–27 contain very specific and detailed criminal conducts that cover every possible sexual assault conduct that could be committed against a child or in his/her presence.

Serious Crime Act 2015

This act, amending also the Sexual Offences Act in Article 68, addresses in a whole part the sexual exploitation of a child.

Section 69 tackles the possession of a paedophile manual, covering all paths for the spreading of knowledge that leads to child sexual abuse by criminalising the possession of any item that contains advice or guidance about abusing children sexually.

Online Safety Bill 2023

The Online Safety Act 2023 is a new set of laws that protects children and adults online by making social media companies and search services more responsible for their users' safety. It requires providers to implement systems to reduce risks, remove illegal content and protect children from age-inappropriate content. It also ensures transparency about potentially harmful content and gives users more control over what they see (DSIT, nd).

Ofcom, the UK's online regulator, has issued detailed guidance on protecting children online, including methods to make sure children are not exposed to pornography by using age check techniques including photo ID matching, facial age estimation and credit card checks (Ofcom, 2024).

The UK legislative framework for combating OCSEA covers all criminal conduct provided for in Budapest and the UN convention in a comprehensive and detailed manner aligned with the relevant institutional framework, especially through the involvement of internet service providers, as provided for in the Online Safety Bill.

6. Conclusion

Addressing OCSEA necessitates a cohesive integration of international frameworks and regional legal systems, underpinned by an understanding of cultural, legal and societal nuances. International instruments such as the Budapest Convention and the UN Cybercrime Conventions provide comprehensive frameworks that set the standard for combating OCSEA.

Some modalities of the crime, such as sextortion and the online incitement of violent or coerced sexual acts (where the perpetrators go online and order certain sexual acts to be performed on a minor in real time) are not explicitly mentioned in international cybercrime-focused texts, we believe because such types of crime are already fully covered in texts on the offline type of this crime; extortion and violent sexual acts are already criminalised in all jurisdictions, which means the simple act of using information technology for the commission of the crime is subsequently criminalised, as with most cyber-enabled crimes.

The variability in legislative approaches across the MENA region highlights the complexities involved in achieving legal harmonisation. To bridge these gaps, MENA countries should prioritise the alignment of their domestic legal systems with internationally recognised standards, addressing critical deficiencies such as the absence of explicit provisions for solicitation, grooming and financial facilitation of OCSEA-related crimes. At the same time, it is imperative that these efforts incorporate cultural and religious considerations to ensure the effectiveness and contextual relevance of the adopted measures.

A unified international strategy, augmented by region-specific adaptations, is pivotal in enhancing global and regional capacities to combat OCSEA effectively. Strengthened co-operation within the MENA region and with international stakeholders will be instrumental in creating a robust and co-ordinated response to this pervasive issue, ultimately safeguarding vulnerable children and ensuring accountability for perpetrators.

7. Recommendations

The disparities in the frameworks of the MENA countries create a disjointed legislative environment in the region, despite them sharing the same religious and cultural background. This incoherent framework may provide criminal safe havens for perpetrators, who can exploit its inconsistencies to commit crimes from under-criminalising states.

As we noticed from looking at the Egyptian legislative framework, as relatively comprehensive as it is, it still does not address some of the crime modalities provided for in the UN Cybercrime Convention or the Budapest Convention, even though, in our view, punishments are an adequate deterrent for the Egyptian community and according to legal standards.

On the other hand, the Saudi Arabia legal framework lacks clear criminalisation for most of the crime modalities.

States in the MENA region should take serious steps towards enhancing their legislative and operational framework combating OCSEA considering the following:

Legislative harmonisation: MENA countries should align domestic laws with the Budapest Convention and the UN Cybercrime Convention, criminalising all OCSEA modalities, including grooming, sextortion and funding. Explicit provisions for handling digital evidence and criminalising online communication for grooming should be introduced to fill existing gaps guided by the mentioned international texts.

Strengthening institutions: Governments should establish specialised cybercrime units, train law enforcement and judicial officials on digital evidence, and create centralised databases to track OCSEA incidents. This exist on the law enforcement level in Egypt and the UAE but more specialised judges and prosecutors are needed to leverage the process of combating OCSEA. Partnerships with Interpol and other international bodies should enhance operational capacity and co-ordination.

Regional cooperation: Regional frameworks such as the Arab Convention should be strengthened to harmonise laws, streamline mutual legal assistance and enable effective cross-border prosecution of OCSEA offenders.

References

Al Azhar University (2005) *Children in Islam Their Care, Upbringing and Protection*. https://jliflc.com/wp-content/uploads/2021/01/children_in_islam_english.pdf

Ali, M. (2024) 'Constitutional Regulation of the Status of Religion in the State: A Comparative Study'. *Journal of the College of Law and Political Science at Aliraqia University*.

Al Sayed, S. (2004) *Fiqh Al Sunnah*. Cairo: Dar Al Hadeeth.

Brown, R. (2023) *Eliminating Online Child Sexual Abuse Material*. New York: Routledge.

Burton, P., Bulger, M., Davidson, J. et al. (2016) 'Child Online Protection in the MENA Region'. Report for the Centre of Justice and Crime Prevention.

Council of Europe (2001) 'Budapest Convention on Cybercrime'. https://www.coe.int](https://www.coe.int

Delegation of Egypt (2024) 'Statement by H.E. Ambassador Mohamed ElMolla, Head of the Delegation of the Arab Republic of Egypt'. Concluding Session of the Ad-Hoc Committee on the Elaboration of a Draft Convention on the Use of Information and Communication Technologies for Criminal Purposes. www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/MEMBER_STATES/Closing_Statement_final.pdf

DSIT (Department for Science, Innovation & Technology) (nd) 'Online Safety Act Explainer'.

www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer (12 December 2024).

Essa, R.E. (2024) 'Lectures in Penal Law'. King Saud University.

https://faculty.ksu.edu.sa/sites/default/files/shrh_lnzm_ljzyy_1_-_lqnwn_ljnyy_lm.pdf

Interpol and ECPAT (2018) 'Towards a Global Indicator on Unidentified Victims of child Sexual Exploitation Material'. https://ecpat.org/wp-content/uploads/2021/05/TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL-Summary-Report.pdf

Khaled, S. (2021) 'Violation of the Sanctity of Women by Sexual Harassment'. *Sharia and Law Magazine*, Al Azhar University.

Ofcom (2024) 'Consultation: Protecting Children from Harms Online'. Last updated 25 November. https://www.ofcom.org.uk/online-safety/protecting-children/protecting-children-from-harms-online

UN (2024) 'Countering the Use of Information and Communications Technologies for Criminal Purposes'. Report of the 3rd Committee: General Assembly, 79th session. https://documents.un.org/symbol-explorer?s=A/79/460&i=A/79/460_1733767802442

UNHCR (UN Refugee Agency) (nd) 'Defining Sexual Abuse, Exploitation and Harassment'. Geneva: UNHCR. https://www.unhcr.org/what-we-do/how-we-work/tackling-sexual-exploitation-abuse-and-harassment/what-sexual-exploitation (19 November 2024).

UNICEF (nd) 'Protecting Children Online'. https://www.unicef.org/protection/violence-against-children-online?utm_source=chatgpt.com (1 February 2025).

UNODC (UN Office on Drugs and Crime) (2022) 'Overview of Existing Instruments, Recommendations and Other Documents on Countering the Use of Information and Communications Technologies for Criminal Purposes'. A/AC.291/CRP.10, 20 April. www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/CRP10.pdf

UNODC (2024) 'Draft UN Convention against Cybercrime'. Press Release, 9 August.

WHO (World Health Organization) (1999) 'Report of the Consultation on Child Abuse Prevention'. Geneva: WHO.

Zaidan, A.A.K. (2011) *Al-Madkhal li Dirasah al-Shariah al-Islamiyyah.* Beirut: Muassasah al-Risalah.

About the authors

Mohamed Hemdani is a criminal appeal judge with 21 years experience as a judge and a prosecutor in Egypt, specialising in cybercrime and money laundering. He holds an LLM in IT law from the University of East Anglia, UK, and a master's degree in international commercial law from Cairo university and Dauphine, France. He serves as a consultant for the Council of Europe's Cybercrime Program Office (C-PROC), UNODC, and Eurojust providing expertise on international cooperation in criminal matters. He is a lecturer in the National Judicial Training Center and National Prosecution Training Center in Egypt.

The Commonwealth

Commonwealth Cyber Journal \ 119
ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cyber-journal

Cyberstalking and Technology-Facilitated Intimate Partner Violence: A Review of Three African Countries

Chioma Andeh

Abstract

Cyberstalking and technology-facilitated intimate partner violence (TFIPV) have emerged as critical challenges in the digital age, allowing abusers to monitor, exert control over and intimidate victims beyond physical spaces. With the widespread adoption of smartphones, social media and GPS tracking, digital tools are increasingly weaponised in intimate relationships, exacerbating psychological, emotional and physical harm.

This study examines the impact of TFIPV in three countries in Africa – Kenya, Nigeria and South Africa – that have enacted legislative measures to regulate technology companies and address digital abuse. Given the limited scope of relevant legal frameworks across the continent, additional cases are considered to provide a broader comparative perspective. The study explores prevalent cyberstalking tactics, including spyware deployment, unauthorised access to personal data, location tracking and social media harassment. It further analyses the gendered dimensions of these abuses, highlighting the heightened vulnerabilities of marginalised groups, including women with limited literacy, those in rural areas and women with disabilities.

In addition to assessing African legal responses, this study reviews global initiatives to combat cyberstalking and TFIPV, analysing international legal frameworks, policy interventions and corporate accountability measures. By comparing regional and global approaches, the study identifies best practices and enforcement gaps that hinder victim protection and legal redress.

The findings underscore the urgent need for stronger legal frameworks, enhanced digital literacy programmes and increased accountability from technology companies. The study concludes with policy recommendations and technological innovations aimed at mitigating digital abuse, protecting survivors and fostering safer online environments.

1. Introduction

1.1 Background, definitions and theoretical framework

The rapid proliferation of digital technology has redefined human communication and interpersonal relationships, offering both transformative opportunities and unprecedented risks. While digital tools enhance connectivity and democratise access to information, they also create new avenues for harm, particularly in cases of intimate partner violence (IPV). The World Health Organization (WHO, 2021) defines IPV as the infliction of physical, sexual, psychological or emotional harm by a current or former partner. Cyberstalking, a digital extension of traditional stalking, involves persistent online surveillance, harassment and intimidation through platforms such as social media, smartphones and GPS tracking (Reed et al., 2022).

A robust theoretical framework is essential for understanding these phenomena. Feminist technology theory (Wajcman, 2004) examines how digital innovations can both challenge and reinforce gendered power structures, highlighting the paradox in which technology, designed to empower, may also facilitate coercive control. Complementing this perspective, power and control theories (Pence and Paymar, 1993) explore how abusers leverage digital tools to extend coercive control, further restricting victims' autonomy and agency.

1.2 Psychological underpinnings of digital abuse

Psychological theories offer further insights into the motivations behind technology-facilitated IPV (TFIPV) and its effects on victims. Attachment theory (Bowlby, 1969) suggests that individuals with insecure attachment styles may resort to obsessive surveillance and control behaviours as maladaptive mechanisms to maintain relational dominance. Meanwhile, the online disinhibition effect (Suler, 2004) explains how digital anonymity and reduced accountability embolden perpetrators to engage in harassment and stalking – behaviours they might avoid in face-to-face interactions.

These dynamics contribute to learned helplessness (Seligman, 1975), where victims feel trapped because of the pervasive nature of digital abuse. Continuous monitoring, digital manipulation and online threats erode victims' sense of agency, exacerbating psychological trauma and increasing dependency on their abusers.

1.3 Power dynamics in technology-mediated relationships

Technology has restructured power dynamics in intimate relationships, particularly in abusive contexts. Digital tools offer perpetrators multiple avenues for coercive control, extending their influence beyond physical presence. Some of the key strategies include:

- **Surveillance and monitoring**: Perpetrators use spyware, GPS tracking and social media monitoring to track victims' activities, reinforcing dominance and restricting autonomy (Douglas et al., 2019).
- **Digital harassment and social manipulation:** Abusers engage in online shaming, impersonation and misinformation campaigns to isolate victims and undermine their credibility. Doxing, or the public exposure of private information, has become an increasingly common tool to instil fear and compliance (Rege, 2020).
- **Economic control via technology:** Financial abuse in TFIPV includes monitoring mobile banking apps, restricting access to online employment opportunities and weaponizing digital financial services to create financial dependency (Woodlock, 2017).

While technology can be a tool for oppression, it also has the potential to empower IPV survivors. Digital platforms provide avenues for accessing support networks, reporting abuse and seeking legal assistance. However, without proper safeguards, these same platforms can be weaponised against victims, highlighting the dual role of technology in IPV contexts.

1.4 Focus on Africa: relevance and scope

Africa presents a unique and compelling context for examining TFIPV, given the rapid digital transformation occurring alongside systemic socio-economic and legal challenges. While mobile and internet penetration have increased significantly, many African countries lack adequate regulatory frameworks for digital safety and cybercrime enforcement. Weak legal infrastructure, combined with socio-cultural barriers such as stigma, economic dependency and patriarchal dominance, exacerbates the risks IPV survivors face.

Studies indicate that in Nigeria, over 60 per cent of IPV cases involve a digital component, yet fewer than 20 per cent of survivors report abuse, out of fear of social backlash and distrust in legal institutions (Aderibigbe, 2021). Similarly, Kenya has witnessed a sharp rise in cyber-related IPV, particularly among women, as perpetrators exploit social media and location-tracking tools (Mwangi and Otieno, 2021). In South Africa, where the internet penetration rate is among the highest on the continent, digital stalking and online harassment are escalating threats, yet law enforcement mechanisms remain weak and inconsistent (Chigbu et al., 2020a).

2. Methodology and literature review

This section outlines the research design, data collection methods and analysis approach while situating the study within the broader academic discourse on cyberstalking and TFIPV. The research focuses on Kenya, Nigeria and South Africa, where digital technology has transformed intimate relationships, introducing new forms of control, surveillance and coercion in IPV.

2.1 Research design and data collection

Given the complex and evolving nature of TFIPV, a qualitative research design was adopted. This approach is well suited to capturing the socio-legal dimensions and psychosocial effects of digital abuse in intimate relationships. The study employs a systematic scoping review of academic literature, policy reports, legal frameworks and case studies from the selected countries.

Scoping review approach

A systematic review of peer-reviewed journal articles, legal statutes and organisational reports was conducted using JSTOR, SpringerLink, SAGE Journals and Google Scholar. Search parameters were restricted to studies published between 2015 and 2025 to ensure relevance.

The research aimed to:

- Analyse the prevalence, forms and impact of TFIPV in Kenya, Nigeria and South Africa;
- Examine the role of digital technology in facilitating IPV;
- Evaluate the effectiveness of legal responses and institutional mechanisms in addressing TFIPV.

Search strategy and selection criteria

The literature search incorporated thematic keywords such as 'cyberstalking', 'technology-facilitated intimate partner violence', '' 'Kenya', 'Nigeria', 'South Africa' and 'cyber harassment'.

Studies were included if they:

- Focused on cyberstalking or TFIPV in Kenya, Nigeria or South Africa;
- Were empirical research studies, systematic reviews or policy analyses;
- Provided legal, psychological or socio-cultural insights on TFIPV.

Studies were excluded if they lacked empirical or theoretical grounding or were purely opinion-based without substantive evidence.

Data extraction and thematic analysis

A structured data extraction framework was developed to classify sources based on:

- Study objectives and methodologies;
- Findings on prevalence and impact;
- Legal and policy implications.

A thematic analysis was conducted, identifying emerging patterns related to:

- Surveillance and coercive control mechanisms in IPV;
- Legal and institutional gaps in addressing TFIPV;
- Socio-cultural factors influencing digital abuse.

Ethical considerations

Although this study relies on secondary data, ethical integrity was maintained by:

- Ensuring accurate attribution of sources (Douglas et al., 2019; Rege, 2020);
- Documenting selection criteria and methodology for transparency;
- Critically appraising sources to minimise bias.

2.2 Literature review

The literature on cyberstalking as an extension of IPV has expanded significantly in recent years. This section examines key themes in the existing literature, including the role of technology in enabling abuse, legal and policy challenges, and regional responses.

2.2.1 Cyberstalking in the context of intimate partner violence

The widespread use of social media, smartphones and location-tracking tools has reshaped intimate relationships, making cyberstalking a dominant form of coercive control in IPV cases (Douglas et al., 2019; Rege, 2020). Victims often experience persistent surveillance, online harassment and unauthorised access to personal information.

Studies indicate that cultural interpretations of digital control further complicate victim responses. In Nigeria, some victims misinterpret persistent online surveillance as an expression of affection, reinforcing coercive behaviours within intimate relationships

(Aderibigbe, 2021). In South Africa, victims report heightened levels of psychological distress resulting from the continuous presence of abusers in their digital spaces (Nkosi, 2022).

2.2.2 The role of technology in enabling abuse

Digital tools such as social media, spyware and tracking applications have revolutionised how abusers perpetrate IPV. These technologies facilitate a seamless transition of abuse from the offline to the online environment, thereby increasing isolation, fear and dependency among victims (Dragiewicz et al., 2019). In Africa, economic disparities and variations in digital literacy compound these challenges. Rural victims, in particular, may lack the skills to recognise or counteract digital surveillance; urban victims may face overwhelmed support services and insufficient legal protections (Chigbu et al., 2020b).

2.2.3 Country-specific legal frameworks and enforcement challenges

A country-specific analysis of TFIPV prevalence, legal protections and enforcement gaps in Kenya, Nigeria and South Africa provides insights into the effectiveness and limitations of existing laws. While these nations have established cybercrime laws, challenges persist in legal enforcement, digital forensic capacity and victim support mechanisms.

Kenya

Prevalence and manifestations

Kenya has experienced a rise in cyber-related IPV, particularly affecting women and LGBTQ+ individuals. Studies estimate that 30–35 per cent of internet users have been victims of online stalking, digital impersonation or image-based abuse (Kamau and Njoroge, 2021). Perpetrators often exploit social media and location-tracking technologies to harass, threaten or blackmail victims (Mutua, 2019).

Legal framework

Kenya has introduced laws targeting cybercrime, but gaps remain in IPV-specific digital protections:

- The Computer Misuse and Cybercrimes Act (2018) prohibits cyber harassment and unauthorised monitoring but does not address scenarios where victims are coerced into sharing access credentials.
- The Kenya Data Protection Act provides data privacy protections but lacks provisions safeguarding IPV survivors from tech-facilitated surveillance.

Enforcement challenges

Several barriers impede the effectiveness of legal measures:

- **Limited technical capacity:** Law enforcement lacks adequate cyber forensic training, leading to low prosecution rates (Njogu, 2020).
- **Lack of victim-centred protections:** Most laws do not consider power imbalances in intimate relationships, allowing abusers to manipulate legal loopholes (Mutua, 2019).
- **Overburdened legal system:** Kenya's judiciary faces case backlogs, delaying justice for IPV survivors (KICTANet, 2022).

Nigeria

Prevalence and manifestations

Nigeria has witnessed a significant increase in cyberstalking, online harassment and digital surveillance as tools of IPV. Estimates suggest that 30–35 per cent of Nigerian internet users have experienced cyber harassment, GPS tracking or unauthorised digital surveillance (Okafor, 2020; Adebayo and Musa, 2021).

Legal framework

Nigeria has enacted several laws to address cyberstalking and online harassment, yet gaps remain in protecting IPV survivors:

- The Cybercrimes (Prohibition, Prevention, Etc.) Act (2015) criminalises cyberstalking and electronic harassment but does not adequately account for intimate partner contexts, where abusers may have pre-existing access to victims' digital lives.
- The Nigeria Data Protection Regulation 2019 aims to safeguard personal data but lacks explicit provisions addressing coercive control through digital access in IPV settings (Mba et al., 2020).

Enforcement challenges

Despite the legal provisions, several systemic barriers hinder enforcement:

- **Limited digital forensic capacity:** Law enforcement agencies lack expertise in gathering digital evidence, leading to low conviction rates (Adeyemi, 2018).
- **Cultural misconceptions:** Some victims misinterpret digital surveillance as an expression of care, reinforcing coercive control dynamics (Eze and Chukwudi, 2019).
- **Lack of institutional co-ordination:** Poor collaboration between law enforcement, judicial bodies and digital platforms weakens victim protection mechanisms (Hinson et al., 2018).

South Africa

Prevalence and manifestations

South Africa has among the highest rates of both offline and online IPV in Africa. Studies indicate that one-third of South Africans report cyberstalking, non-consensual image distribution or digital harassment (Smith et al., 2019). Digital abuse is particularly prevalent among women in urban areas, where high internet penetration increases exposure to tech-facilitated abuse (Moyo and Nkosi, 2020).

Legal framework

South Africa has a more developed cybercrime legal framework, yet enforcement remains inconsistent:

- The Protection from Harassment Act 2011 recognises cyber harassment as a legal offense but does not explicitly cover TFIPV.
- The Cybercrimes Act (2020) criminalises revenge pornography, cyberstalking and unauthorised access to digital information; however, enforcement is often hampered by lack of technical expertise (Nkosi, 2022).

Enforcement challenges

Despite strong legal provisions, enforcement remains weak owing to structural constraints:

- **Underreporting owing to stigma:** Victims often avoid legal action out of fear of retaliation or social judgement, particularly in patriarchal communities (Department of Home Affairs, 2021).
- **Judicial delays:** Backlogs in cybercrime cases lead to prolonged legal processes, discouraging victims from seeking justice (Watson et al., 2022).
- **Resource constraints:** Insufficient training of law enforcement officials in handling digital evidence collection and lack of adequate cyber forensic training, leading to low prosecution rates (Njogu, 2020).

2.2.4 Broader challenges in legal frameworks

Despite legislative advancements in Kenya, Nigeria and South Africa, several cross-cutting legal challenges undermine the effectiveness of legal protections against TFIPV across African jurisdictions. These challenges include:

- Lack of IPV-specific digital protections: Most cybercrime laws criminalise cyberstalking but fail to account for coercive control within intimate relationships (Nkosi, 2022). Existing laws often treat digital abuse as isolated incidents rather than part of a broader pattern of IPV.

- Weak law enforcement training in digital forensics: Many African law enforcement agencies lack cyber forensic expertise, making it difficult to gather digital evidence and prosecute cases effectively (Aderibigbe, 2021). Without specialised training, officers may dismiss cyberstalking complaints or fail to trace online perpetrators.
- Jurisdictional limitations and cross-border cybercrime: Perpetrators often use social media, virtual private networks or offshore digital platforms to evade law enforcement. Since many African cybercrime laws are restricted to domestic jurisdiction, authorities struggle to hold online abusers accountable when attacks originate from outside national borders (Watson et al., 2022).
- Limited collaboration between governments and technology companies: While global tech firms (e.g., Meta, Google) have introduced reporting tools and privacy features, there is little direct collaboration between African governments and social media companies to proactively curb digital abuse (Mason, 2021). Many victims report that their abuse reports on social media are ignored or inadequately addressed.
- Inconsistent implementation of cybercrime laws: While several African countries have enacted cybercrime legislation, their enforcement is often weak, inconsistent or hindered by judicial delays (Chigbu et al., 2020b). In many cases, victims report that police trivialise digital abuse complaints, advising survivors to simply block the perpetrator instead of launching investigations (Mwangi and Otieno, 2021).
- Cultural barriers and victim stigmatisation: Social norms often discourage victims from reporting digital abuse, especially in rural and patriarchal communities. Victims may be blamed for engaging in online spaces or told that cyberstalking is a private matter rather than a criminal offence (Eze and Chukwudi, 2019).

2.2.5 Comparative insights from Morocco, Rwanda and Uganda

While the primary focus of this study is on Nigeria, South Africa, and Kenya, examining the legal frameworks in Morocco, Rwanda and Uganda provides valuable regional context. Morocco has made strides with a new criminal code targeting cyber blackmail and sexual harassment; however, the application of this to TFIPV remains limited by cultural stigmas and enforcement challenges (Zouiten, 2024). In Rwanda, despite the explicit criminalisation of cyberstalking, the penalties do not always serve as effective deterrents, particularly in cases of IPV where the abuse is intertwined with personal relationships. In Uganda, existing laws such as the Anti-Pornography Act, although intended to curb digital abuse, often criminalise survivors of TFIPV as a result of overlapping provisions and societal prejudices (Nyeko, 2023).

2.3 Synthesis and research implications

The country-specific analysis underscores systemic weaknesses in addressing TFIPV, revealing key gaps in legislation, enforcement and victim support.

- Legal frameworks exist but lack IPV-specific protections. Laws generally criminalise cyberstalking and harassment but fail to recognise the nuanced power dynamics in intimate relationships (Nkosi, 2022).
- Weak enforcement undermines legislative progress. Many cases go unreported or unprosecuted as a result of limited technical training and case backlog issues (Aderibigbe, 2021).
- Cultural and economic factors hinder victim protection. Stigma, financial dependency and digital illiteracy prevent many survivors from seeking help (Chigbu et al., 2020a).

3. Mechanisms of cyberstalking in intimate partner violence

The integration of technology into IPV has significantly altered the ways in which abuse is perpetrated. Cyberstalking enables abusers to exert control, monitor and harass their victims remotely, leveraging digital tools such as social media, GPS tracking, spyware and online threats. These mechanisms disproportionately impact women, particularly those from marginalised communities, whose vulnerabilities are exacerbated by cultural norms, economic dependency and systemic inequities. This section explores the key mechanisms of cyberstalking within IPV and examines how gendered vulnerabilities shape the experiences of victims in African contexts.

3.1 Mechanisms of cyberstalking in intimate partner violence

Cyberstalking within IPV manifests through multiple digital tactics, each reinforcing the abuser's control over the victim.

3.1.1 Social media surveillance

Social media platforms such as Facebook, Instagram and WhatsApp provide abusers with extensive opportunities to monitor victims' activities, interactions and locations.

- **Tactics of surveillance:** Abusers create fake profiles to track victims, impersonate them to manipulate relationships and spread misinformation, or demand access to victims' accounts through coercion.

- **Psychological impact:** Victims engage in self-censorship, restricting online interactions out of fear of retaliation. The constant surveillance erodes privacy and autonomy, reinforcing entrapment. Studies in Kenya indicate that social media surveillance contributes to social isolation and emotional exhaustion among victims (Mwangi and Otieno, 2021).

3.1.2 GPS and location tracking

The widespread availability of GPS-enabled devices has provided abusers with advanced tools to track victims' movements in real-time.

- **Methods:** Abusers use applications such as Find My iPhone or Life360 to secretly track victims. GPS trackers placed on vehicles or personal belongings allow them to monitor movements without consent.
- **Consequences:** Victims report feeling constantly monitored, fearing retaliation if they deviate from expected routines. In South Africa, a case study revealed that a woman's partner had secretly tracked her for months, leading to increased psychological distress and further isolation (Nkosi, 2022).

3.1.3 Spyware and unauthorised access

Spyware applications enable abusers to infiltrate victims' digital devices, gaining unauthorised access to private communications and online activities.

- **Common tools**: Spyware such as FlexiSPY and mSpy allows abusers to monitor text messages, emails and call logs in real time. Many victims unknowingly have such software installed on their devices or are coerced into revealing their passwords.
- **Impact on victims**: The invasive nature of spyware fosters constant fear and helplessness, making it difficult for victims to escape abusive relationships. In Nigeria, spyware use has been identified as a significant barrier for women attempting to seek help or leave abusive partners (Aderibigbe, 2021).

3.1.4 Digital harassment and threats

Cyberstalking often extends beyond monitoring to direct digital harassment, including threats, blackmail and non-consensual sharing of intimate images.

- **Forms of harassment**: Abusers send threats through email or social media, often coercing victims into compliance. Revenge pornography, where abusers share or threaten to share explicit images, is a particularly harmful tactic used to humiliate and control victims.

- **Barriers to protection:** Despite the criminalisation of digital harassment in some African countries, victims face difficulties in proving abuse because of the challenges of collecting evidence. Additionally, many are deterred by societal stigma and fear of retaliation (Chigbu et al., 2020b).

3.2 Gendered vulnerabilities and systemic barriers

Women, particularly those from marginalised communities, face heightened risks of cyberstalking and TFIPV as a result of entrenched structural inequalities, cultural expectations and economic dependency.

3.2.1 Disproportionate impact on women

Research suggests that over 60 per cent of women in IPV situations in Africa have experienced cyberstalking, with social media surveillance and GPS tracking being the most commonly reported methods of abuse. The psychological toll includes heightened anxiety, fear and symptoms of post-traumatic stress disorder (PTSD), as digital monitoring creates an omnipresent sense of surveillance and entrapment (Nkosi, 2022). Societal norms further reinforce victim-blaming attitudes, discouraging women from seeking legal or social recourse (Aderibigbe, 2021).

3.2.2 Unique vulnerabilities of marginalised women

Certain groups of women face compounded risks linked to social, economic and systemic factors:

- **Women with disabilities:** Abusers exploit their reliance on technology for communication and healthcare, using digital tools to isolate and manipulate them. Limited access to legal and social services further exacerbates their vulnerability (Chigbu et al., 2020a).
- **Women from lower socio-economic backgrounds:** Financial dependence makes it difficult for these women to leave abusive relationships. Many lack digital literacy, leaving them unaware of how to protect themselves from spyware or tracking apps. Rural women are particularly at risk as a consequence of restricted access to education and digital resources (Mwangi and Otieno, 2021).
- **Women from marginalised ethnic groups:** Cultural biases and systemic discrimination often prevent these women from reporting abuse. In Nigeria, for example, expectations of familial loyalty deter victims from seeking help, reinforcing cycles of digital and physical IPV (Aderibigbe, 2021).

3.2.3 Cultural and social norms exacerbating risk

- **Cultural silence and victim-blaming:** In many African societies, IPV is normalised, and victims are discouraged from speaking out to preserve family harmony. Fear of retaliation or social backlash often forces women to endure abuse in silence (Nkosi, 2022).
- **Technological literacy and access:** Many women, particularly in rural and underserved communities, lack awareness of digital security tools that could protect them from cyberstalking. Without knowledge of privacy settings, secure passwords or protective applications, victims remain highly vulnerable to invasive technologies (Mwangi and Otieno, 2021).

3.3 Economic and structural barriers to protection

Financial dependency, inadequate legal enforcement and lack of institutional support further entrench victims in digitally abusive relationships.

- **Economic barriers:** Many victims are financially reliant on their abusers, limiting their ability to access secure devices, legal assistance or digital safety training. In Nigeria, economic constraints are a significant factor preventing women from escaping abusive relationships (Aderibigbe, 2021).
- **Weak legal protections and enforcement:** While some African nations have criminalised digital harassment, enforcement remains inconsistent owing to a lack of specialised training among law enforcement personnel. Victims frequently report that authorities dismiss their claims or lack the technical skills to collect digital evidence effectively (Chigbu et al., 2020a).
- **Limited collaboration with technology companies:** Although social media platforms have introduced safety features, their effectiveness in IPV cases is limited. Reporting mechanisms are often slow, and technology firms lack streamlined processes for assisting law enforcement in cyberstalking cases (Mason, 2021).

4. The impact of cyberstalking and law enforcement negligence in addressing TFIPV

The psychological toll of cyberstalking in IPV is profound, often surpassing that of traditional forms of abuse. Unlike physical violence, which leaves visible marks, digital abuse is persistent, invasive and difficult to escape. Cyberstalking intensifies emotional trauma, induces feelings of helplessness and isolates victims in ways that significantly hinder their ability to seek help. Additionally, barriers to reporting and inadequate law enforcement responses exacerbate the harm experienced by victims, leaving them vulnerable to ongoing abuse.

4.1 Psychological and emotional effects of cyberstalking

Cyberstalking imposes severe psychological consequences, including anxiety, depression and PTSD. Victims often experience chronic anxiety from knowing their every move may be monitored, creating a persistent state of fear that undermines their mental health and sense of security (Cowan and Boyle, 2019). The emotional toll frequently results in depression and PTSD symptoms such as nightmares, flashbacks and hyperarousal (Priebe et al., 2017). The psychological distress is heightened when abusers exploit GPS tracking, spyware or hidden cameras to exert control over victims, making them feel powerless and constantly watched (Baker and Stonard, 2021).

4.2 Feelings of helplessness and entrapment

Cyberstalking fosters a profound sense of entrapment for victims. The continuous surveillance, digital harassment and online threats often make victims feel unable to escape abusive relationships. Abusers exploit victims' dependence on technology to control them, monitoring messages, dictating social interactions and restricting access to online platforms (Baker and Stonard, 2021). Victims frequently report losing autonomy, experiencing deepening isolation and becoming increasingly dependent on their abusers. This digital control tends to escalate over time, reinforcing the cycle of abuse. Many victims hesitate to leave their homes or maintain personal connections owing to fear of retaliation or intensified abuse.

4.3 Social isolation and economic control

Cyberstalking and digital abuse exacerbate social isolation by severing victims' connections to their support networks. Abusers may force victims to block contacts, delete social media accounts or stop communicating with friends, further increasing their psychological dependence (Watson and Joubert, 2022). Economic dependence also heightens vulnerability, particularly when abusers manipulate digital tools to control finances – denying victims access to accounts, restricting online banking or interfering with professional communication (Nkosi, 2022). The lack of financial independence makes it even harder for victims to escape abusive relationships.

4.4 Barriers to seeking help and documenting abuse

Despite the severity of cyberstalking in IPV, significant barriers prevent victims from seeking legal protection:

- **Difficulties in documenting digital abuse:** Many victims lack the technical expertise to track spyware, recover deleted messages or gather digital evidence. This makes it challenging to prove harassment to law enforcement or in court (Aderibigbe, 2021).

- **Law enforcement's limited technical knowledge:** Police officers often lack training in cybercrime investigation and struggle to handle digital evidence effectively (UNODC, 2011).
- **Victim-blaming and dismissive attitudes:** Victims frequently report being dismissed, ridiculed or advised to 'just block the perpetrator' rather than receiving meaningful legal support (Mwangi and Otieno, 2021).
- **Fear of retaliation:** Many survivors hesitate to report cyberstalking out of fear that abusers will escalate their threats or retaliate, particularly when perpetrators have access to victims' digital devices (Aderibigbe, 2021).

4.5 Law enforcement failures in addressing TFIPV

Despite the rising prevalence of TFIPV, law enforcement in many African countries has struggled to investigate and prosecute cases effectively. Key challenges include outdated legal frameworks, lack of digital forensic capabilities and systemic neglect.

4.5.1 Case studies: law enforcement negligence

Several high-profile cases illustrate law enforcement's failure to address TFIPV effectively:

- **Kenya – the murder of Ivy Wangechi (2019):** Ivy Wangechi, a 26-year-old university student, was murdered by her stalker after months of online harassment and threats. Despite filing complaints, law enforcement failed to intervene, ultimately leading to her tragic death (Musambi and Inganga, 2024).
- **Nigeria – international sextortion case (2024):** A Nigerian man was extradited to the US after operating a sextortion scheme that led to the suicide of a South Carolina teenager. This case exposed gaps in Nigeria's cybercrime enforcement, as similar domestic cases often remain underreported and uninvestigated (Collins, 2024).
- **South Africa – dismissal of cyber harassment complaints (2022):** A South African woman reported persistent digital stalking, but police dismissed her complaint and advised her to 'just block the number' instead of offering legal recourse (UNODC, 2011).

4.5.2 Notable incidents of cyberstalking and digital harassment in Africa

- **Kenya – cyberattacks and digital violence (2024):** Hackers targeted government platforms, exposing cybersecurity vulnerabilities. Victims of cyber harassment struggled to obtain police assistance owing to wider instability in Kenya's digital security systems (Jackson, 2024).

- **Nigeria – social media scams and online harassment (2024):** Meta removed over 63,000 fake Nigerian Instagram and Facebook accounts linked to romance scams, identity theft and cyber harassment. Despite victims' reports, law enforcement follow-up remained inadequate (Adeoye, 2024).
- **South Africa – digital stalking and revenge pornography:** Despite legal protections under the Cybercrimes Act, many cases of cyberstalking and revenge pornography remain unresolved owing to weak enforcement and limited police resources (Ekanem, 2024).
- **Africa-wide sextortion networks:** Reports reveal that sextortion networks across Africa have blackmailed thousands of victims, yet law enforcement fails to provide consistent legal protection (Ekanem, 2024).

5. Combating cyberstalking in TFIPV

Cyberstalking, as a form of TFIPV, requires a comprehensive, evidence-based and policy-driven approach to effectively combat it. This includes legal reforms, digital literacy initiatives, enhanced victim support, industry accountability and international co-operation. However, moving beyond broad recommendations, it is crucial to outline concrete, actionable steps for implementation, ensuring technological, legal and institutional mechanisms work together to protect victims.

This section examines ongoing global and regional initiatives to combat TFIPV while presenting key recommendations for legal enforcement, victim assistance, digital security measures and international co-operation.

5.1 Ongoing global and regional efforts to combat TFIPV

Several international and regional initiatives have been developed to address cyberstalking within IPV. These efforts focus on harmonising legal frameworks, fostering cross-sector collaboration and leveraging technology for prevention and intervention.

5.1.1 Global initiatives

Budapest Convention on Cybercrime

The Council of Europe's Convention on Cybercrime, also known as the Budapest Convention (2001), provides an international legal framework to combat cybercrime, including cyberstalking. Adopted in 2001, the Convention facilitates the harmonisation of national laws, promotes international co-operation and establishes procedures for investigating and prosecuting cybercrimes. It is considered the benchmark for developing global legal standards to address technology-facilitated abuse.

WePROTECT Global Alliance

The WePROTECT Global Alliance is a multi-stakeholder initiative that unites governments, technology companies and civil society organisations to combat online abuse and exploitation. Its focus extends to TFIPV, as it promotes evidence-based policies and practices to safeguard vulnerable groups. The alliance's Global Threat Assessment Report highlights emerging threats and provides recommendations for addressing technology-facilitated violence (WePROTECT Global Alliance, 2022).

Making All Spaces Safe Programme (UNFPA)

The Making All Spaces Safe Programme, under the United Nations Population Fund (UNFPA), specifically addresses technology-facilitated gender-based violence. The initiative aims to fill critical gaps in prevention and response by integrating targeted activities into existing gender-based violence programming. It promotes rights-based laws and safety-by-design standards in technology development. With pilot programmes in Benin and Kenya, the initiative employs a participatory, context-driven approach to ensure tailored and sustainable solutions for communities (UNFPA, 2022).

Digital Services Act (EU)

The Digital Services Act enacted by the EU establishes robust regulations for online platforms, mandating them to proactively combat online harassment and abuse. The Act holds technology companies accountable for ensuring user safety, requiring transparency in content moderation and the implementation of effective reporting mechanisms.

Global Network Initiative

The Global Network Initiative brings together technology companies, academics and human rights organisations to promote privacy and freedom of expression online. It provides a framework for companies to address online harassment while safeguarding digital rights, emphasising the importance of transparency and accountability in mitigating cyberstalking and TFIPV (GNI, 2021).

Girls Can Code Initiative (ITU)

The International Telecommunication Union (ITU) Girls Can Code Initiative is an educational programme aimed at equipping women and girls with technical skills to safely navigate digital spaces. By enhancing digital literacy, the initiative empowers women to recognise, prevent and respond to online abuse, fostering resilience against technology-facilitated violence (ITU, 2022).

5.1.2 African-focused efforts

Efforts to combat TFIPV in Africa span regional, national and grassroots levels. These initiatives focus on legal reforms, policy harmonisation, victim protection and digital literacy programmes to create safer online environments and empower survivors of digital abuse.

Convention on Cyber Security and Personal Data Protection (AU)

Known as the Malabo Convention, the Convention on Cyber Security and Personal Data Protection, adopted by the AU in 2014, serves as a foundational regional instrument in combating cybercrime, including cyberstalking and digital abuse. It urges member states to criminalise technology-facilitated abuse, establish robust frameworks for victim protection and harmonise cybercrime laws across African nations. By advocating for uniform legal responses and cross-border co-operation, the Malabo Convention seeks to strengthen regional cybersecurity governance. However, its adoption and implementation remain inconsistent, with many African nations yet to ratify or fully integrate its provisions into domestic law (Bakibinga, 2022).

National legislative efforts on TFIPV

Several African countries have enacted legal frameworks to address TFIPV, including Kenya, Morocco, Nigeria, Rwanda, South Africa and Uganda. Laws such as the Computer Misuse and Cybercrimes Act (Kenya 2018), the Cybercrimes (Prohibition, Prevention, Etc.) Act (Nigeria 2015) and the Cybercrimes Act (South Africa 2020) criminalise cyberstalking, online harassment and unauthorised access to digital information. Additionally, Morocco's Law No. 103-13 2018 on Combating Violence Against Women, Rwanda's Cybercrime Law 2020 and Uganda's Computer Misuse Act 2011 contain provisions addressing online abuse. While these legislative efforts demonstrate progress, enforcement gaps, limited law enforcement capacity and low public awareness continue to hinder their effectiveness (Moyo and Nkosi, 2020). Greater focus on implementation and survivor-centred legal responses is essential to strengthening protections against digital IPV.

Paradigm Initiative and Digital Rights Advocacy

The Paradigm Initiative (PIN) is a leading digital rights advocacy organisation in Africa, working to ensure cybercrime laws incorporate protections for IPV survivors. Through research, policy engagement and legal aid, PIN provides critical support for victims of digital abuse while pushing for survivor-centred legislation. The organisation also offers digital security training, equipping women with the knowledge to protect themselves from online threats. PIN's advocacy efforts have contributed to key policy discussions on cyber rights and safety, influencing legal reforms in multiple African countries (PIN, nd).

FEMNET and policy reform for women's digital safety

FEMNET, a pan-African feminist network, actively engages governments and regional bodies to promote policies that protect women from online harassment and digital violence. The organisation works on gender and technology issues, advocating for stronger legal frameworks that address TFIPV. FEMNET also collaborates with civil society groups to raise awareness of digital gender-based violence and supports initiatives that provide legal aid to survivors. By integrating feminist perspectives into policy discussions, FEMNET ensures legal and technological interventions remain gender-sensitive and survivor-centred (FEMNET, nd).

Safe Sisters programme and digital security training

The Safe Sisters programme is a grassroots initiative aimed at equipping women with practical cybersecurity skills to protect themselves from online abuse. Through workshops and mentorship, it empowers survivors with knowledge on securing personal data, recognising digital threats and implementing protective measures against cyberstalking and digital harassment. The programme also builds peer support networks, enabling women to share experiences and strategies for digital self-defence. Safe Sisters plays a crucial role in bridging the digital literacy gap, particularly for women in underserved communities (Internews, nd).

CyberSafe Foundation's Cybersmart Women initiative

The CyberSafe Foundation's Cybersmart Women initiative focuses on educating women on online safety, particularly those in marginalised communities who are at greater risk of digital abuse. The programme provides accessible training on cybersecurity best practices, helping survivors navigate online spaces securely while advocating for broader digital rights awareness. By fostering community-driven awareness campaigns, the CyberSafe Foundation ensures women have the tools to defend themselves against TFIPV and other forms of online gender-based violence. The initiative also partners with tech companies and law enforcement agencies to improve digital safety resources for vulnerable women (CyberSafe Foundation, nd).

While these initiatives mark significant progress in addressing TFIPV, continued efforts are needed to strengthen law enforcement capabilities, expand legal protections and improve digital literacy programmes, particularly in marginalised communities. A holistic, survivor-centred approach – integrating legal, educational and technological interventions – remains critical to effectively combating technology-facilitated abuse across Africa.

5.2 Recommendations for combating cyberstalking in intimate partner violence

Addressing cyberstalking within the context of IPV in Africa requires a multi-faceted, evidence-based and policy-driven approach that includes legal reforms, digital literacy initiatives, victim support structures, industry accountability and international co-operation. However, to move beyond broad recommendations, specific, actionable steps are necessary to guide policy implementation, technological solutions, funding mechanisms and specialised training programmes for stakeholders.

The following recommendations present a robust and sustainable framework to combat TFIPV.

5.2.1 Strengthening legal frameworks

Enacting IPV-specific cyberstalking legislation

African governments should introduce laws that explicitly criminalise cyberstalking within IPV cases, recognising digital coercive control methods like spyware, GPS tracking and non-consensual sharing of intimate images. These laws should impose strict penalties for unauthorised access to personal devices and online accounts used for abuse. Legal reforms should also mandate technology companies to co-operate with law enforcement in IPV-related cyberstalking cases and integrate specific protections for IPV survivors to prevent abusers from exploiting legal loopholes (Aderibigbe, 2021).

Enhancing enforcement through specialised training

To improve enforcement, governments should implement mandatory, specialised training programmes for law enforcement officers to identify, investigate and prosecute digital abuse cases. Judicial personnel should be trained to understand the intersection of IPV and technology-facilitated abuse. Digital forensic teams should receive advanced training in handling digital evidence in IPV cases. Public–private partnerships should support these training initiatives, with contributions from technology firms and civil society organisations (Nkosi, 2022).

Establishing cross-border legal co-operation

Cyberstalking laws should be harmonised across African jurisdictions to address the borderless nature of digital abuse. Countries should develop extradition agreements for IPV-related cyberstalking offenders and establish cross-border data-sharing protocols to facilitate access to digital evidence. Regional cybercrime taskforces under the AU should be developed to track and dismantle online IPV-related abuse networks.

5.2.2 Digital literacy and victim support mechanisms

Creating multilingual digital safety resources

Governments, non-governmental organisations and technology companies should collaborate to develop and distribute multilingual, culturally relevant digital safety materials. These resources should educate IPV survivors on securing personal devices, recognising spyware and using digital privacy tools. Ensuring accessibility in rural and underserved areas is essential, with resources provided in audio-visual formats for individuals with low literacy levels (Mwangi and Otieno, 2021).

Expanding and funding IPV support networks

IPV survivors need comprehensive, technology-sensitive support services, including 24/7 digital abuse hotlines and online safe spaces. Free digital security clinics should be established to assist survivors in removing spyware and securing devices. Governments should establish sustainable funding mechanisms, including public–private partnerships with technology companies, national budget allocations and international donor grants to ensure long-term financial sustainability.

5.2.3 The role of technology companies in safeguarding users

Strengthening privacy and security features

Technology companies must enhance platform security to protect users from IPV-related cyberstalking. This includes implementing stronger encryption, account security measures, automatic alerts for suspicious activity and easy-to-use account recovery processes for IPV survivors facing cyber threats.

Enhancing reporting mechanisms for IPV-related abuse

Companies should develop user-friendly, multilingual reporting channels that allow IPV survivors to report abuse discreetly. Platforms should offer real-time assistance from digital safety specialists and provide anonymised legal resources for survivors seeking justice.

Collaborating with law enforcement and advocacy groups

Technology firms should work with law enforcement agencies and IPV advocacy groups to improve protection measures for survivors. This includes facilitating priority access to digital security assistance, implementing secure information-sharing protocols and supporting funding initiatives for legal and psychological assistance to victims of digital abuse.

5.2.4 International co-operation and policy implementation

Developing regional and global cyberstalking agreements

African governments should establish intergovernmental task forces under the AU to address cross-border IPV-related cybercrime. Standardised legal frameworks for online IPV prosecution should be developed to ensure uniformity in law enforcement responses. Partnerships with global cybersecurity organisations should be pursued to enhance access to digital crime expertise and technological resources.

Implementing clear policy action plans

Governments should develop clear implementation roadmaps to ensure accountability and measurable progress. This includes assigning responsible agencies for enforcing IPV-related cyberstalking laws; setting time-bound targets for legal reforms, technology upgrades and funding allocation; and establishing monitoring and evaluation mechanisms to assess the effectiveness of implemented policies.

6. Conclusion

The digital age has introduced new dimensions to IPV, particularly through cyberstalking, online harassment and digital surveillance. As technology becomes more integrated into daily life, abusers have new tools to control, manipulate and intimidate their partners. This study highlights the vulnerabilities of victims and the inadequacies of legal systems, digital platforms and social services in addressing technology-facilitated abuse. It explores the legal, social and psychological dimensions of digital abuse and provides actionable recommendations to address these issues.

The findings underscore the need for stronger legal frameworks tailored to digital abuse in IPV contexts. While some African countries have made progress by implementing cybercrime laws and anti-stalking provisions, these laws often remain inadequate in addressing the nuances of digital IPV. Lack of enforcement, limited resources within law enforcement agencies and insufficient public awareness contribute to the continued prevalence of cyberstalking and digital harassment in abusive relationships. Many legal systems lack the capacity to handle the technicalities of technology-facilitated abuse, leaving victims without sufficient recourse.

In addition to legal reform, enhancing digital literacy and providing robust support for victims of cyberstalking are essential steps towards mitigating the impact of digital IPV. Victims often face significant barriers, including a lack of awareness of their rights, limited knowledge of how to protect their digital privacy and social stigmas that prevent them from reporting abuse. Empowering individuals, particularly women and marginalised groups, with the tools to recognise and resist online abuse is key to breaking the cycle of control and manipulation enabled by technology.

The role of technology companies is also crucial in preventing and responding to digital IPV. While many tech companies have implemented safety features, these measures remain insufficient in preventing cyberstalking and ensuring user privacy. There is an urgent need for stronger privacy protections, proactive abuse detection and collaboration between tech companies, law enforcement and advocacy groups. Creating a more user-centred, safety-oriented environment can help the tech industry reduce its role as an enabler of IPV.

Artificial intelligence (AI) introduces additional complexities to the landscape of digital IPV. AI can be exploited by abusers to enhance surveillance, automate harassment and manipulate digital environments. For instance, AI-driven tools can be used to track victims' online activities, generate deepfake content or deploy automated bots for continuous harassment. Future research should explore the implications of AI in exacerbating digital abuse and develop strategies to counteract these threats. This includes advocating for AI ethics in technology development, implementing robust AI detection and mitigation tools, and ensuring AI systems are designed with abuse prevention in mind.

Finally, international co-operation is necessary to address the cross-border nature of cyberstalking. As the internet transcends national borders, abusers and victims of digital abuse often reside in different countries, complicating efforts to prosecute and hold offenders accountable. Strengthening legal co-operation between African countries and beyond, while establishing international norms for digital abuse, will ensure cyberstalking abusers can be held accountable, no matter where they are located.

In conclusion, addressing cyberstalking within IPV requires a multi-dimensional approach involving legislative reform, victim support, digital literacy and industry accountability. African nations must commit to reforming and harmonising legal frameworks, enhancing digital literacy and fostering collaboration between stakeholders to protect IPV victims from technology-facilitated abuse. A co-ordinated, comprehensive response can help mitigate the risks posed by cyberstalking, protect survivors and create a safer, more supportive digital environment. Future writing should delve deeper into the role of AI in digital abuse, exploring both the challenges it presents and potential solutions to safeguard victims in an increasingly AI-driven world.

References

Adebayo, T. and Musa, S. (2021) 'Digital Abuse in Nigeria: The Role of Cyberstalking in Intimate Partner Violence'. *Journal of African Media Studies* 13(2): 89–105.

Adeoye, A. (2024) 'Meta Removes over 63,000 Fake Nigerian Instagram and Facebook Accounts Tied to Scams'. *Financial Times*, 26 August. https://www.ft.com/content/42caef4f-c6d5-41e5-8e91-9b5bebc37b13

Aderibigbe, A. (2021) 'Digital Intimate Partner Violence in Nigeria: Challenges and Interventions'. *Journal of African Studies* 58(3): 221–236.

Adeyemi, A. (2018) 'Cybercrimes and the Nigerian Legal System: Challenges and Opportunities'. Lagos: *Nigerian Law Review*.

Baker, L. and Stonard, K. (2021) 'The Impact of Technology on IPV: A Psychological Perspective'. *Journal of Domestic Violence Studies* 16(2): 81–98.

Bakibinga, P. (2022) 'Cybercrime and Governance in Africa: Evaluating the Implementation of the Malabo Convention'. *African Journal of Law & Technology* 7(1): 45–62.

Bowlby, J. (1969) 'Attachment and Loss: Vol. 1. Attachment'. *New York: Basic Books*.

Chigbu, U., Ezeh, C. and Nnadi, N. (2020a) 'Addressing Cyberstalking in African Societies: Legal and Social Implications'. *African Journal of Cyber Law* 12(1): 15–32.

Chigbu, U., Okoro, P. and Nwankwo, E. (2020b) 'Digital Divide and IPV: The Role of Technology in Rural and Urban Settings in Africa'. *International Journal of Cyber Criminology* 14(2): 233–247.

Collins, J. (2024) 'Nigerian Man Extradited to the U.S. over Sextortion Case Linked to South Carolina Teenager's Death'. AP News, 27January. https://apnews.com/article/832b99698558ccc37beb80d15ea4d83b

Cowan, A. and Boyle, P. (2019) 'Psychological and Emotional Abuse in Intimate Partner Violence: The Role of Technology'. *Journal of Abuse and Trauma* 14(4): 183–205.

CyberSafe Foundation (nd) 'Cybersmart Women Initiative: Empowering Women Against Digital Violence'. www.cybersafefoundation.org (accessed 15 February 2025).

Department of Home Affairs (2021) 'The Cybercrimes Act in South Africa: Implementation Challenges and Prospects'. Pretoria: Government Printer.

Douglas, H., Harris, B.A. and Dragiewicz, M. (2019) 'Technology-Facilitated Domestic and Family Violence: Women's Experiences'. *British Journal of Criminology* 59(3): 551–570.

Dragiewicz, M., May, P.J. and Mohr, G. (2019) 'Technology-Enabled IPV: A Study of Cyber Abuse in Intimate Relationships'. *Violence Against Women* 25(6): 659–677.

Ekanem, S. (2024) '10 Major Cyberattacks That Targeted African Organizations in 2024'. Business Insider Africa, 2 January. https://africa.businessinsider.com/local/lifestyle/10-major-cyberattacks-that-targeted-african-organizations-in-2024/qsqgmlq

Eze, P. and Chukwudi, U. (2019) 'Patriarchy and Digital Abuse: An Analysis of Gender Norms in Nigeria'. *African Journal of Gender Studies* 8(1): 45–62.

FEMNET (nd) 'Digital Rights and Gender Justice in Africa'. https://femnet.org (accessed 15 February 2025).

Global Network Initiative (GNI) (2021) 'Annual Report 2021'. Available at: https://globalnetworkinitiative.org/gni-annual-report-2021/ (Accessed: 11 November 2024).

Hinson, L., Mueller, J., O'Brien-Milne, L. and Wandera, N. (2018) *Technology-Facilitated Gender-Based Violence: What Is It, and How Do We Measure It?* Washington, DC: International Center for Research on Women.

International Telecommunication Union (ITU) (2022) 'Measuring digital development: Facts and figures 2022'. Available at: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (Accessed: 11 November 2024).

Internews (nd) 'Safe Sisters Program: Strengthening Digital Security for Women'. https://www.internews.org (accessed 15 February 2025).

Jackson, A. (2024) 'Cyberattack in Kenya Impacts Online Government Platforms'. *Cyber Magazine*, 31 July. https://cybermagazine.com/application-security/cyberattack-in-kenya-impacts-online-government-platforms

Kamau, J. and Njoroge, R. (2021) 'Cyberstalking and Intimate Partner Violence in Kenya: An Emerging Digital Threat'. *Journal of Cyber Policy* 6(1): 112–130.

KICTANet (Kenya ICT Action Network) (2022) 'Annual Report 2022: Advancing Digital Rights in Kenya'. Nairobi: KICTANet.

Mason, A. (2021) 'The Role of Technology Companies in Preventing and Reporting Cyber Abuse'. *Journal of Digital Law and Practice* 2(3): 112–129.

Mba, O. and Nwankwo, E. (2020) 'The NDPR and Cybercrime in Nigeria: Opportunities and Challenges'. *Journal of Cyber Law in Africa* 14(2): 35–50.

Moyo, T. and Nkosi, B. (2020) 'Digital Misogyny: Exploring the Intersection of Gender-Based Violence and Technology in South Africa'. *South African Journal of Social Research* 8(3): 78–94.

Musambi, E. and Inganga, B. (2024) 'Protests Erupt in Kenya over Gender-Based Violence and Femicide'. AP News, 10 December. https://apnews.com/article/4db1006b745e51dbbed5005f664e632b

Mutua, D. (2019) 'Stigma, Reporting, and Gendered Violence in Kenya: Challenges in the Digital Era'. *East African Social Science Review* 12(2): 55–73.

Mwangi, L. and Otieno, J. (2021) 'Social Media and IPV: Emerging Trends in Kenya'. *East African Journal of Social Sciences* 10(4): 35–48.

Njogu, M. (2020) 'Assessing the Impact of the Computer Misuse and Cybercrimes Act in Kenya'. *Kenyan Journal of Law and Technology* 4(1): 33–48.

Nkosi, Z. (2022) 'Exploring the Impact of Cyber IPV in South Africa'. *South African Journal of Gender Studies* 19(2): 50–65.

Nyeko, O. (2023) 'Ugandan Parliament Passes Extreme Anti-LGBT Bill'. Human Rights Watch, 22 March. www.hrw.org/news/2023/03/22/ugandan-parliament-passes-extreme-anti-lgbt-bill

Okafor, C. (2020) 'Digital Harassment in Nigeria: Prevalence and Implications'. *African Journal of Digital Studies* 7(2): 201–219.

Pence, E. and Paymar, M. (1993) 'Education Groups for Men Who Batter: The Duluth Model'. *New York: Springer.*

PIN (Paradigm Initiative) (nd) 'Protecting Digital Rights in Africa: Advocacy for Legal Reforms'. https://paradigmhq.org (accessed 15 February 2025).

Priebe, G., Holmes, D. and Walker, B. (2017) 'Cyberstalking: The Psychological Effects of Digital Abuse'. *Journal of Psychological Violence* 21(5): 112–127.

Rege, A. (2020) 'Cyberstalking Victimization: An Analysis of Behavioral Impacts'. *Journal of Interpersonal Violence* 35(7-8): 1501–1522.

Reed, L.A., Ward, K. and Parisi, D. (2022) 'Technology and Coercive Control in IPV Cases'. *Criminology & Public Policy* 21(2): 389–415.

Seligman, M. E. P. (1975) 'Helplessness: On Depression, Development, and Death'. *San Francisco: W. H. Freeman.*

Smith, L., Brown, R. and Naidoo, P. (2019) 'Online Harassment and Cyberstalking in South Africa: An Empirical Analysis'. *Cyberpsychology, Behavior, and Social Networking* 22(5): 310–317.

Suler, J. (2004) 'The online disinhibition effect', *Cyberpsychology & Behavior*, 7(3), pp. 321–326.

United Nations Population Fund (UNFPA) (2022) 'Annual Report 2022'. Available at: https://www.unfpa.org/annual-report-2022 (Accessed: 11 November 2024).

UNODC (United Nations Office on Drugs and Crime) (2011) *Handbook on Police Accountability, Oversight and Integrity*. Vienna: UNODC.

Wajcman, J. (2004) 'TechnoFeminism'. *Cambridge: Polity Press*.

Watson, R. and Joubert, E. (2022) 'Addressing Digital Harassment in South Africa: A Review of Legal Gaps'. *South African Law Review* 36(1): 75–98.

Watson, M., Pretorius, L. and van der Westhuizen, C. (2022) 'Digital Forensics in IPV Cases: Challenges and Recommendations'. *South African Journal of Criminal Justice* 35(2): 148–165.

WePROTECT Global Alliance (2022) 'Global Threat Assessment 2022'. Available at: https://www.weprotect.org/global-threat-assessment-2022/ (Accessed: 11 November 2024)

WHO (World Health Organization) (2021) *Intimate Partner Violence: Key Facts*. Geneva: WHO.

Woodlock, D. (2017) 'The abuse of technology in domestic violence and stalking', *Violence Against Women*, 23(5), pp. 584–602.

Zouiten, S. (2024) 'Ouahbi Announces Stricter Penalties for Online Harassment, Blackmail in Morocco'. *Morocco World News*, 22 May. www.moroccoworldnews.com/2024/05/362792/ouahbi-announces-stricter-penalties-for-online-harassment-blackmail-in-morocco

About the author

Chioma Andeh is a cybersecurity and ICT governance professional with nearly a decade of experience spanning legislation, cybersecurity consulting, and digital policy, and open source intelligence. She holds a Master's degree in Information Security and is passionate about privacy, data protection, and digital rights, particularly within the African context. As the Team Lead for Communications and Media at WiCyS Nigeria, she actively promotes cybersecurity awareness and policy advocacy, working to strengthen Africa's digital resilience through research, engagement, and strategic communication.

The Commonwealth

Commonwealth Cyber Journal \ 145
Print ISSN 2959-3018, online ISSN 2959-3026
thecommonwealth.org/cyber-journal

Nexus between Cybercrime Financial Fraud and Online Gambling in Bangladesh

Mahfuzul Mithun[1], Md Masudul Islam Khan[2] and Md Habibur Rahman[3]

Abstract

This study explores how online gambling leads to cybercrime and relates to financial fraud, money laundering and other illegal activities in Bangladesh, drawing on an investigation of local agents for gambling companies.

A significant finding is the increasing use of online gambling by criminal organisations as a mechanism for money laundering, via digital payment systems and mobile financial services. Local gambling agents, often unaware of their participation in illegal financial activities, function as intermediaries in these transactions. Meanwhile, fraudulent practices arise within the online gambling industry. Manipulated algorithms and deceptive promotional strategies induce players into sustained financial losses. Social media platforms, particularly Facebook, Telegram and WhatsApp, play a pivotal role in recruiting new gamblers, with targeted advertisements enticing vulnerable groups, including students and unemployed youth, into the gambling network.

The absence of effective law enforcement and regulatory oversight exacerbates the issue. Corruption, bureaucratic inefficiencies and inadequate cybercrime monitoring tools have enabled gambling operators to function with impunity. Despite legal prohibitions, bribery and political influence frequently impede authorities from taking decisive action. There is an urgent need for policy interventions, including legislative reforms, financial monitoring enhancements and cross-border co-operation to mitigate cyber-financial crimes associated with online gambling.

1 Master's student of Public Administration, Shahjalal University of Science and Technology
2 Graduate of Social Science in Public Administration, Shahjalal University of Science and Technology
3 Graduate of Social Science in Public Administration, Shahjalal University of Science and Technology

1. Introduction and background

Cybercrime can be described as any criminal activity taking place via the internet or other electronic means. Virtual financial crime falls within the category, comprising financial crimes such as fraud, money laundering and scams that take place on the internet (Chambers-Jones and Hillman, 2014). Online gambling is considered a form of cybercrime in many jurisdictions, including in certain Commonwealth countries, and strict regulations exist to combat it in these cases.

The global rise of online gambling highlights widespread legal and ethical concerns, and the situation in Bangladesh reflects these challenges on a local scale. A recent report states that more than 5 million individuals are engaged in gambling in Bangladesh (UNB, 2024). As a predominantly Muslim country, Bangladesh regards gambling as culturally unacceptable, in alignment with religious and societal norms. The High Court of Bangladesh has declared all sorts of gambling across the country illegal, and has directed the government to take steps against gambling organisers and gamblers (Prothom Alo, 2020). The Constitution of the People's Republic of Bangladesh Article 18(2) clearly states that 'The State shall adopt effective measures to prevent prostitution and gambling.' Therefore, online gambling is undoubtedly a crime in the context of Bangladesh but there is legal ambiguity surrounding the matter and there are no specific laws to regulate the industry.

The absence of proper regulatory frameworks has led to unregulated access to foreign online gambling platforms, resulting in substantial financial outflows from the country (The Daily Star, 2024). A recent investigation report in Bangladesh reveals the extensive involvement of local agents in facilitating online gambling operations like Bet Winner and BetVisa, where funds are laundered through mobile financial services (MFS) and converted into cryptocurrency for international transfer. These activities highlight the growing nexus between online gambling, money laundering and cybercrime, posing significant regulatory and enforcement challenges (Bonik Barta, 2023). Such an unregulated environment makes it essential to study the issues related to online gambling within the Bangladeshi context.

The activities of gamblers can range from simple fraud to more sophisticated operations involving extortion and money laundering (Prakash et al., 2024). Interestingly, the digital environment of the internet has altered conventional understandings of gambling-related criminal relationships. The anonymity and global nature of online platforms have created new opportunities for criminals to operate across borders and jurisdictions (McMullan and Rege, 2010). This has made it challenging for authorities to regulate and control these activities effectively.

Cyber fraud is a significant concern in online gambling, illegal gambling activities, money laundering, fraud and theft (Banks, 2017). One of the most prevalent forms of fraud is money laundering through online gambling sites. Fraudsters use modern financial services and products provided by banking institutions to legalise criminal proceeds and

finance terrorism (Kuzmenko et al., 2022). The billion-dollar online gambling industry includes illegal ways of exchanging virtual assets for real money, causing imbalances in economic processes (ibid.).

The relationship between online gambling and money laundering is complex and varies across jurisdictions. In Taiwan, online gambling has been linked to organised crime, fraud and money laundering, posing significant challenges for law enforcement (Huang et al., 2022). Similarly, in Malaysia, there is growing concern about the threats of online gaming and its potential for money laundering, prompting calls for new legislation and control mechanisms (Dhillon and Miin, 2013). To address these issues, countries are exploring various regulatory approaches, such as the European Commission's Green Paper on Online Gambling and Australia's Interactive Gaming Act 2001 (ibid.). As the online gambling industry continues to evolve, it is crucial for regulators and law enforcement agencies to adapt their strategies to combat money laundering risks effectively.

In the realm of online gambling, the internet has revolutionised accessibility and convenience, allowing gamblers to place bets or play casino games from the comfort of their homes (Smith and Rupp, 2005). This increased accessibility has raised concerns about the potential for addiction and financial devastation. The online gambling industry has excelled in customer service, offering advanced technologies and promotional campaigns to attract users (ibid.). However, this has led to various ethical and regulatory dilemmas, including questions about targeting vulnerable populations and the use of credit cards for gambling purposes (ibid.; Gainsbury et al., 2013).

The rise of online gambling represents a transformative shift in how individuals engage with gambling activities, driven largely by advancements in internet technology and the proliferation of digital platforms (Smith and Rupp, 2005). While the convenience and accessibility of online gambling have contributed to its global growth, these same factors have introduced significant legal, ethical and regulatory challenges. This study seeks to examine these challenges, particularly focusing on the intersection of online gambling, cybercrime and money laundering, which represent critical areas of concern for governments, regulators and law enforcement agencies worldwide.

Given the manifold nature of online gambling and its associated risks, this study is both timely and necessary. Gambling is illegal in Bangladesh, and numerous illicit activities are being conducted through online platforms. The proliferation of online gambling is considered a form of cybercrime. From this point, then, the study addresses the role of online gambling as a gateway to cybercrime and its impact on financial fraud, money laundering and illicit activities in the context of Bangladesh.

By examining the intersections of cybercrime, money laundering and regulatory approaches, this research aims to provide valuable insights for policy-makers, regulators and other stakeholders. The findings will contribute to the development of effective strategies to combat the challenges posed by online gambling while promoting consumer protection and maintaining the integrity of financial systems.

2. Study methodology

This study follows Husserlian phenomenology (Creswell and Creswell, 2017) grounded in the constructivist paradigm (Wahyuni, 2012) to explore the issues related to online gambling as a means of cybercrime. By employing epoché, researchers set aside preconceived notions to centre participants' lived experiences. Semi-structured interviews provided an open space for participants to share their perspectives, while thematic analysis ensured that insights emerged organically from their narratives. Additionally, reflexivity and bias control measures were implemented to minimise subjective interference, maintaining the integrity of data interpretation.

Given the sensitive and socially unrecognised nature of gambling in Bangladesh, a combination of purposive and snowball sampling was employed. This dual approach ensured access to a diverse and relevant group of participants. The study conducted in-depth interviews with a total of 15 participants, categorised into different professions and roles within online gambling networks, and also known as 'agents'. The lack of social recognition and the limited availability of online gambling industry agents meant it was challenging to determine an appropriate population size, resulting in a limited sample size for this research.

The collected data were transcribed and analysed using a thematic analysis approach, which is recognised for its flexibility and effectiveness in qualitative research (Castleberry and Nolen, 2018). This method enabled the identification, organisation and interpretation of patterns and themes within the dataset (Braun and Clarke, 2013). An inductive approach was employed to allow patterns to emerge directly from the data, rather than relying on pre-existing theories (Patton, 2002).

To enhance the validity and reliability of the analysis, reflexivity was practised throughout the process. Regular reflexive notes recorded the researcher's assumptions and potential biases. Additionally, peer debriefing and constant comparison with raw data ensured the findings accurately reflected participants' perspectives.

Ethical guidelines were strictly followed. Participants were informed about the study's purpose and nature, and written consent was obtained prior to their participation. Verbal approval from the Social Science Ethics Board at Shahjalal University of Science and Technology further validated the study's adherence to institutional ethical standards; written approval will be available upon publication of the study. Anonymity and confidentiality of participants were ensured throughout the research process.

This study has several limitations that should be acknowledged. The small sample size, of only 15 participants, restricts the generalisability of the findings, limiting their applicability to broader populations. Furthermore, the absence of quantitative data prevents the triangulation of findings, which could have strengthened the reliability of the qualitative insights. Lastly, the limited demographic diversity among participants may constrain the depth of understanding regarding the experiences of different population groups.

3. Findings

This section presents the findings derived from thematic analysis of the qualitative data gathered from 15 participants, primarily individuals working as local agents and facilitating gambling operations. The analysis focuses on the study's objectives.

3.1 Online gambling as a cybercrime and its impact on financial fraud

3.1.1 Perceptions of online gambling as a criminal activity

Participants recognised that online gambling was prohibited under Bangladesh's legal regime. The respondents said that they had never engaged in online gambling with the intention of engaging in criminal activities, but that their actions were spur of the moment, fuelled by socio-economic status: they were extremely needy, poor, unemployed or broke. To most of them, online gambling came across as a solution for their financial difficulties amid few employment opportunities and high living costs. It was common to hear that internet gambling was a mere act of survival not a criminal act. One participant noted:

> *'We all know it's illegal, but the reality is people here don't have many options to make money quickly. Life is tough, and gambling seems like an easy way to earn. Besides, law enforcement doesn't pay much attention to it unless something big happens or it becomes a media issue.'*

This statement confirms the social concerns of the participants but also reveals an important contradiction in most jurisdictions: while online gambling is unlawful, lack of enforcement means there is a kind of normative acceptance of gambling, particularly among those in situations of financial precarity. Another respondent stated:

> *'I don't feel like I'm doing anything seriously wrong. I am just helping people connect to these platforms, and in return I get a commission. If the authorities really cared, they would shut it all down, but they don't.'*

This presentation and justification of online gambling as a means of earning a living rationalises a deeper societal problem. Lack of solutions to socio-economic problems by established systems mean online gambling is an accepted and unspoken part and parcel of the lives of many people, despite it being prohibited.

Online gambling is seen as a criminal endeavour in a highly contingent manner. Although participants know it is unlawful, desperation compounded by poor policing lead to internet gambling seemingly being ca legal business. This also underlines the importance of suggestions made to not only increase the effectiveness of measures to prevent the violation of existing laws but also address the problems that force people to participate in online gambling.

3.1.2 Online gambling leading to financial fraud

The participants highlighted a close association between online gambling sites and financial scams, and noted that these businesses operated based on deceit. Employees of gambling agencies, which sometimes organise co-operation between players and online platforms, explained how these systems were created to milk participants through scheming computations and lying marketing messages. All such fraudulent mechanisms result in both monetary losses and decreased trust among participants, with perpetrators who remain outside the law given that internet gambling is, for the most part, illicit and uncontrolled.

Especially typical was a frustration with the fact that some of these sites and services function secretly. Agents also confessed that these sites rigged their software so that the house, in other words the operators, would always triumph. A captivating feature is preliminary gains that give the player the feeling of expertise. However, as participants advance their stakes, the platforms consciously arrange matters in a way that leads them to incur large losses. This vicious cycle takes people into a cycle of gambling, as they try to reclaim what they have lost but mostly end up losing even more money.

One participant described this practice candidly:

> *'At first, you win a little, and it makes you think you've figured out the system. But then the game changes. The platform knows exactly how to keep you hooked while taking your money. People keep gambling, thinking the next round will be different – but it never is.'*

Participants also shared cases where the winnings were promised but never paid out. Some of the platforms entice gamblers by displaying high pay-outs or bonuses that are almost impossible to resist, knowing well they will close down or refuse to pay customers once people have wagered considerable amounts. Such fraud is common, as participants in such scams know very well the illicit nature of the actions they perform and are unlikely to report them to the police. The victims are too afraid of being punished or exposing their financial losses and fraud to the authorities.

One agent explained:

> *'People bet expecting to win big, but these platforms are tricked. Even if you win, the money doesn't always come. The big guys running it just vanish overnight. You can't even complain because, in the end, you're the one doing something illegal.'*

This statement points to the critical challenge of the combination of illegality and a lack of regulatory oversight creating a breeding ground for unchecked fraud. Participants who suffer financial losses are left without any legal remedy, as reporting such issues might implicate them in criminal activity. This situation emboldens operators to engage in increasingly sophisticated scams, knowing that victims are unlikely to pursue action against them.

The findings reveal that financial fraud within online gambling is not limited to isolated incidents but is systemic and pervasive. Platforms capitalise on the illegal and unregulated environment, exploiting participants' desperation and lack of awareness. Fraudulent behaviour is fuelled by the anonymity of online transactions, the absence of legal accountability and the psychological manipulation inherent in gambling systems.

3.2 Online gambling and its relationship with money laundering

3.2.1 Online platforms as tools for money laundering

The participants brought to bear their knowledge on how online gambling had transformed into what they described as a complex tool for money laundering. Given that online gambling operates through pseudo-anonymous transactions and features a high degree of obscurity, it represents an almost perfect way of laundering 'dirty' money into what may best be described as 'clean' money. Participants described how criminals, mafias, corrupt officials and other 'whales' used the uncontrolled financial environment to launder the money.

One of the main strategies mentioned was the use of unauthorised MFS, virtual wallets and international remittances. These systems are convenient for consumers but also full of holes that money makers do not hesitate to exploit. The transactions are channelled through a number of MFS accounts, opened under false identification or dummy names, making it extremely difficult to establish the actual ownership of the money. The agents explained that it was very easy to open such accounts using fake identification cards, or through local agents.

One participant elaborated on this practice:

> *'Big players use gambling platforms to clean their dirty money. They create fake bets – sometimes placing bets to win, sometimes deliberately losing. The money comes out looking clean, like gambling winnings, but it's all part of a plan. They just play the system to their advantage.'*

It is important to note that this flow is not an accidental manipulation of the gambling process but rather aims at tightening the 'layering' stage of the online gambling cycle. The process typically unfolds in three stages: placement, layering and integration. In the first stage, the proceeds of crime are introduced into the system of internet gambling, usually under the veil of legal funds for gambling. The second phase is one of layering, where many transactions are made, and bets are placed or winnings collected, or losses simulated to disguise the original transaction. Lastly, the clean money is withdrawn, returned to the legal financial stream and offered as gambling revenue, thus giving the figure a veneer of authenticity.

One thing that emerged clearly in participants' responses was the frequency of use of local agents and intermediaries in the conduct of these activities. Some money launderers are not involved in any way with gambling but contract agents to deal with the technical and financial aspects of the processes. These agents therefore have a number of accounts all purposely for the management of the transactions on behalf of the clients, to ensure that the real criminals are not seen. They carry out many small, disparate transactions, bringing no appreciable attention to themselves and avoiding current regulatory equipment.

One agent explained this role in detail:

> *'Many transactions happen through MFS accounts under fake names or through local agents like us. We handle the accounts and money flow, so the real culprits never come into the picture. It's all planned so no one can trace where the money is actually coming from.'*

The agents also pointed out how international remittances created an additional layer of uncertainty. Money is moved internationally, for example as personal transfers or masquerading as genuine business transactions, and channelled into the sites that offer internet gambling. Once the money is fed in, the laundering process is in effect almost pure, given that many of the operations are internet-based and many international jurisdictions do not co-operate with each other.

When money is derived from organised crime or any other vices, such as corruption, the use of online gambling to manage it not only undermines the organisation's activities but also threatens the integrity of financial systems. The risk is of the emergence of a parallel economy where black money obtains a legal veneer and distorts the actual structure of the economy and further encourages activities like the supply of controlled substances, human trafficking and terrorism.

3.2.2 Exploiting loopholes in financial systems

Interviewees pointed to key risks in financial environments, especially in cross-border transactions, with international online shops and organised criminals able to benefit systematically. These legal grey areas allow the easy channelling of embezzled money across national borders, and it is very hard for law enforcers to even see let alone follow the circulation of such money. There are few laws, and the enforcement of those laws that exist is inadequate, thus providing fertile ground for financial crimes or, for instance, money laundering or other fraudulent activities.

Most of the participants said that international gambling and gambling platforms existed in the legal loopholes across countries' borders. Most of these platforms are based in countries that have poor legal standards, and disclosure standards are lenient.

Money pumped into these platforms can easily be pulled out and transferred to other jurisdictions, and the transactions can easily pass as lawful to elude the fiscal authorities of nations such as Bangladesh.

One participant explained the situation concisely:

> *'There are no strict controls on foreign websites. Money moves across borders without any restrictions, and Bangladesh doesn't have strong systems to track this. These platforms exploit this weakness to hide illegal transactions.'*

This is so because there is no proper co-operation or collaboration among the various regulatory bodies in different countries. The international online platforms generally operate from countries that are notorious for refusing to provide financial details or that come with substandard anti-money laundering standards. The platforms can thus operate without restraint, arranging unlawful transfers as well as acting beyond the control of local governments. The respondents observed that this had left a legal vacuum through which money launderers, terrorists and other offenders can filter, conceal and spiral their money back into the legitimate economy.

3.3 Online gambling fraud through social media platforms

Social networks such as Facebook, WhatsApp, Telegram and Instagram are becoming popular means to advertise and encourage online gambling. Such sites act as entry points to recruit participants, including students, jobless youths and low-income earners. Interviews confirmed that people could freely access gambling operators through social media platforms and remain anonymous.

One of the most frequently used promotional strategies is the creation of open Facebook groups and pages that present the existing online gambling offers. These groups usually sell to 'soft targets', telling participants they are taking simple shortcuts to earn huge profits within the shortest time. Posts contain content such as positive comments by supposed participants, fake stories about success and pictures of large amounts of money, leading participants to believe that gambling is an easy way to obtain a large amount of money, and nothing bad will happen. Young individuals are directly targeted. An agent explained their strategy:

> *'We use Facebook groups to find clients. Young people are easy targets because they are always online and looking for ways to earn quick money. A flashy post about big winnings gets their attention immediately.'*

The organisation of agents and participants through accounts that are linked to official games and other platforms such as Telegram and WhatsApp also makes gambling easy since this is a means of real-time communication. Sport, lotteries and card game betting timetables are posted daily, with clear guidelines on how to pay through MFS or virtual wallets. Agents are there to offer direct assistance to newcomers, to help them

learn how the game works, to get them ready to place their bets and to encourage them to make more bets via bonuses or free bets. These fundamentals enhance participant engagement and ensure a constant stream of revenue to gambling operators.

It is of serious concern that platforms engage vulnerable demographics, in particular students and unemployed youths. Young people are easily preyed on, as a result of financial need, peer pressure or a thirst for excitement. This weakness is well understood by agents, who justify gambling as the ability to obtain financial freedom within a short time and literally at the touch of a button. One agent revealed:

> *'We give new players a small bonus to start. It's like a hook – once they win even a little, they think it's easy money and keep playing. Before they know it, they're hooked and spending more than they can afford.'*

A participant also highlighted that popular social media sites such as Facebook and Instagram promoted gambling content based on user actions. When a user clicks on a gambling post or becomes a subscriber to a gambling community, the program recommends more posts about gambling and shows them more ways to gamble. This leads to a cycle whereby users are exposed to and overwhelmed by advertisements and as such feel more compelled to be involved.

The spiral can then lead to youth, especially students and the unemployed, taking out credit and getting trapped in debt that may lead to substance use. Several participants reported cases of young people, after early successes, developing a gambling dependency, spending borrowed money and falling into cycles of indebtedness. Some turn to unlawful and unethical practices to fund their addiction, for example robbing family and friends.

3.4 Legal challenges and regulatory inefficiencies in Bangladesh

The study exposed some important legal voids in Bangladesh's legal regime on cybercrimes, more specifically on online betting and related offences including fraud, financial abuse and money laundering. Theoretically, there are laws against gambling enterprise; however, it is impossible to enforce them, penalties are insufficient and the systems are prone to corruption. People stressed that complex and inadequate complex legislation encouraged criminals, so persons involved in unlawful illegal gambling networks acted with no sanctions.

Modern law enforcement agencies lack knowledge and funds to monitor, investigate and prosecute digital gambling operators. Participants explained that, often, the authorities did not know who to arrest, since the culprits tend to work from other countries or under fake accounts. Almost every platform uses offshore financial systems and encrypted communication lines, as well as fake identities to mask operations, and therefore no one can be prosecuted under the current legislation.

One respondent elaborated:

> *'Most of these gambling websites are based in foreign countries. Even if we know what's happening, local authorities don't have the tools or international connections to shut them down.'*

This is made worse by corruption within the system whereby offenders can get themselves let off the hook by paying a bribe or using political influence. People interviewed agreed that, even when people were apprehended, the sanctions were light, and many were set free without major consequence. This lack of deterrence not only emboldens gambling operators but also hurts society's confidence in the legal and judicial institutions of the land.

One agent pointed out:

> *'If someone gets caught running a gambling operation, they just pay a bribe to the police, and everything goes away. The people at the top know they won't be punished, so they don't stop.'*

A judicial backlog and slow legal procedures in Bangladesh add to these issues. Fraud and cybercrime cases usually take a long time to come to court; by the time the culprits are apprehended, their networks have had time to pack up and move.

4. Discussion

The study discovered that most online gambling sites were fake, defrauding customers by promising hefty profits that most do not pay. This confirms the findings of Sultana et al. (2021), who argue that gambling platforms are manipulative, acting only to take advantage of their users. However, this study builds on this understanding by also finding that this has impacts on agents also, who are usually in the dark regarding these scams, and lose their credibility and capital as the main big operators take off with the money. The result is that fraudulent gaming networks are parasitic of not only gamblers but also agents, as they undermine confidence between agents and within local communities.

The study reveals that online gambling is a front through which money laundering is facilitated using unregulated MFS, virtual wallets and international remittances. These findings support several similar international studies, including by Holt et al. (2023), who noted that online gambling was a popular choice among cybercriminals when engaging in money laundering given its high level of convenience but also complexity. Financial institutions operating in the Bangladeshi environment do not have adequate tools to monitor and track these transactions. The cross-border nature of operations only adds to the problem of enforcement, as Hossain (2024) has noted. Thus, this study emphasises the need for international co-operation and the strengthening and establishment of efficient financial supervision tools.

Public discussion forums are influential ways to advertise online gambling, as well as to approach the target audience, including students and unemployed youth. Balhara et al. (2024) also highlight the part played by social media in the socialisation of young people to gambling behaviours. Holt et al. (2013) present examples of money laundering on social media. This study heard of raffle schemes, for instance closed communities in WhatsApp and unregistered Facebook pages, with promises of 'easy win' results. These platforms normalise gambling, which points to the need for increased scrutiny of content shared on social media and increased efforts to promote digital literacy to counter misguided information.

This study aimed to establish the status of Bangladesh's legal provisions in relation to prohibiting and combating online gambling and related enforcement measures. It found that the country's law and enforcement structures are unable to effectively address the issue of online gambling. Participants mentioned major barriers to the implementation of effective action, including corruption. These findings support Rahman et al. (2014), who claim that weak enforcement provides support for unlawful actors. Nevertheless, our research gives comprehensive insights into how these gaps manifest in practice. For instance, small agents are targeted while the big operators are left alone, and police forces cannot tackle the cross-border crisis. These issues point to a larger call for synergy in legal transformation policies and the strengthening of the personnel in law enforcement authorities.

Elbanna and Nirwana (2025) point out that online gambling leads to financial and emotional losses for the victims, especially those from vulnerable groups. Our research contributes to this body of literature by showing how agents are also victimised, leading to credibility and trust issues.

Thus, this research builds on Balhara et al. (2024), who focus on the recruitment of Bangladeshi citizens to gambling through social media advertisements, which requires specific regulatory approaches. It also builds on Rahman et al. (2014), in calling for improvements in the law and its enforcement. Extending the focus to emphasise agents enhances the theoretical value of these insights.

5. Conclusion

This study has found a growing overlap of cybercrime, financial fraud and online gambling in Bangladesh, leading to significant economic, social and regulatory concerns. Despite stringent legal prohibitions on gambling in the country, the absence of effective enforcement mechanisms and regulatory oversight has facilitated the proliferation of the online gambling industry, resulting in widespread financial losses, fraudulent activities and money laundering. Inadequate governance, technological vulnerabilities and social media misuse have exacerbated the issue, impeding the monitoring and control of illicit gambling networks.

A key revelation of this study is the role of online gambling in facilitating financial fraud and money laundering. Criminal networks exploit MFS, cryptocurrency transactions and offshore platforms to conceal illicit funds, creating an opaque system that is challenging for authorities to trace. The absence of stringent financial monitoring regulations and limited cybersecurity infrastructure mean these illegal transactions can go ahead largely unchecked. Local gambling agents, often unaware of the broader criminal activities they are involved in, inadvertently become facilitators of these fraudulent schemes.

The study also exposes systemic failures in law enforcement and governance, including corruption, bureaucratic inefficiencies and a lack of technical expertise in handling cyber-related financial crimes. Even when gambling operators are identified, they often evade legal consequences, using political connections or bribery, undermining public trust in the legal system. The current legislative framework is outdated and fails to address the digital complexities of online gambling, leaving a critical gap in regulatory enforcement.

To address these challenges, immediate policy and legal interventions are necessary. The government must introduce new legislation that explicitly criminalises online gambling, strengthens financial monitoring systems and ensures stricter oversight of mobile payment transactions. Additionally, cross-border co-operation is essential to track and dismantle international gambling networks operating in Bangladesh. Law enforcement agencies should be equipped with advanced cybersecurity tools and trained personnel to effectively investigate and prosecute cyber-financial crimes.

Public awareness campaigns are equally important to educate individuals about the risks of online gambling, fraudulent platforms and financial scams. Digital literacy programmes should be implemented, particularly targeting youth and vulnerable groups, to reduce their susceptibility to online gambling schemes. Furthermore, social media platforms should be held accountable for enabling gambling advertisements and facilitating illegal financial transactions.

In conclusion, a multifaceted approach combining legal reforms, financial oversight, technological enforcement and public awareness is crucial to curbing the rapid rise of cybercrime and financial fraud linked to online gambling in Bangladesh. Without swift action, these challenges will continue to threaten the country's economic stability, social fabric and digital security, making it imperative for stakeholders to implement robust regulatory measures and proactive enforcement strategies.

References

Balhara, Y.P.S., Gulati, D.D.K. and Rajguru, A.J. (2024) 'Fantasy Sports as Gaming or Gambling? Perception, Attitudes, and Engagement Behavior of College Students'. *Indian Journal of Psychological Medicine* 46(1): 60–65.

Banks, J. (2017) 'Internet Gambling, Crime and the Regulation of Virtual Environments'. In J. Banks (ed.) *Gambling, Crime and Society* (pp. 183–223). Basingstoke: Palgrave Macmillan.

Bonik Barta (2023) 'Billions of Taka Laundered Through Online Gambling: 4 Agents Arrested'. 16 August. https://shorturl.at/4XVYC

Braun, V. and Clarke, V. (2013). *Successful Qualitative Research: A Practical Guide for Beginners*. Thousand Oaks, CA: Sage.

Castleberry, A. and Nolen, A. (2018) 'Thematic Analysis of Qualitative Research Data: Is It as Easy as It Sounds?' *Currents in Pharmacy Teaching and Learning* 10(6): 807–815.

Chambers-Jones, C. and Hillman, H. (2014) *Financial Crime and Gambling in a Virtual World: A New Frontier in Cybercrime*. Cheltenham: Edward Elgar Publishing.

Creswell, J.W. and Creswell, J.D. (2017). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Thousand Oaks, CA: Sage.

Dhillon, G. and Miin, N.Y. (2013) 'The Regulations and Control of Online Betting in Malaysia'. *UUM Journal of Legal Studies* 4: 79–97.

Elbanna, M. and Nirwana, A. (2025) 'Analysing the Role of Conti Entertain as a Gateway to Digital Gambling Among Teenagers Sharia Perspective: Challenges and Solutions'. *Demak Universal Journal of Islam and Sharia* 3(1): 1–12.

Gainsbury, S., Parke, J. and Suhonen, N. (2013) 'Consumer Attitudes Towards Internet Gambling: Perceptions of Responsible Gambling Policies, Consumer Protection, and Regulation of Online Gambling Sites'. *Computers in Human Behavior* 29(1): 235–245.

Holt, T., Kulkarni, Y. and Shah, S. (2023) 'Similarities and Differences between the Neurobiology of Gambling and Substance Addiction'. *Archives in Neurology & Neuroscience.*

Hosain, M., Islam, M. and Rahman, M. (2024) 'Online Betting Addiction in Higher Education: Effects on Academic and Mental Health'. *International Journal of Research and Scientific Innovation* XI: 14–20.

Hossain, J. (2024) 'Online Gambling: Exploring the Academic, Social, and Mental Health Consequences of Online Gambling Among University Students in Bangladesh'. https://doi.org/10.13140/RG.2.2.35373.05604

Huang, R.-T., Shih, C.-H., Lin, T.-C. and Lin, W.-Y. (2022) 'The Study on Illegal Online Gambling Investigation in Taiwan'. *Procedia Computer Science*, 207: 2901–2910.

Kuzmenko, O., Boyko, A. and Dotsenko, T. (2022) 'Risk of Legalization of Funds by Bank Clients from Gambling Conducted on the Internet: Approaches to Measurement'. *Visnik Sums'kogo Deržavnogo Universitetu* 31–41. https://doi.org/10.21272/1817-9215.2022.3-3

McMullan, J.L. and Rege, A. (2010) 'Online Crime and Internet Gambling'. *Journal of Gambling Issues* 24(5): 54–85.

Patton, M.Q. (2002) *Qualitative Research & Evaluation Methods*. Thousand Oaks, CA: Sage.

Prakash, P., Girdhar, S. and Jose, A. (2024) 'Online Gambling Addiction: A Study Among College Students of Kerala State, India'. *Pakistan Journal of Criminology* 16(2). https://doi.org/10.62271/pjc.16.2.929.942

Prothom Alo (2020) 'HC Declares All Sorts of Gambling Illegal'. 10 February. https://en.prothomalo.com/bangladesh/HC-declares-all-sorts-of-gambling-illegal?utm_source=chatgpt.com

Rahman, A.S., Xu, J. and Potenza, M.N. (2014) 'Hippocampal and Amygdalar Volumetric Differences in Pathological Gambling: A Preliminary Study of the Associations with the Behavioral Inhibition System'. *Neuropsychopharmacology* 39(3): 738–745.

Smith, A.D. and Rupp, W.T. (2005) 'Service Marketing Aspects Associated with the Allure of e-Gambling'. *Services Marketing Quarterly* 26(3): 83–103.

Sultana, S., Mozumder, M.M.H. and Ahmed, S.I. (2021) 'Chasing Luck: Data-driven Prediction, Faith, Hunch, and Cultural Norms in Rural Betting Practices'. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*: 1–17.

The Daily Star (2024) 'Investigating Online Gambling Complicated as There's No Clear Law'. 30 June. www.thedailystar.net/news/bangladesh/crime-justice/news/investigating-online-gambling-complicated-theres-no-clear-law-3645706

UNB (United News of Bangladesh) (2024) '50 Lakh People Involved in Online Gambling'. 24 June. https://unb.com.bd/category/Bangladesh/50-lakh-people-involved-in-online-gambling-palak/137975?fbclid=IwZXh0bgNhZW0CMTEAAR3F8d9SP1x5j8DMMKgnb95ntDEYROhWD03f4uzxBYEHySJhWeyZTZfTjyQ_aem_8Bleqt5CN3oww44dQMNMPw

Wahyuni, D. (2012) 'The Research Design Maze: Understanding Paradigms, Cases, Methods and Methodologies'. *Journal of Applied Management Accounting Research* 10(1): 69–80.

About the authors

Mahfuzul Mithun (m.mithunpad@gmail.com) is a graduate Master's student of Public Administration at Shahjalal University of Science and Technology, Sylhet, Bangladesh. His research focuses primarily on cybercrime, online betting and security administration.

Md Masudul Islam Khan (corresponding author: masudulik@gmail.com) completed his Bachelor of Social Science in Public Administration at Shahjalal University of Science and Technology, Sylhet, Bangladesh. He has published several articles in reputed journals. His research interests include policing, gender-based violence and women in organisations.

Md Habibur Rahman (rahman94.mh@gmail.com) has a Bachelor of Social Science in Public Administration from Shahjalal University of Science and Technology, Sylhet, Bangladesh. His research interests include governance and security administration, cybersecurity and sustainable development.

The Commonwealth

Contents

Editorial 1

Nkechi Amobi

The Use and Legality of Honeypots, Tracers and Trackers in Active Cyber Defence 5

Brendan Walker-Munro, Andrew Cox, Grant Haroway, Joe Otway, Duncan Unwin and Sascha Dov Bachmann

Strengthening Nigeria's Cyber Frontier: Building Cybersecurity Resilience Through Legal Innovation 27

Iheanyi Samuel Nwankwo

Cybersecurity Threats to Critical Energy Infrastructure in India: Challenges, Opportunities and Insights for Developing Nations 53

Rohini Haridas, Satish Sharma, Rohit Bhakar[2] and Chenghong Gu

Strengthening Cybersecurity and Data Protection Frameworks in Commonwealth Member Countries: Policy and Institutional Approaches 79

Otshepeng Mazibuko

Child Protection in the Digital Age 97

Mohamed Hemdani

Cyberstalking and Technology-Facilitated Intimate Partner Violence: A Review of Three African Countries 119

Chioma Andeh

Nexus between Cybercrime Financial Fraud and Online Gambling in Bangladesh 145

Mahfuzul Mithun, Md Masudul Islam Khan and Md Habibur Rahman