International Journal of Law and Societal Studies
ISSN: 3079-2614
DOI: https://doi.org/10.61424/ijlss.v3i2.921
Journal Homepage: https://bluemarkpublishers.com/index.php/IJLSS

IJLSS
BLUEMARK PUBLISHERS

| RESEARCH ARTICLE

Strengthening the Nexus between Criminology and Cybersecurity

Fosu Bora
Ghana Police Service, National Police Headquarters-Accra/Accra Metropolitan University-Ghana
Corresponding Author: Fosu Bora, **E-mail**: borafosu@gmail.com

| ABSTRACT

Cybercrime is broadly defined in criminological literature as an umbrella concept that includes both conventional offences committed through digital means and offences that can only exist within networked environments. The former category, often termed 'cyber-enabled crimes', involves traditional crimes such as fraud and theft that are facilitated by technology, while the latter, 'cyber-dependent crimes', refers to acts like hacking and malware distribution that are intrinsic to digital systems. Similarly, cybersecurity operates as an expansive and interdisciplinary domain encompassing both academic research and applied practice. Within computer science and information security, it is generally understood as the set of policies, procedures, technologies, and behaviours aimed at safeguarding data, networks, systems, and digital infrastructure from unauthorised access, alteration, or disruption (NIST, 2018). Beyond its technical scope, cybersecurity has gained prominence across subnational, national, and international governance structures as states and institutions respond to escalating digital threats and transnational cyber risks. The relationship between cybercrime and cybersecurity has become increasingly interwoven. Cybercrimes are frequently framed as direct threats to cybersecurity, a development that has contributed to the growing involvement of national security institutions in cybercrime prevention, detection, and response activities. Despite these developments, however, the fields of cyber criminology and cybersecurity remain largely segmented in both theoretical and practical terms, thereby limiting opportunities for meaningful interdisciplinary engagement and knowledge exchange. This article adopts a conceptual and interdisciplinary analytical approach, drawing on existing criminological, cybersecurity, and security governance literature to examine the relationship between cybercrime and cybersecurity. It synthesises key theoretical perspectives and applies Brodeur's (2010) distinction between "high" and "low" policing as an analytical framework to explore the convergence of crime control and security governance in cyberspace. The article argues that stronger intellectual and operational linkages between cyber criminology and cybersecurity are necessary to effectively respond to the evolving nature of digital threats. Within Brodeur's framework, cybercrime is positioned at one end of the continuum, traditionally associated with the functions of low policing, while cybersecurity is situated at the opposite end, increasingly aligned with high-policing institutions concerned with intelligence, national security, and strategic risk management. By situating cybercrime and cybersecurity within a unified analytical framework, the article highlights the increasingly blurred boundaries between crime control and security governance in digital environments. This perspective contributes to a more integrated understanding of contemporary cyber threats and underscores the need for closer collaboration between cybercrime and cybersecurity researchers, policymakers, and practitioners. Ultimately, the article advances a unifying approach that promotes cross-fertilisation between the two fields and supports the development of more comprehensive and coherent responses to emerging challenges in cyberspace.

| KEYWORDS

Cybercrime; Cybersecurity; Cyber Criminology; High and Low Policing; Security Governance; Interdisciplinary Research

| ARTICLE INFORMATION

ACCEPTED: 09 May 2026 **PUBLISHED:** 05 July 2026 **DOI:** https://doi.org/10.61424/ijlss.v3i2.921

1. Introduction

Cybercrime and cybersecurity have emerged as some of the most pressing social, political, and economic challenges of the digital era. Cybercrime is commonly used as an umbrella term that covers two distinct categories: cyber-enabled crimes, which are traditional offences facilitated or enhanced through networked technologies, and cyber-

dependent crimes, which could not exist without digital networks and information technologies (McGuire and Dowling 2013; Wall 2001). Criminological scholarship has focused mainly on cyber-enabled offences, with less attention paid to the policing and regulatory responses to these activities. Research in this area is broadly located within the field of cyber criminology (Grabosky 2016). Cybersecurity, by contrast, is a broad and inherently multidisciplinary field of both research and practice. Within computer science and information security, it generally refers to the policies, processes, and practices designed to protect data, networks, and information systems from unauthorised access, misuse, disruption, or exploitation (Carley 2020; Fichtner 2018). Cybersecurity applies across multiple domains, from personal devices and household networks through to organisational systems and critical national infrastructure. Yet, like the broader concept of security itself, cybersecurity remains a contested and evolving term that is understood differently across institutional, professional, and disciplinary contexts.

The increasing securitisation of cybersecurity has become a defining feature of contemporary digital governance (Kremer, 2014). Indeed, cybersecurity can be understood as the convergence of traditional computer security concerns with broader processes of securitisation (Hansen & Nissenbaum, 2009). This transformation reflects a shift from a purely technical focus on system protection toward a security-oriented discourse that frames cybersecurity as an issue of national security, strategic competition, and societal resilience. Within this framing, a wide range of threats—including state-sponsored espionage, cyberterrorism, critical infrastructure attacks, and cybercrime—are increasingly incorporated into cybersecurity agendas.

As cybercrime becomes progressively framed as a cybersecurity concern, institutions traditionally associated with national security have assumed an expanding role in cybercrime prevention and response. Intelligence agencies, defence institutions, and national cybersecurity authorities are now actively engaged in addressing activities that were once considered primarily matters for law enforcement. At the same time, states themselves may also constitute threats to cybersecurity through practices such as excessive surveillance, intrusive monitoring, and restrictions on digital freedoms. Consequently, cybersecurity has evolved into a complex governance field concerned not only with protecting digital infrastructures—including communication, financial, transportation, and governmental systems—but also with regulating relationships between states, organisations, and individuals in digital environments (Fichtner, 2018). Increasingly, individuals and private organisations are also expected to assume responsibility for cybersecurity through everyday practices of risk management and digital hygiene.

Given that both cyber criminology and cybersecurity are concerned with understanding and responding to harms within digital environments, one might expect substantial overlap between the two fields. However, closer examination reveals that they have largely developed as distinct intellectual and professional domains. Each field is characterised by different conceptual foundations, research priorities, methodological approaches, publication ecosystems, and professional trajectories. As a result, opportunities for meaningful interdisciplinary engagement remain limited despite the increasingly interconnected nature of cyber-related phenomena.

This article argues that cyber criminology and cybersecurity need greater conceptual integration. It builds on Valverde's 2011 argument that security is best understood through the practices carried out in its name, rather than through abstract theoretical definitions alone. This means attention must go beyond theorising security to also examine the practical realities of how security is governed. These practices are shaped by different institutional logics, operational scales, and governance objectives, all of which affect how cyber threats are identified, prioritised, and managed. The article develops this argument in two stages. First, it traces the historical development of cyber criminology and cybersecurity as distinct but interrelated fields. This analysis shows why the two have diverged and where there are opportunities for stronger interdisciplinary engagement. Second, the article examines the relationship between cybercrime and cybersecurity, with a focus on cyber harms and the actors responsible for preventing and controlling them. Drawing on Brodeur's 2010 distinction between "high" and "low" policing, it treats crime and security as points on a continuum rather than separate domains. At one end sits crime, traditionally linked to low-policing functions, and at the other sits security, more closely tied to high-policing institutions and national security apparatuses. Between them lies an increasingly important space where crime and security overlap. Many current cybersecurity challenges fall within this middle zone, with direct implications for governance, regulation, and institutional responsibility. The article concludes by reflecting on these points of convergence and

considering what they mean for future research, policy development, and interdisciplinary collaboration across the wider cyber domain.

2. Cyber-criminology and Cybersecurity: Divergent but Interconnected Fields

Cyber criminology and cybersecurity have largely developed as separate academic fields, which means their researchers, theoretical frameworks, and publication outlets have had limited interaction. This separation stems mainly from their different intellectual roots and epistemological foundations. Cybersecurity has grown out of computer science, engineering, and information systems, while cyber criminology has developed within criminology and the broader social sciences. As a result, the two fields tend to work from different theoretical assumptions, methodological approaches, and analytical priorities.

These divergences are further reinforced by differences in conceptual focus and institutional orientation. Cybersecurity tends to emphasise technical systems, risk mitigation, and the protection of digital infrastructures, whereas cyber-criminology is more concerned with understanding deviant behaviour, victimisation, policing responses, and the social contexts in which cyber offences occur. Consequently, each field privileges different forms of evidence, ranging from computational and systems-based datasets in cybersecurity to qualitative, quantitative, and socio-legal analyses in cyber-criminology.

In addition, the logics, spatial scales, temporal horizons, and institutional jurisdictions that shape each field differ considerably. Cybersecurity frequently operates within fast-moving, real-time environments characterised by rapid threat detection and response cycles, often aligned with national security imperatives and organisational risk management frameworks. By contrast, cyber-criminology tends to adopt longer analytical timeframes, focusing on patterns of offending, structural inequalities, and the broader evolution of cyber-related harms within society.

These distinctions have contributed to the development of relatively parallel academic and professional communities, with limited cross-fertilisation despite addressing overlapping phenomena. Nevertheless, such separation obscures the increasingly interconnected nature of cyber harms, where technological vulnerabilities, criminal motivations, and security responses are deeply intertwined. Understanding this convergence requires a more integrated analytical lens that recognises both the technical and social dimensions of cyber phenomena.

Accordingly, examining the historical and intellectual trajectories of both fields is essential for understanding the roots of this divergence, while also identifying opportunities for greater interdisciplinary engagement in addressing contemporary cyber challenges.

3. Cybercrime and the Criminological Tradition

The earliest recorded uses of computers and digital networks for illegal purposes appeared soon after they were introduced into organisations in the 1960s (Parker 1976). At that time, computers were mainly isolated mainframe systems that were not yet connected to networks. As a result, early cybercrime took the form of insider offences, where individuals used privileged access within organisations to commit unlawful acts (Brenner 2007).

The spread of personal computers in the 1980s, followed by the commercial growth of the internet in the 1990s, fundamentally changed the cybercrime landscape. These developments opened up new opportunities for offending. Technically skilled individuals began creating malicious software, while financially motivated actors increasingly targeted weaknesses in digital payment systems and online trust relationships (Brenner 2007; Grabosky 2016; Lusthaus 2018). Since then, digital technologies have become embedded in almost every part of social and economic life. This widespread integration has continually expanded the range of opportunities for criminal innovation. As personal computing moved from specialised labs into homes and offices, offending shifted from isolated insider acts to more distributed forms of crime. The internet's commercialisation in the 1990s accelerated this shift by connecting users, businesses, and financial systems at scale. That connectivity lowered barriers to entry for offenders and created new markets for stolen data, fraud, and other illicit services. At the same time, organisations and individuals came to rely on digital platforms for communication, commerce, and record-keeping, which increased both exposure and potential rewards for cybercriminals. The result has been a steady expansion in the types of cyber offences, the tools used to commit them, and the actors involved. What began as niche technical

exploits has evolved into a diverse ecosystem of cybercrime that mirrors and exploits the structure of legitimate digital activity (Brenner 2007; Grabosky 2016; Lusthaus 2018).

One of the first challenges for criminologists was how to place cybercrime within existing criminological frameworks. Scholars debated whether cybercrime was a fundamentally new type of offending that needed entirely new theories, or whether it was simply a technological extension of traditional crime — the familiar "old wine in new bottles" debate (Grabosky 2001).

To address this conceptual challenge, cyber criminologists developed typologies that could account for both traditional crimes carried out through technology and new forms of offending that exist only in digital environments. Most current classifications draw a distinction between cyber-enabled crimes and cyber-dependent crimes, while some scholars add a third category of cyber-assisted offences (McGuire and Dowling 2013; Grabosky 2016; Levi et al. 2015; Wall 2017). Cyber-enabled crimes involve conventional offences such as fraud, theft, or harassment that are made possible or easier through digital tools. Cyber-dependent crimes, by contrast, can only occur within computer networks and would not exist without them, such as malware attacks, hacking, or denial-of-service incidents. Cyber-assisted offences sit between these poles, referring to crimes where technology plays a supporting role but is not essential to the offence. While these classifications have been useful for organising the field, they also reveal how fluid and evolving cybercrime is as a concept. Technological innovation constantly changes the relationship between crime and technology. New tools, platforms, and methods create novel forms of offending and stretch existing categories. What counts as cyber-dependent today may become cyber-enabled tomorrow as technologies diffuse and offender tactics adapt. This means cybercrime cannot be treated as a fixed concept. It requires ongoing theoretical refinement as digital environments and criminal practices shift (McGuire 2020; Powell et al. 2018). The difficulties in defining cybercrime also create problems for measurement and analysis. Traditional crime statistics were designed to capture physical offences and often fail to record the digital dimension of offending. Many cyber-enabled crimes are still logged under their substantive offence category — for example, fraud or theft without noting that a computer or network was used to commit them. This masks the scale and nature of technology-facilitated crime and makes it hard to compare trends over time or across jurisdictions. The growing integration of online and offline activities further complicates the picture. Many offences now move across digital and physical spaces, blurring the line between cybercrime and conventional crime (Levi 2017; Roks et al. 2020). A fraud may begin with a phishing email, continue through phone calls, and end with cash withdrawal at an ATM. When crime is hybrid in this way, simple binary classifications break down. As a result, researchers struggle to produce reliable estimates of cybercrime prevalence and impact. To fill these gaps, researchers often rely on estimates and datasets produced by private cybersecurity firms. These organisations collect large volumes of data on malware, intrusions, and fraud from their clients and security products. While valuable, this data does not always meet strict scientific standards. Collection methods vary, coverage is uneven, and firms may have commercial incentives that shape what they report (Florêncio et al. 2014). Public agencies and academic studies therefore face a trade-off between using incomplete official statistics and relying on industry data with limited transparency. This measurement challenge has direct consequences for policy and practice. Without accurate data, it is difficult to assess which types of cybercrime are growing fastest, which groups are most at risk, or which interventions are most effective. It also affects how resources are allocated between policing, regulation, and prevention. If cyber-enabled fraud is undercounted because it is recorded as general fraud, policymakers may underestimate the role of digital platforms in enabling harm. If cyber-dependent attacks are measured mainly through industry reports, academic understanding may be skewed toward threats that affect corporate clients more than individuals or small organisations. Addressing these issues requires better conceptual clarity and stronger data infrastructure. Typologies need to remain flexible enough to capture new forms of offending, while measurement systems must be designed to record both the offence and the technological means used to commit it. Collaboration between researchers, law enforcement, and the private sector will be essential to improve the quality and coverage of cybercrime data (McGuire 2020; Powell et al. 2018; Florêncio et al. 2014). Until then, our understanding of cybercrime will remain partial and evolving, shaped as much by what we can measure as by what offenders actually do.

Despite these challenges, cyber-criminology has produced important empirical insights. Researchers have examined offender behaviour in online forums, illicit marketplaces, and digital communities, providing detailed analyses of trust, reputation, criminal entrepreneurship, and underground market dynamics (Holt, 2017; Pastrana et al., 2018; Rossy & Décary-Hétu, 2018). Other studies have focused on pathways into cyber-offending, victimisation experiences, and law enforcement responses (Brewer et al., 2018; Button & Cross, 2017; Fox & Holt, 2020; Harkin et al., 2018; Holt & Bossler, 2012). Theoretically, cyber-criminology has remained strongly influenced by established criminological perspectives, including routine activity theory, social learning theory, general strain theory, deterrence theory, and the general theory of crime (Bossler, 2020).

4. Cybersecurity: From Technical Protection to Security Governance

The development of cybersecurity has followed a markedly different trajectory. Although cybersecurity has not yet emerged as a fully autonomous academic discipline, it has developed into a rapidly expanding interdisciplinary field situated at the intersection of computer science, engineering, political science, and security studies (Carley, 2020). The evolution of terminology from "computer security" to "information security" and, more recently, to "cybersecurity" reflects a gradual broadening of scope from the protection of individual machines to the governance of complex digital ecosystems and the social, economic, and political institutions that depend upon them (Landwehr, 2010).

Unlike cyber-criminology, cybersecurity research remains largely dominated by computer scientists and engineers. As a result, the field has traditionally focused on identifying technical vulnerabilities, designing defensive mechanisms, and securing information systems against unauthorised access and exploitation. However, increasing recognition of the human and organisational dimensions of cyber risk has gradually encouraged greater engagement with behavioural sciences, organisational studies, and human computer interaction research (Briggs et al., 2017; Moore, 2010).

Cybersecurity has also become closely intertwined with national security agendas. The military and strategic origins of internet infrastructure have contributed to a policy environment in which digital threats are frequently framed as existential risks requiring exceptional responses from intelligence, military, and defence institutions (Castells, 2002; Kremer, 2014). This securitisation process has expanded the scope of cybersecurity beyond technical system protection to include concerns such as espionage, cyberterrorism, geopolitical competition, and the safeguarding of critical infrastructure (Hansen & Nissenbaum, 2009). Consequently, cybersecurity increasingly occupies a central position within contemporary governance and security architectures.

From an empirical perspective, cybersecurity research has developed advanced methodologies for measuring cyber risk and assessing system vulnerabilities. Through automated data collection systems, machine learning techniques, incident reporting platforms, and large-scale digital datasets, researchers have generated valuable insights into evolving threat landscapes and organisational weaknesses (Woods & Böhme, 2020). Nevertheless, these technical advances have not always translated into deeper theoretical engagement with criminological questions surrounding offending behaviour, victimisation dynamics, and crime prevention strategies.

5. Bridging the Divide

Despite addressing many of the same underlying harms, cyber-criminology and cybersecurity continue to operate largely as separate academic fields. Cyber-criminology primarily concentrates on offenders, victims, and criminal justice responses, whereas cybersecurity focuses on system vulnerabilities, risk management, and the protection of digital infrastructures. This disciplinary separation has limited opportunities for sustained intellectual exchange, methodological integration, and interdisciplinary collaboration.

The consequences of this divide are becoming increasingly evident. Cybersecurity scholarship often underutilises criminological insights relating to offending behaviour, crime prevention, deterrence strategies, victimisation processes, and the structure of criminal networks. Conversely, cyber-criminology has been comparatively slower in incorporating advances in data analytics, automated threat detection systems, and evolving technical understandings of cyber risk. As cyber threats become more complex, adaptive, and interconnected, maintaining rigid disciplinary boundaries becomes increasingly difficult to justify both analytically and practically.

Accordingly, there is a growing imperative to integrate criminological and cybersecurity perspectives. Such integration would enable a more comprehensive understanding of cyber harms, enhance the design of prevention and intervention strategies, and strengthen institutional responses to emerging digital threats. Rather than treating cybercrime and cybersecurity as separate domains, they should be conceptualised as interdependent components of a broader cyber governance ecosystem. This reconceptualization provides a foundational basis for examining how contemporary security institutions are increasingly converging in their governance of digital risks and cyber-related harms.

6. Appreciating the Relational Dynamics of the Cyber Field

6.1 Intersecting Cyber Harms

The diverse range of cyber-related harms constitutes a primary concern for the various institutional actors operating within the broader cyber field. Rather than attempting a comprehensive mapping of these actors which would largely result in a descriptive exercise the emphasis here is on the relational dynamics that connect them. These relationships are significant because cyber harms rarely fall neatly within the jurisdiction of a single institution, sector, or governance framework. Instead, they emerge across overlapping domains of crime control, national security, intelligence operations, risk management, and digital governance.

Several scholars have sought to classify cybercrime and cybersecurity threats in order to provide conceptual clarity and inform policy responses (e.g. Agrafiotis et al., 2018; de Bruijne et al., 2017). Such classifications are valuable insofar as they help to structure thinking around the distribution of responsibilities, capabilities, and governance functions across different institutional actors. However, these typologies should be understood as analytical starting points rather than definitive or fixed categories. The cyber environment is characterised by rapid technological change, evolving threat landscapes, and increasingly blurred boundaries between different forms of harm. As such, rigid classifications often struggle to adequately capture the complexity of contemporary cyber threats.

Australia's most recent Cyber Security Strategy highlights this challenge by grouping cyber threats into four broad categories: financially motivated criminals, issue- or politically motivated actors, terrorist and extremist actors, and state-sponsored actors or nation states (Australian Government 2020). Traditionally, the first two categories are treated as cybercrime, while the last two are placed within cybersecurity and national security frameworks. In practice, however, these distinctions often hide important areas of overlap. The motivations, capabilities, and impacts of cyber actors frequently cut across these simplified categories.

For instance, financially motivated cybercriminals may range from relatively unsophisticated offenders engaging in low-level fraud to highly organised criminal enterprises capable of targeting major financial institutions and critical infrastructure. In such cases, the consequences of criminal activity may extend beyond individual victimisation to produce systemic economic disruption and broader societal harm (Bouveret, 2018). Similarly, issue- or politically motivated actors may engage in activities ranging from symbolic hacktivism and online protest to operations capable of undermining public trust, disrupting essential services, or threatening national stability. What initially appears as a criminal matter may therefore escalate into a broader security concern.

The complexity of cyber harms is further intensified by the diversity of actors involved. Some incidents may be perpetrated by isolated individuals acting independently, while others involve highly structured networks operating across multiple jurisdictions. These networks may include organised criminal groups, extremist organisations, intelligence operatives, private contractors, or hybrid coalitions that defy clear categorisation within existing institutional frameworks. As a result, the distinction between cybercrime and cybersecurity increasingly becomes one of degree rather than a clear binary division.

Moreover, new threat configurations continue to emerge that challenge traditional understandings of cyber risk. The disclosure of offensive cyber tools developed by the United States National Security Agency (NSA) and the Central Intelligence Agency (CIA) provides a notable example. These tools, allegedly leaked through intelligence-related breaches, were subsequently adopted by financially motivated cybercriminals and integrated into large-scale cybercrime campaigns, effectively transforming state-developed capabilities into instruments of organised criminal activity (Trend Micro, 2019).

A similar convergence can be observed in the growing interaction between state-sponsored cyber actors and cybercriminal groups. Evidence indicates that state-linked operators engaged in espionage activities have, in some instances, sold access to compromised networks to criminal actors or conducted ransomware campaigns for financial gain (Group IB, 2020). Conversely, state-sponsored groups have also been reported to purchase network access and intelligence from cybercriminal organisations to advance strategic objectives (Global Research & Analysis Team, 2020). These developments illustrate an ongoing process of hybridisation in which the boundaries between criminal activity, intelligence operations, and national security increasingly blur.

Such realities complicate attempts to categorise cyber harms according to traditional institutional divisions. A single cyber incident may simultaneously involve elements of criminality, espionage, economic disruption, and national security risk. Consequently, the actors responsible for prevention, investigation, and response often operate across overlapping governance domains. This complexity reinforces the relevance of Brodeur's (2010) distinction between "low policing" and "high policing." While low policing is traditionally associated with crime control and law enforcement, high policing relates to intelligence gathering, state security, and the protection of strategic national interests. In cyberspace, however, these domains are increasingly intertwined.

Understanding cyber harms therefore requires moving beyond rigid distinctions between crime and security. Cyber threats exist along a continuum in which criminal, political, economic, and security dimensions frequently intersect. Appreciating these relational dynamics is essential for understanding contemporary cyber governance, as effective responses increasingly depend on cooperation among actors operating across both crime-control and national-security spheres. It is within this space of convergence that the relationship between cybercrime and cybersecurity becomes most apparent, underscoring the need for greater integration between cyber-criminological and cybersecurity perspectives.

6.2 New Cybersecurity Actors

It is therefore not surprising that cybersecurity involves a diverse set of actors that cross traditional organisational boundaries. These include policing agencies, intelligence services, defence institutions, and policy departments operating at local, national, and international levels of government. These actors differ markedly in their institutional mandates, technical expertise, and operational capacity to respond to cyber harms. Policing institutions illustrate these challenges clearly. They are widely recognised as struggling to address cybercrime, largely because they have limited technical resources and specialist staff. This problem is compounded by the nature of cyber offending itself, which is transnational, technically complex, and changes rapidly as tools and platforms evolve. Police forces are also structured around territorial jurisdictions and physical evidence, which makes investigating borderless digital crimes difficult. As a result, many cases go unreported, investigated, or are resolved through civil rather than criminal processes. In contrast, signals intelligence agencies have built substantial technical expertise in cybersecurity operations over several decades. Their core mission has always involved monitoring, intercepting, and securing communications, so they were well placed to adapt as threats moved online. Because of this capability, they have received increased funding and greater institutional prominence. Today they often serve as central actors within national cybersecurity strategies, taking responsibility for threat detection, incident response, and protection of critical infrastructure. This contrast highlights a wider issue within cybersecurity governance. Responsibility for cyber harms is spread across institutions with very different histories, cultures, and powers. Defence and intelligence agencies focus on national security threats and state actors, while police focus on individual offenders and criminal justice outcomes. Policy departments must coordinate these efforts while also balancing privacy, regulation, and public accountability. The result is a fragmented field where capabilities and priorities do not always align. Effective responses to cybercrime therefore depend not just on technical solutions, but on managing the relationships, roles, and limits of these diverse actors.

Over the past decade, and especially in the last five years, many governments have responded to the growing complexity of cyber threats by creating new organisational structures. These structures are designed to bring different capabilities together under one institutional framework. The aim of these hybrid governance arrangements is to break down the traditional silos that separate law enforcement, intelligence, defence, and policy-making bodies. A clear example is the Australian Cyber Security Centre (ACSC). It was established as a standalone agency within the Australian Signals Directorate (ASD). The ACSC brings together staff from five government agencies

covering law enforcement, criminal intelligence, security intelligence, signals intelligence, and defence. In addition, Computer Emergency Response Teams (CERTs) that were previously housed in separate policy departments were moved into the ACSC structure. The main goal of the ACSC is to act as a central hub for coordination. It focuses on information sharing and collaboration between the public and private sectors on cybersecurity. Its responsibilities cover both prevention and response to cyber threats and harms. By combining expertise from agencies with different mandates, the ACSC is intended to provide a more integrated and faster response to incidents than fragmented, standalone agencies could achieve.

Similar institutional models have appeared internationally. The United Kingdom's National Cyber Security Centre (NCSC), established in 2016, and Canada's Canadian Centre for Cyber Security, established in 2018, both operate within or alongside their national signals intelligence agencies. Like the ACSC, these centres are mandated to work with private sector stakeholders. However, formal membership structures in both cases remain limited to state actors. Alongside these institutional changes, governments have also invested heavily in cybersecurity research centres and innovation hubs. The aim is to strengthen national cyber resilience and build greater technological capability. These centres are intended to connect government, academia, and industry, so that new research and technical expertise can be translated more quickly into practical security measures.

Despite these broad similarities, important institutional differences remain across jurisdictions. For example, the ACSC's scope is arguably wider than that of its UK and Canadian counterparts. In addition to coordinating cybersecurity, it also handles cybercrime reporting. These reporting functions were previously managed by the Australian Criminal Intelligence Commission (ACIC). When cyber incident reports are submitted, they are typically categorised as originating from individuals, businesses, or government entities. Reports submitted by individuals most often relate to cybercrime incidents and are subsequently referred to relevant state police agencies for potential investigation. However, not all cases proceed to formal investigation, and many are primarily used for intelligence-gathering and situational awareness purposes. Importantly, Australia does not operate a unified national police structure for cybercrime, and responsibility for investigation remains distributed across state jurisdictions, each with distinct reporting and response mechanisms.

In contrast, the United Kingdom uses a more decentralised but coordinated model. Regional Organised Crime Units (ROCUs) are hosted by the National Crime Agency (NCA) and handle cybercrime investigations. These units are operationally linked to the National Cyber Security Centre (NCSC). Australia has also committed to building comparable multi-agency structures. However, its Joint Cyber Security Centres focus mainly on stakeholder engagement and cybersecurity coordination rather than direct cybercrime investigation. There are also differences in how public reporting is handled. In the United Kingdom, the NCSC does not run public cybercrime reporting systems. That responsibility sits with Action Fraud and the National Fraud Intelligence Bureau. While cybercrime and fraud are not the same, fraud makes up a large proportion of cyber-enabled offences reported by the public. Canada has taken a different approach. Its National Cyber Security Strategy led to the creation of a National Cybercrime Coordination Unit within the Royal Canadian Mounted Police (Public Safety Canada 2018). This unit is mandated to coordinate investigations, provide advice to local law enforcement, liaise with national and international security partners, and manage national cybercrime reporting systems (Public Safety Canada 2019).

These comparative cases demonstrate that while investment in cyber governance structures has increased across jurisdictions, institutional arrangements vary significantly in how they integrate cybercrime and cybersecurity functions. In Australia, coordination efforts are more concentrated within cybersecurity frameworks, whereas in the United Kingdom and Canada, more explicit multi-agency structures integrate both cybersecurity and cybercrime enforcement functions. Nevertheless, even within these systems, the effectiveness of coordination across subnational jurisdictions remains uneven and, in some cases, unclear.

Since the establishment of the ACSC, there has also been a notable shift toward greater public visibility of intelligence and cybersecurity agencies. Senior leadership within the Australian Signals Directorate has increasingly engaged in public communication strategies, reflecting a broader trend across the Five Eyes intelligence community in which agencies traditionally associated with secrecy now occupy more prominent roles in public cybersecurity discourse. This increased visibility reflects the growing centrality of cyber-related harms within national security

agendas and the expanding convergence between intelligence functions and public-facing cybersecurity awareness initiatives.

As a result, signals intelligence agencies historically low-profile now have a more public role. They advise businesses, critical infrastructure operators, and individual users on cybersecurity resilience and how to reduce digital risk. The ACSC, for example, runs ongoing public awareness campaigns aimed at improving cyber hygiene and lowering vulnerability to online threats. Similarly, the Australian Security Intelligence Organisation (ASIO) has launched public-facing initiatives such as "think before you link" to raise awareness of cybersecurity risks among citizens. Despite this higher visibility, the roles of these institutions remain legally and functionally separate. The ACSC sits within the Australian Signals Directorate, but its mandate is distinct from other ASD functions. It does not cover offshore intelligence collection or offensive cyber capabilities. ASIO, in contrast, has a domestic security and counterintelligence mandate that differs from traditional policing. ASD has also publicly acknowledged its role in offensive cyber operations. These include disruptions targeting terrorist networks and foreign cybercriminal groups running COVID-19-related phishing campaigns against Australian users (Australian Government 2020).

Overall, these developments illustrate the increasing convergence of intelligence, security, and cybersecurity functions within contemporary governance systems. However, they also highlight persistent institutional fragmentation and jurisdictional complexity, particularly in relation to the integration of cybercrime enforcement and cybersecurity coordination across different levels of government.

7. Blurring Boundaries across the Crime–Security Continuum

These boundaries are increasingly blurred. Recent debates have focused on whether the Australian Signals Directorate (ASD) should support offensive cyber capabilities against transnational crime networks. The discussion centres particularly on groups involved in child sexual exploitation and people smuggling (Australian Broadcasting Corporation 2020). Traditionally, these activities fall under the Australian Federal Police (AFP), which is the main federal agency responsible for investigating and prosecuting such offences. This overlap raises questions about institutional roles. Although most signals intelligence agencies across the Five Eyes alliance are legally barred from collecting intelligence within their own countries, many have provisions that allow them to assist other agencies. They can provide support to national police services or domestic security intelligence agencies when a formal request is made. As cybercrime becomes more technically complex and crosses borders, the line between foreign intelligence collection and domestic law enforcement is harder to maintain. Agencies like ASD are being asked to contribute capabilities that were once outside their core mandate. The result is growing pressure to redefine how responsibilities are divided between intelligence agencies, police, and security services in responding to serious transnational crime.

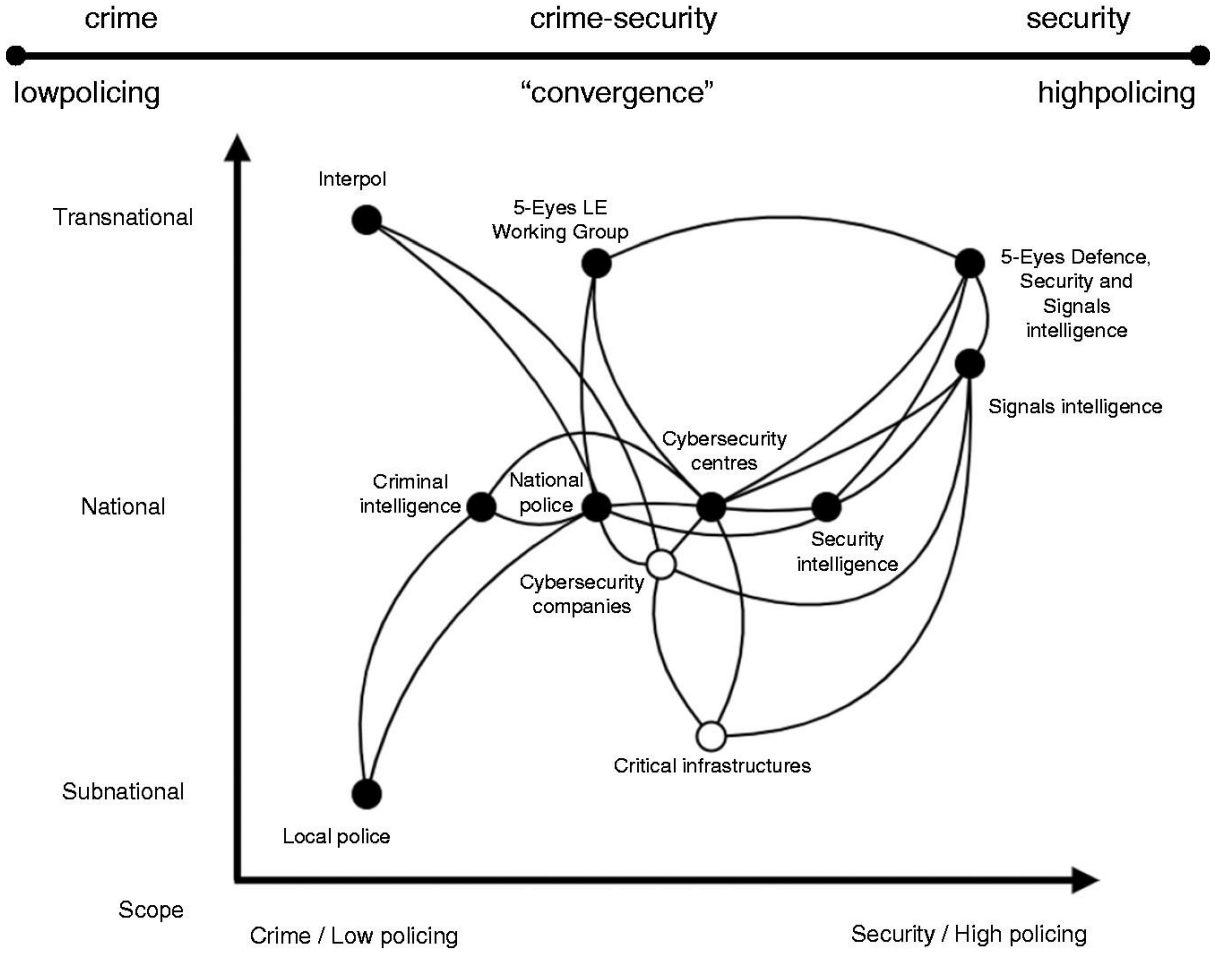
These examples reinforce the central point: cybercrime and cybersecurity threats intersect at multiple points. Importantly, this is not unique to Australia. In 2015, the United Kingdom set up a co-located Joint Operations Cell that brings together the Government Communications Headquarters (GCHQ) and the National Crime Agency (NCA) (GCHQ 2015). The Cell was initially created to disrupt online child sexual exploitation. Since then, its work has expanded to cover a wider range of serious and organised crime. This now includes fraud, money laundering, people trafficking, and different forms of illicit smuggling. This shift shows how high-policing institutions are becoming more involved in work that was once handled by lower-level policing. Agencies like GCHQ were traditionally focused on national security and foreign threats. They are now working directly with police on crimes that affect citizens domestically. The move reflects how cyber-enabled offending blurs old divisions between national security, intelligence, and criminal justice. As threats evolve, governments are relying more on collaboration between agencies that were once kept separate by mandate and culture.

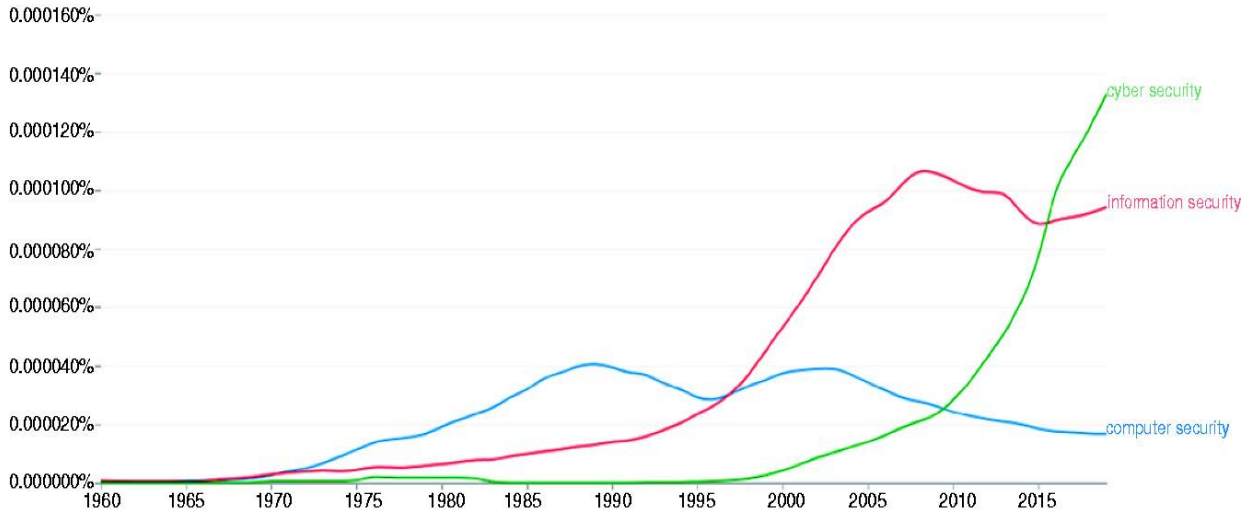
The idea of a crime security continuum helps make sense of the complexity in the cyber field. In this continuum, 'crime' sits at the low-policing end, while 'security' sits at the high-policing end. What this framing shows is that there are multiple points of overlap in the middle of the spectrum. See Figure 2. For example, de Bruijne et al. (2017) reviewed cyber threat actor typologies and identified eleven ideal-type actors: extortionists, information brokers, crime facilitators, digital robbers, scammers and fraudsters, crackers, insiders, terrorists, hacktivists, state actors, and

state-sponsored networks. They also distinguish these actors by their level of expertise, available resources, organisational structure, and underlying motivations.

While actors like state actors and state-sponsored networks are clearly cybersecurity threats, the same cannot be said for cybercrime actors. As noted earlier, financially motivated criminals often commit straightforward criminal acts. But those same actors may also target high-value systems such as critical infrastructure. In some cases, they are even recruited by state actors to carry out espionage or cyberattacks. The line between crime and security also blurs for other offences. Take child sexual exploitation. It is not only the nature of the crime that pushes it from a policing issue into a security concern. The limited capacity of police to respond to these complex, transnational activities plays a major role as well. Local forces often lack the technical resources, jurisdiction, and international partnerships needed to investigate and prosecute offenders effectively. As a result, offences that start as "crime" problems can quickly become "security" problems when institutions cannot cope.

As a result, more cyber harms are being pushed toward the middle of the crime–security continuum, and in some cases closer to the security end. This shift means the actors operating in the cyber field are deeply connected. See Figure 3 for a high-level illustration of these relationships, where black dots represent state actors and white dots represent private actors. The overlap is growing because threats no longer fit neatly into "crime" or "security" categories. Criminal groups, businesses, and state actors often use similar tools, target similar systems, and sometimes work together. When policing agencies cannot respond effectively, security and intelligence institutions step in. This pushes more activity toward the centre of the continuum and blurs the old boundaries between them.





Beyond mapping the cyber field, the crime–security continuum also has important normative implications. We argue that certain cyber harms sit firmly at either the low-policing or high-policing end, depending on their nature. This is not about how serious the harm is for victims. Victim impact can be severe at both ends of the continuum. Instead, the point is conceptual. Some harms make more sense as "crime" problems than "security" problems. When that is the case, the institutions responding to them should match their position on the continuum. In other words, policing agencies are better placed to deal with harms at the low end, while security and intelligence agencies are better placed for harms at the high end. Aligning the response this way helps avoid overreach and keeps mandates clear. It also recognises that not every cyber harm requires a national security response, even if it causes serious harm. The continuum gives us a way to sort harms and assign responsibility based on what the activity actually is, not just how damaging it looks.

In particular, we argue that police institutions, especially local police, need to engage more actively in the cyber field. Certain activities are fundamentally criminal and should stay with policing agencies. Fraud and scams targeting individuals or organisations are the clearest example. We recognise that securing successful prosecutions for these offences remains difficult. Jurisdiction issues, anonymity online, and limited technical resources make investigations complex. But the nature of the harm does not change. The same applies to other serious offences. Child sexual exploitation networks and transnational organised crime groups commit acts that cause major harm and threaten individual safety. Yet these are still classified as criminal offences, not security threats. This is similar to how we treat comparable offences in physical environments. Assault, theft, and trafficking are serious, but they remain police matters unless they cross into national security territory. Placing these harms at the "crime" end of the continuum does not downplay their impact on victims. It simply clarifies which institution is best placed to respond. Police are trained, resourced, and mandated to investigate and prosecute crime. If we shift too much responsibility to security and intelligence agencies, we risk stretching their mandate and leaving core policing functions underdeveloped. For that reason, building police capacity in cyber investigations, digital forensics, and international cooperation is essential.

In the Australian context, many of these activities are handled by relatively small specialist units. Other jurisdictions use more extensively resourced, multi-agency structures. The UK's Regional Organised Crime Units, or ROCUs, are one example. Mapping these different arrangements raises broader questions about institutions and governance. Who should be responsible for which types of cybercrime? Should local police handle some offences while national police handle others? When should policing be separated from intelligence work? Where should intelligence agencies lead instead of defence institutions? And how should international bodies like Interpol fit into cooperative responses? Answering these questions needs a deeper and more nuanced understanding of the cyber field. It also requires sustained, critical engagement with governance and accountability. As institutional roles shift and overlap, new challenges emerge around oversight, legal authority, and transparency. Without careful design, responsibilities can become blurred and accountability can fall through the gaps.

8. Conclusion

This paper is a starting point for stronger collaboration across disciplines in the study of cybercrime and cybersecurity. It shows how the two fields emerged as separate research domains. It also argues that closer integration is needed if both areas of scholarship are to move forward. We contend that cybercrime and cybersecurity have both been limited by this split. Each field can gain a lot from insights in the other. By treating them as separate, we miss important overlaps in actors, threats, and responses. The main objective of this paper has been to examine the relationship between cybercrime and cybersecurity. It also reflects on what that relationship tells us about how this complex security field should be understood and conceptualised going forward.

Ultimately, what this paper may have shown is just how large and complex this task is. Like the broader idea of 'security' (e.g. Zedner 2009), 'cybersecurity' is still a contested term. It means different things to different actors and disciplines. Various conceptions of security have developed to capture different threats and referent objects. We often distinguish between 'human security', 'national security', and 'international security', for example. If cybersecurity is treated mainly as a branch of national security, then it makes sense that political scientists focus heavily on its securitisation. But cybersecurity goes beyond narrow national security frames. Its referent objects are wide-ranging. They include individuals, organisations, and corporations of all sizes, as well as nation states and transnational networks of both state and non-state actors. Given that range, it may be worth asking whether adding more prefixes to 'cybersecurity' would actually improve conceptual clarity. More labels could help, but they could also add confusion.

The long-standing distinction between 'low' and 'high' policing (Brodeur 2010) still has analytical value at the two extremes of the spectrum. 'Low cybersecurity' can be understood as routine digital security practices. This includes protecting personal accounts, devices, and everyday systems. 'High cybersecurity', by contrast, refers to protecting government systems and critical infrastructure from sophisticated intrusions by state actors. But between these two poles is a wide range of harms. They do not fit neatly into one category. How they are classified often depends on context, the actors involved, and how institutions frame the problem.

The difficulty of clearly defining cyber-related harms also shows up in how governments and security institutions respond. Network-based cybersecurity centres have brought real benefits. They raise awareness, improve coordination, and pull resources together to respond to cyber threats across agencies and disciplines. But the scope of harms now grouped under 'cybersecurity' keeps expanding. The mandates of these centres are also becoming more diverse. Because of that, 'cybersecurity' does not always mean the same thing. Its meaning shifts depending on the context. It covers very different ground when applied to personal devices, financial institutions, or state infrastructure. Even within government, the term carries different weight. In defence and intelligence contexts, cybersecurity is about protecting sensitive and highly classified information. In other parts of government, the focus may be on routine systems and public services. The same word is being used, but the stakes and responsibilities are not the same.

Beyond definitional issues, the cybersecurity field is converging into new configurations. These blur the old boundaries between law enforcement and national security, between low and high policing, and between public and private security actors. This creates important questions about roles. Is it desirable for traditional high-policing institutions, such as signals intelligence agencies, to take on such visible, public-facing roles in cybersecurity? That question is especially relevant for cybercrime issues that are better understood as criminal problems rather than security threats. There is also a risk of distortion. When these agencies take the lead, certain categories of cyber threat can be elevated. Their perceived significance grows. At the same time, other threats that are equally important may get less attention. The cybersecurity landscape is becoming more crowded and complex, and that "crowding" can push some harms to the margins.

More specifically, when cybersecurity responses are elevated without equal attention to cybercrime risks, policy can become unbalanced. Cybercrime starts to get conflated with broader cybersecurity concerns. As a result, it loses its distinct analytical and policy focus. This dynamic is clear in high-profile cases. The Solar Winds hack on the US supply chain drew major global attention, for example. Incidents like that shift focus toward national security threats. Meanwhile, routine but widespread cybercrimes can be pushed aside. For that reason, there is a strong case

for continued, deeper scrutiny of the relationship between cybercrime and cybersecurity. Both scholars and policymakers need to keep engaging with it. This paper does not offer definitive solutions. Its aim has been to critically examine these emerging dynamics. We also hope it will stimulate more interdisciplinary research and new policy thinking in this evolving field.

8.1 Limitations of the Study

This study is conceptual in nature and therefore relies on the analysis and synthesis of existing literature rather than primary empirical data. Consequently, the proposed framework has not been empirically tested within specific institutional or national contexts. Although the article draws upon established scholarship from criminology, cybersecurity, and security studies, the interpretation of the relationship between cybercrime and cybersecurity is shaped by the available literature and the application of Brodeur's (2010) high and low policing framework. As such, the findings should be understood as theoretical propositions intended to stimulate interdisciplinary dialogue rather than as empirically validated conclusions. In addition, because cybersecurity policies, technologies, and cyber threats continue to evolve rapidly, some institutional practices and governance arrangements discussed in this article may change over time.

8.2 Suggestions for Future Research

Future research should empirically examine the conceptual relationships advanced in this article by investigating how law enforcement agencies, cybersecurity organisations, and national security institutions collaborate in responding to cyber threats. Comparative studies across jurisdictions could assess whether the convergence between cybercrime and cybersecurity varies according to legal systems, institutional arrangements, and national cybersecurity strategies. Further research could also evaluate the practical applicability of Brodeur's high and low policing framework within digital environments and explore whether alternative criminological and security theories provide complementary explanations of cyber governance. Finally, interdisciplinary empirical studies involving criminologists, cybersecurity specialists, policymakers, and practitioners would contribute to validating and refining the integrated framework proposed in this article, thereby strengthening both theory and practice in addressing contemporary cyber threats.

In addition, future studies could investigate how emerging technologies, such as artificial intelligence, machine learning, blockchain, quantum computing, and the Internet of Things, are reshaping both cybercrime and cybersecurity. These technologies present new opportunities for innovation while simultaneously creating novel forms of cyber risk that require integrated analytical approaches. Researchers may also explore the role of public–private partnerships in strengthening cyber resilience, particularly in protecting critical national infrastructure and responding to large-scale cyber incidents. Another promising area of inquiry is the development of interdisciplinary education and training programmes that combine criminology, cybersecurity, computer science, and public policy to prepare professionals for increasingly complex cyber environments. Longitudinal studies examining the evolution of cybercrime governance and institutional responses over time would further enhance understanding of how crime control and security practices continue to converge in the digital age.

Disclosure Statement: The author reports there are no competing interests to declare. The views expressed in this article are those of the author and do not necessarily reflect the official policy or position of the Ghana Police Service.

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors

References

[1] Aborisade, R. A. (2023). Yahoo Boys, Yahoo Parents? An Explorative and Qualitative Study of Parents' Disposition Towards Children's Involvement in Cybercrimes. Deviant Behavior, 44(7), 1102–1120. https://doi.org/10.1080/01639625.2022.2144779

[2] Adewopo, A., Mensah, K., & Okafor, T. (2024). Regional cybersecurity cooperation in West Africa: Legal gaps and enforcement challenges. ECOWAS Legal Studies Review, 11(1), 23–45.

[3] African Union. (2018). "Cyber Security and Cybercrime Policies for African Diplomats Cyber Security and Cybercrime Policies for African Diplomats." African Union.

[4] African Union. (2024, July 8). List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection. https://au.int/sites/default/files/treaties/29560-sl-
[5] AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf
[6] Agrafiotis I., Nurse J., Goldsmith M., Creese S., Upton D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4(1), 1–15. https://doi.org/10.1093/cybsec/tyy006
[7] Ahmad, M. A., Wisdom, D. D., & Isaac, S. (2020). An empirical analysis of cybercrime trends and its impact on moral decadence among secondary school level students in Nigeria. advances in multidisciplinary & scientific research journal publication. https://doi.org/10.22624/iSTEAMS/V26P10-IEEE-NG-TS
[8] Ajayi O, Ososami S (1998), "Nigeria: On the Trail of a Spectre — Destabilisation of Developing and Transitional Economies". Journal of Money Laundering Control, Vol. 1 No. 4 pp. 342–351, doi: https://doi.org/10.1108/eb027160
[9] Ajijiola, A., and N. Allen. (2022). "African Lessons in Cyber Strategy." African Lessons in Cyber Strategy – Africa Center for Strategic Studies.
[10] Alhassan, AR.K., Ridwan, A. Identity Expression—the Case of 'Sakawa' Boys in Ghana. Hu Arenas 6, 242–263 (2023). https://doi.org/10.1007/s42087-021-00227-w
[11] Australian Broadcasting Corporation. (2020, 19 February). Government considering bringing foreign cyber spy powers onshore to hunt Australian paedophiles. https://www.abc.net.au/news/2020-02-19/powers-for-asd-spy-dark-web-australians/11980728
[12] Ayodele, O. 2021. "The Digital Transformation of Diplomacy: Implications for the African Union and Continental Diplomacy." South African Journal of International Affairs 28 (3): 379–401. doi:10.1080/10220461.2021.1968944.
[13] Azizi, S., Pakshad, P., Shameli-Sendi, A., & Faraji Daneshgar, F. (2025). Vulnerability scoring metric of CVSS needs to be adjusted per each product: Our analysis on Linux and Apache. Information Security Journal: A Global Perspective, 1–26.
[14] Ball, K. 2017. "African Union Convention on Cyber Security and Personal Data Protection." International Legal Materials 56 (1): 164–192. doi:10.1017/ilm.2016.3.
[15] Ball, K. 2017. "African Union Convention on Cyber Security and Personal Data Protection." International Legal Materials, 56 (1): 164–192.
[16] Beskow DA, Carley KM (2019) Social cybersecurity: an emerging national security requirement, military review, March–April 2019—see https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Mar-Apr-2019/117-Cybersecurity/b/
[17] Bouke, M. A., Abdullah, A., Alshatebi, S. H., El Atigh, H., & Cengiz, K. (2023). African Union Convention on Cyber Security and Personal Data Protection: Challenges and future directions. https://arxiv.org/abs/2307.01966
[18] Business Continuity Institute. (n.d.). Digital transformation, development and resilience in West Africa. https://www.thebci.org/news/digital-transformation-development-and-resilience-in-west-africa.html
[19] Button, M., Hock, B., Suh, J.B. et al. Policing cross-border fraud 'Above and below the surface': mapping actions and developing a more effective global response. Crime Law Soc Change 83, 5 (2025). https://doi.org/10.1007/s10611-024-10186-2
[20] Calandro, E. 2021. "Partnering with Africa on Cyber Diplomacy" EU Cyber Direct.
[21] Carley, K.M. Social cybersecurity: an emerging science. Comput Math Organ Theory 26, 365–381 (2020). https://doi.org/10.1007/s10588-020-09322-9
[22] Council of Europe. (2023). GLACY+ activities in Ghana. https://www.coe.int/en/web/cybercrime/ghana
[23] Cross, C., & Lee, M. (2022). Exploring Fear of Crime for Those Targeted by Romance Fraud. Victims & Offenders, 17(5), 735–755. https://doi.org/10.1080/15564886.2021.2018080
[24] Cyber Security Authority. (2023a). Ghana signs Council of Europe Second Additional Protocol to the Convention on Cybercrime. https://www.csa.gov.gh
[25] Cyber Security Authority. (2023b). Annual cybercrime and cybersecurity report. Government of Ghana. https://www.csa.gov.gh
[26] Dawson, M., & Walker, D. (2022). Argument for improved security in local governments within the Economic Community of West African States. In Cybersecurity measures for e-government frameworks (pp. 96–106). IGI Global.
[27] Delport, J. 2021. "The State of Cybersecurity in Africa." The State of Cybersecurity in Africa - IT News Africa - Up to date technology news, IT news, Digital news, Telecom news, Mobile news, Gadgets news, Analysis and Reports.
[28] Dunch, R. 2002. "Beyond Cultural Imperialism: Cultural Theory, Christian Missions and Global Modernity." History and Theory 41 (3): 301–325. doi:10.1111/1468-2303.00208.
[29] Dupont, B., & Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. Journal of Criminology, 54(1), 76-92.
[30] Economic and Financial Crimes Commission. (2006). High-profile convictions. EFCC Nigeria.
[31] FBI. (2020). Nigerian national arrested for fraud and money laundering. U.S. Department of Justice.
[32] Fokuoh Ampratwum E (2009), "Advance fee fraud "419" and investor confidence in the economies of sub-Saharan African (SSA)". Journal of Financial Crime, Vol. 16 No. 1 pp. 67–79, doi: https://doi.org/10.1108/13590790910924975

[33] GIABA. (2022). Threat assessment on cyber-enabled financial crimes in West Africa.
[34] Handler, S. 2021. "The 5 × 5—Cyber Capacity and Conflict in Africa" The Cyber Statecraft Initiative The 5 × 5—Cyber capacity and conflict in Africa - Atlantic Council.
[35] INTERPOL. (2024a). Cybercrime threat assessment for West Africa.
[36] INTERPOL. (2024b). Arrests in international operation targeting cybercriminals in West Africa.https://www.interpol.int/en/News-and-Events/News/2024/Arrests-in-international-operation-targeting-cybercriminals-in-West-Africa
[37] Kaaniru, J. (2023). The African Union Convention on Cyber Security and Personal Data Protection: Key insights. Centre for Intellectual Property and Information Technology Law (CIPIT). https://cipit.strathmore.edu
[38] Kaspersky. (2024, December 13). Threat landscape for industrial automation systems – Regions, Q2 2024. https://ics-cert.kaspersky.com
[39] Kurbalija, J. (2016). An introduction to internet governance (7th ed.). DiploFoundation. https://www.diplomacy.edu
[40] Lene Hansen, Helen Nissenbaum, Digital Disaster, Cyber Security, and the Copenhagen School, International Studies Quarterly, Volume 53, Issue 4, December 2009, Pages 1155–1175, https://doi.org/10.1111/j.1468-2478.2009.00572.x
[41] MyJoyOnline. (2024). Hajia 4Reall sentenced to over a year in U.S. prison for romance scam. https://www.myjoyonline.com
[42] National Communications Authority. (2020). Amendments to the Electronic Communications Act on SIM box fraud and pre-registered SIMs. Government of Ghana.
[43] New York Post. (2024, March 9). Influencer Mona Montrage pleads guilty in multimillion-dollar catfishing scam. https://nypost.com
[44] Orji, U. J. (2019). ECOWAS legal framework for cybersecurity and cybercrime: A review of regional responses and obligations for member states. African Journal of International and Comparative Law, 27(1), 101–121. https://doi.org/10.3366/ajicl.2019.0260
[45] Osumanu, I. K. (2021). Rituals and cybercrime in Ghana: Understanding the practice of Sakawa. Journal of African Cultural Studies, 33(1), 56–72.
[46] Pakshad, P. (2025). An in-depth analysis of a cyber-attack: Case study and security insights. In Integrating artificial intelligence in cybersecurity and forensic practices (pp. 379–400). IGI Global.
[47] Pakshad, P., & Aqanasiri, S. (2025). Are textual prompts in large language models sufficient for vulnerability detection? In Navigating law and policy in STM enterprises: Ethical governance, regulation, and innovation strategy (pp. 121–138). IGI Global.
[48] Pakshad, P., Shameli-Sendi, A., & Khalaji Emamzadeh Abbasi, B. (2023). A security vulnerability predictor based on source code metrics. Journal of Computer Virology and Hacking Techniques, 19(4), 615–633.
[49] Quarshie, M. (2019). Sakawa: Hybrid spiritualities and the politics of occult economies in Ghana. African Studies Review, 62(2), 154–176.
[50] Ronald J. Deibert, Rafal Rohozinski, Risking Security: Policies and Paradoxes of Cyberspace Security, International Political Sociology, Volume 4, Issue 1, March 2010, Pages 15–32, https://doi.org/10.1111/j.1749-5687.2009.00088.x
[51] Tade, O., & Aliyu, I. (2011). Social organization of internet fraud among university undergraduates in Nigeria. International Journal of Cyber Criminology, 5(2), 860–875.
[52] U.S. Department of Justice. (2005). Report on international advance-fee fraud and bank fraud cases. DOJ Archives.
[53] U.S. Department of Justice. (2024). Social media influencer pleads guilty in romance scam targeting elderly Americans. https://www.justice.gov
[54] Udupa, S., & Pohjonen, M. (2019). Digital cultures of political participation: Internet memes and misinformation in Africa. In S. Udupa & M. Pohjonen (Eds.), Media as politics in postcolonial Africa (pp. 121–142). Zed Books.
[55] UNODC. (n.d.). Using technology to combat crime and promote the rule of law. https://www.unodc.org
[56] Walker G, Adomi EE, Igun SE (2008), "Combating cyber crime in Nigeria". The Electronic Library, Vol. 26 No. 5 pp. 716–725, doi: https://doi.org/10.1108/02640470810910738
[57] World Bank. (2024). Development projects: Digital transformation for Africa/Western Africa Regional Digital Integration Program SOP1 - P176932. https://projects.worldbank.org