Cyber Threat Map of the Central Sahel Region – A Fragile Foundation of Development[1]

Gyula Vörös[2], Viktor Szulcsányi[3]

Abstract:

The developing, but often fragile digital infrastructure of the Central Sahel region – especially the countries of Burkina Faso, Mali, Niger and Chad – are recent targets of various cyberattacks. Despite the financial situation of these countries, cybercriminals and even state-sponsored threat actors are continuously exploiting public internet-facing IT systems that are affected by security vulnerabilities. This study aims to describe the current state of the region's digital infrastructure and cyber threat landscape, while identifying the key aspects of sustainable growth and the potential limitations of the countries' cybersecurity posture. Although the region had limited access to the internet in the past, it has witnessed significant increase in the number or households with mobile internet connectivity. This digital expansion affects the daily life of the population, alongside the difficulties of infrastructural underdevelopment, social and financial inequalities and the political instability and all of these factors are leading to a fragile digital environment. Social media usage had also shown a significant increase in the last decade in this region, and it also gave room for political influence, spreading propaganda or deepfake messages and even for the online requitement of armed groups (e.g. JNIM, ISGS). This paper also provides an overview of the current regulations and legal landscape of the countries in this region. In this constantly evolving territory, the legal and institutional background of cybersecurity governance is of key importance in addressing cyber threats and incidents. This study also discusses the main cyber events affecting the Central Sahel region in the recent years and aims to analyse the presence, operational capacity and maturity level of national CERTs and international partnerships to address cyber threats.

Keywords:
Sahel region; cybersecurity; threat; digital infrastructure; development.

[1] DOI: https://doi.org/10.12700/jceeas.2025.5.3.416
[2] Independent Researcher; ORCID: 0009-0007-4934-2254; voros.gyula@protonmail.com.
[3] Doctoral Student at the Doctoral School on Safety and Security Sciences, Óbuda University, Budapest, Hungary; ORCID: 0009-0003-7946-6312; szulcsanyi.viktor@uni-obuda.hu.

Introduction

Cybercrime is evolving alongside cybersecurity, a phenomenon that challenges experts around the world proves to be an especially difficult problem in a region that recently went through the first stages of digital transformation. The Central Sahel region is making great efforts to handle the exponentially growing need to expand digital access and modernize governance, however, the technological and cultural foundations supporting these changes remain fragile. This progress made the region vulnerable not only to traditional security threats but also to the rapidly evolving domain of cyber threats.

In the region, cybersecurity is often overlooked in both academic and political discourse, even though it is increasingly important to understand the broader security posture and development trajectory of the Central Sahel. As mobile phone use and internet connectivity becomes more widespread, so do the effects of cybercrime, hacktivism, online disinformation and even cyber-based terrorism. These digital threats are exploiting existing social inequalities and infrastructure gaps and often have cross border and cross-sectoral consequences - from undermining public trust in institutions to destabilizing financial systems and threatening humanitarian operations.

This article provides a comprehensive analysis of the recent and recurring cyber threats affecting the IT infrastructures of the public or private sector and even the daily life in the Central Sahel region, while also examining the technical and geopolitical aspects of their impact. It also aims to address the state of the digital infrastructure, the prevalence and nature of cyber-attacks, and the capacity of national and regional actors to respond. Furthermore, the research emphasizes the analysis of regulations affecting public institutions and critical infrastructure, and the legal framework underpinning cybersecurity procedures.

Digital Infrastructure

The region is experiencing a continuous increase in the usage of mobile phone network, internet and along with this, in the usage of social media as well. This chapter aims to present the recent statistic data on these indicators.

During the research, the latest statistics for early 2025 were collected and broken down by country on the regional access and usage of digital services. The comparative analysis included statistical data and covered the security policy implications of digitalization in these countries. The sudden emergence of technological innovations could also negatively impact the infrastructure, causing digital fragility, the impact of disinformation campaigns, data protection challenges, and the risks of the online presence of armed and cyber actors. (Kshetri, 2019)

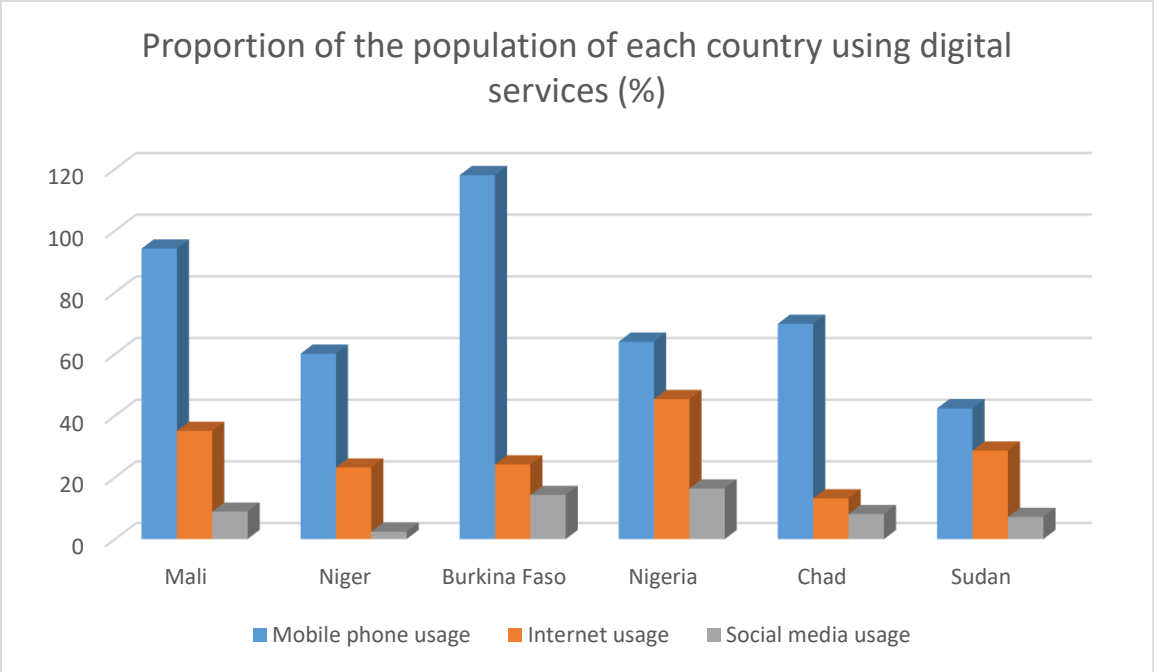

Figure 1: The proportion of the population of each country using digital services

Mali

At the beginning of 2025, only 35.1% of the population of Mali, or about 8.72 million people, used the internet. At the same time, there were 23.4 million mobile subscriptions active in the country, which corresponds to 94.2% of the population. Social media is used even less: in January 2025, only 2.20 million social media accounts were registered in Mali, which represents 8.9% of the total population. Internet access is almost exclusively via mobile networks, as the wired infrastructure is still underdeveloped. There are also significant territorial inequalities, with a much higher proportion of internet users in cities, while access is minimal in rural areas. The most popular social media is Facebook – according to the data published by Meta, approximately 2.2 million people in Mali used Facebook at the beginning of 2025, which is practically the same as the estimated number of social media users. (Kemp, 2025)

Niger

In Niger, only 23.2% of the country's population or approximately 6.37 million people was using the internet at the beginning of 2025, one of the lowest among the countries studied in this paper. However, 60.1% of the population were using the mobile network – this suggests that many people have a phone even if they do not have internet access. Social media usage is very low, with barely 669 thousand users (2.4% of the population) present on social platforms at the beginning of 2025. Since the majority of the population lives in rural areas, network coverage is severely limited outside of large cities, and online presence is mainly concentrated in cities. In Niger, Facebook is also the dominant platform among the few internet users (~669 thousand user base in 2025) (Kemp, 2025).

Burkina Faso

In Burkina Faso, the prevalence of internet usage was 24.2% at the beginning of 2025, representing approximately 5.75 million internet users. At the same time, the number of mobile subscriptions exceeded the population: there were 28.1 million active mobile connections, which equals 118% of the population – indicating the prevalence of multiple SIM usage. Social media was used by 14.3% of the population or approximately 3.40 million people at the beginning of 2025. Although Burkina Faso has a higher proportion of urban dwellers, around two-thirds of the population still lives in rural areas, where internet access is limited. Most internet users connect via mobile networks. Facebook is by far the most significant of the social platforms: it was actively used by approximately 3.40 million Burkinabé in the beginning of 2025, which is practically the same as the total number of social media users in the country (Kemp, 2025).

Nigeria

Nigeria is one of the more digitally advanced countries in this region. The percentage of internet users have reached 45.4% in early 2025, covering around 107 million people – by far the highest among the countries surveyed. In line with its huge population, the number of mobile phone subscriptions is also high: there were 150 million active connections in early 2025 which is nearly two thirds of the country's population. Social media usage is also significant, with 38.7 million users, representing 16.4% of the population. Almost 55% of Nigeria's population lives in cities, so there is a smaller urbanization gap in terms of digital coverage, although internet access is more limited in rural areas. The most popular platform is Facebook, which was actively used by around 38.7 million Nigerians in early 2025 (Kemp, 2025).

Chad

In Chad, 13.2% of the population or around 2.74 million people had access to the internet at the beginning of 2025, which is an extremely low percentage even in comparison with the other countries of the Central Sahel. In contrast, there were 14.5 million mobile connections, equivalent to 69.8% of the population – many people have a mobile phone, presumably often with multiple SIM cards. Social media use is moderately widespread: there were 1.68 million registered user accounts at the beginning of 2025. Most of the population lives in rural areas, so internet access is typically concentrated in cities. Interestingly, TikTok is one of the leading platforms in Chad – its adult reach, based on advertising data, is equal to or exceeds that of Facebook (Kemp, 2025).

Sudan

The prevalence rate of internet usage was 28.7% at the beginning of 2025 in Sudan, representing approximately 14.6 million people. The number of mobile connections was

21.6 million at the same time – covering 42.4% of the population. The number of social media users was approximately 3.68 million at the beginning of 2025. Due to the war situation, internet outages and government restrictions were frequent, further reducing online presence. By 2025, TikTok had become the largest social platform in Sudan based on advertising reach as it had approximately 3.7 million users, as the use of Facebook and other networks was severely hampered by the conflict (Kemp, 2025).

Cybersecurity Posture in the Central Sahel

The Central Sahel region (Burkina Faso, Chad, Mali, Niger, Nigeria, Sudan) has seen rapidly growing internet and mobile usage, but with lagging cybersecurity infrastructure. The spread of social media activity is also high, namely Nigeria and Kenya have some of the world's longest social media engagement times. They are also the countries with the most reported concerns about disinformation campaigns (Africa Center for Strategic Studies, 2024).

The Central Sahel region — mainly Mali, Burkina Faso, and Niger — faces a complex and growing set of cyber risks. These countries are already under pressure from political instability, armed conflict, and limited state capacity. Now, digital threats are being added to the list, and most of the region isn't ready to handle them.

There's not a lot of public data on cyber incidents in this area. That doesn't mean threats don't exist — it just means they often go unreported, unnoticed, or are handled quietly. Government institutions, local banks, and even telecommunication companies in the region have started moving services online, but this digital shift hasn't been matched with enough security. Many public and private networks are vulnerable, either because of outdated systems, weak passwords, or just a general lack of awareness.

The cybersecurity laws in these countries are still pretty new or underdeveloped. For example, Burkina Faso passed a cybercrime law in 2019, but enforcement is patchy. Mali and Niger have some policies in place, but they're not well funded or well known. There also aren't many people trained to work in cybersecurity — this shortage of cybersecurity experts in the region can also be considered as a reason why the attack surface of digital systems is not properly managed.

One of the main issues is that digital development in the region has outpaced regulation. People use phones for money transfers, news, and social media after the sudden spread of digitalization, but that convenience also comes with risks. Phishing scams, fake pages, and fraud are common risks internet users face worldwide and that emphatically applies to those living in the region. However, many governments in the region have only recently begun developing formal cybersecurity strategies.

There have been some steps toward solving the problem cooperatively as the Economic Community of West African States (ECOWAS) has pushed for shared cybersecurity strategies, and a few regional workshops have been held. But actual coordination between the Sahel countries is still very limited. Most governments are dealing with more immediate security threats, like insurgencies and coups, and digital defense isn't yet a top priority.

The lack of trust between states, weak infrastructure, and frequent changes in leadership make it hard to build long-term cyber strategies. Some international partners — including France, the EU, and the UN — have offered funding or training programs. Although these programs contribute to increase cybersecurity, without a strong local foundation, they're less likely to provide permanent solutions.

Threat Landscape of the Central Sahel Region

In recent years, the Sahel has become one of the most volatile regions in the world — not just in a physical or geopolitical sense, but increasingly online. As mobile phones and social media platforms become more widespread, digital risks emerge as well. Militant groups, foreign powers, and criminal networks have all learned how to use the internet to shape opinions, recruit, spread falsehoods, and exploit security gaps. At the same time, most governments in the region are still trying to build digital resilience while struggling with political instability, limited funding, and a shortage of technical expertise. (Maleh, 2022)

Significant changes are taking place related to information flow as disinformation campaigns are affecting the daily life of people in the region. Armed groups like Boko Haram and ISWAP don't just carry out attacks — they film them, edit the footage, and push it out through Telegram, WhatsApp, and YouTube to intimidate opponents and recruit new followers. Pro-Russian networks have also taken aim at Sahel countries, flooding social media with conspiracy theories, pro-junta narratives, and anti-Western propaganda, especially after recent coups. (Wright, 2025) Even local militias and political actors are now using platforms like TikTok and Facebook to sway public opinion or sow division.

There is also a significant increase in the occurrence of cyber-attacks against financial institutions, government websites, and telecommunication providers. Many of these incidents go unreported, but some have caused serious disruption — millions lost to fraud, online services knocked offline, or attackers managed to steal sensitive or even confidential data. Most countries in the region don't have the capability to strengthen cybersecurity of the IT infrastructure of governmental agencies or critical infrastructures, and existing systems are often underfunded or understaffed. (Pantserev, 2022) International support helps to fill some gaps, but it is still necessary to establish well-functioning national CSIRTs.

This section looks at how social media, disinformation, and other cyber threats are shaping the Sahel's digital landscape. From online jihadist propaganda to state-linked hacking and local cybercrime, the battle for influence is no longer just physical. It's digital too — and the region remains deeply vulnerable.

Social Media and Disinformation Threats

Social media plays a central role in both civil communication and disinformation warfare in the Sahel. In Nigeria, Mali, and Burkina Faso, extremist actors such as Boko Haram

and ISWAP use Telegram, WhatsApp, YouTube, and Twitter to spread propaganda, share attack footage, and solicit cryptocurrency donations (Hassan, 2024). They often convey information mixing religious justification with militaristic imagery to achieve a greater psychological impact and therefore support their own recruitment.

These dynamics are further compounded by foreign disinformation campaigns, particularly those linked to Russian or Chinese interests (Wright, 2025). After coups in Mali (2020), Burkina Faso (2022), and Niger (2023), coordinated pro-Russian messaging emerged, portraying military regimes as patriotic defenders, while delegitimizing Western actors. These narratives are driven by media linked to the Wagner Group and local influencers, using platforms like Telegram and Facebook (Africa Center for Strategic Studies, 2024).

Internal conflicts also produce disinformation surges. In Sudan, both sides of the current civil war deploy coordinated messaging to claim battlefield victories, worsening the information disorder. Jihadist groups such as JNIM and ISGS utilize social media and encrypted channels to project ideological legitimacy as they are often targeting the younger generation through these platforms. As social media access spreads, the region faces a new era of information flow, where propaganda, misinformation, and psychological warfare blur traditional distinctions between legitimate media content and deception. (Africa Center for Strategic Studies, 2024)

Notable Cyber Incidents

Current, openly accessible data on cyberattacks in the Sahel is limited, yet available indicators suggest significant risk. Nigeria is consistently among the most targeted nations not only in the Sahel, but in Africa as well. Nigerian entities accounted for nearly 27% of all reported cyber breaches in Africa that year. Attacks are concentrated in the finance, government, and education sectors, with phishing, malware, and ransomware dominating the threat landscape.

Outside of Nigeria, there are only a few, yet significant confirmed cases. In Sudan, political instability impairs cyber monitoring. Elsewhere, regional analogs suggest growing exposure: Ethiopia has faced politically motivated DDoS attacks, and in South Africa, the Snatch ransomware group encrypted 200 TB data of the Ministry of Defence. Although these incidents fall outside the Central Sahel's core, they underscore potential vulnerabilities. If a similar-scale attack targeted a Sahelian government database or utility provider, consequences would likely be severe, since the fragile digital infrastructure and limited forensic capacity probably could not handle the incident properly and in the required time.

Group-IB, a Singapore-headquartered cybersecurity company revealed in a report in November 2022, that OPERA1ER, a French-speaking APT group active since at least 2016, extensively targeted financial institutions across Africa between 2018 and 2022. The group carried out more than 30 successful cyberattacks on banks, financial services, and telecommunication companies in African countries such as Burkina Faso, Benin, Ivory Coast, and Senegal. The attackers gained initial access through carefully crafted

French-language spear-phishing emails posing as legitimate invoices or payment notifications, sent mostly on weekends or holidays when staffing was low. Once inside the system, the group typically stayed inactive or kept a low profile for three to twelve months. This slow approach allowed thorough reconnaissance and credential harvesting. When ready, OPERA1ER launched fraudulent transactions from compromised banking infrastructure, leading to cause damages worth at least $30 million to the affected African firms. (Lakshmanan, 2022)

In January 2024, the hacktivist group Anonymous Sudan claimed a massive cyberattack on Sudachad, Chad's main telecommunications provider. According to their Telegram announcements, the attack focused on network devices, network administration systems, and other infrastructure components. The group reportedly carried out distributed-denial-of-service (DDoS) strikes to overwhelm the network and cause outages. During the incident, monitoring services like NetBlocks observed a significant decrease in internet connectivity throughout Chad, which also confirmed that the attack had been successful. Anonymous Sudan justified the attack by accusing Chad of supporting the paramilitary Rapid Support Forces (RSF) in Sudan. (DarkReading, 2024)

The Malian branch of Bank of Africa (BOA Mali) faced a cyberattack targeting its internal email system and several local workstations in February 2023. The bank promptly blocked access to its information systems and reset user accounts to contain the breach. According to their official statement, the core banking system and monetary platform were not compromised, and no customer or employee data was exposed. BOA Mali confirmed that there were no financial losses and the response effectively neutralized the threat quickly. (L'Economiste, 2023)

In May 2023, the hacker group Mysterious Team launched a series of DDoS (Distributed Denial-of-Service) attacks against multiple Senegalese government websites, including the websites of the Ministry of Finance and the Ministry of the Interior. As a result of the attacks, the sites were inaccessible for several hours. The group claimed responsibility through Twitter posts using the hashtag #FreeSenegal, a slogan associated with opposition movements alleging political repression in the country. (Reuters, 2023)

Cybersecurity Capabilities (CERTs and Response)

Most Sahel countries are still building their cyber response infrastructures. National Computer Emergency Response Teams (CERT/CSIRT) are emerging. Nigeria maintains a National CERT Coordination Centre under the National Security Adviser. Sectoral CERTs include the NCC-CSIRT (telecom regulator) and NITDA's CERT (NITDA-CERT or CERRT), as well as a police National Cybercrime Centre (NPF-NCCC) (Onyido et. al., 2024). Niger's new strategy explicitly calls for establishing a *Centre National de la Cyber Sécurité (CNAC)*, a great improvement towards securing digital infrastructure across the country. Burkina's ANSSI is the coordinating body and has begun setting security standards for public IT systems (ANSSI, 2025). Chad's ANSICE, established in 2015, is

the lead authority for cybersecurity and electronic certification (Global Forum on Cyber Expertise, 2025). Sudan has a Sudan CERT (first responder role) under its Ministry of Information Technology (Council of Europe, 2025) though its effectiveness is unclear amid political turmoil. There is no regional CERT network yet, but all Sahelian states are part of larger efforts (AU, ITU, ECOWAS frameworks).

On offensive operations, there is no public evidence of Sahel governments conducting cyber warfare abroad. Regional capacities focus on defense, enforcement and forensics. For example, under Nigeria's law, failure to report breaches to the National CERT within 72 hours is penalized, indicating that incident detection and response is considered a priority. A few countries have shown initiative, for example Sudan's amended Cybercrime Act even criminalizes "fake news", hinting at efforts to control information flows.

But offensive hacking or cyber-intelligence capability are not documented. In practice, defensive capabilities remain insufficient as most Sahel CERTs have limited staffing and budgets, and cyber forensics labs are only now coming online. (Cinini et. al., 2023)

Terrorist Groups and Cyber Operations

Militant jihadist groups active in the Sahel have increasingly adapted to the digital age, though none have shown advanced "cyber" capabilities akin to sophisticated state actors. Boko Haram (JAS) and ISWAP in Nigeria are the most prolific cyber-savvy terrorists in the region. They produce professional propaganda videos and use encrypted apps (Telegram, WhatsApp) for communication and fund solicitation. Although terrorist groups are also active on the dark web, based on recent trends, their activities have increasingly spread to the public internet, including the use of social media, to reach a larger audience. (Besenyő et. al., 2021) Their online activities serve recruitment, fundraising, and psychological operations, but they have not been known to conduct hacking attacks. Instead, their "cyber" activities are disinformation and propaganda: releasing gruesome execution footage and "governance" propaganda online to influence local populations. African media analyses note that Boko Haram and ISWAP now use social networks extensively (videos, audio, coded chats) to coordinate their actions and recruitment. (Hassan, 2024)

In Mali and Burkina Faso, Al-Qaeda–affiliated groups (JNIM) and Islamic State Sahel affiliate (ISGS) appear online mostly via jihadi channels. Studies show that Katiba Macina and Ansar Dine have used WhatsApp, Facebook and Telegram to urge followers to fight foreign forces. They frame attacks as defending Islam and post images of their operations (e.g. a 2018 suicide bombing in Timbuktu). However, these groups have not demonstrated disruptive cyber operations; their use of the internet is propaganda-driven. Ansaroul Islam, an Islamist group active in Burkina Faso and Mali have limited online presence, mainly communicating through radio broadcasts, though recently started to use Facebook and other social media platforms to spread disinformation about government actions. (Vermeersch et. al., 2020)

Importantly, Jihadist groups have not publicly mounted any significant cyberattacks on institutions. Their focus remains physical attacks and media manipulation. There is no evidence of suicide hackers or state-level cyberwar tactics by these groups. Nonetheless, their online propaganda is a serious threat: by exploiting social media they can radicalize or intimidate, for instance, the Boko Haram in remote Nigeria use "middlemen" to pass on jihadist messages from encrypted apps to offline villagers (Cox et. al., 2018). Furthermore, jihadi-affiliated hacktivist entities have begun to appear globally (e.g. "Anonymous Sudan" claimed a DDoS on Kenya's e-service portal), but their ties to Sahel insurgencies are tenuous. (Bezborodko, 2024) Thus, while Sahel terrorist groups have embraced social media for indoctrination, they currently lack the capability or the motive to conduct cyber espionage or sabotage.

Country-Specific Laws and Recent Developments

Each Sahel country is strengthening its legal framework to encompass the needed regulations addressing recent cyber risks and threats. Nigeria passed a landmark Cybercrimes (Prohibition, Prevention, etc.) Act in 2015 and amended it in 2024 to tighten provisions on hacking and funding terrorism. Nigeria also enacted the Nigeria Data Protection Act 2023. Agencies like NITDA (Digital Policy) and NDPC (Data Privacy) now have enforcement powers including steep fines for breaches. (Onyido et. al., 2024) Niger launched its national cybersecurity strategy (2023–2027) to harmonize with ECOWAS and AU standards, emphasizing new legislation and the creation of a National Cybersecurity Center (CNAC). Burkina Faso updated its cyber law in 2017 and in 2019 implemented a general IS security policy for public agencies. It also has an active data protection authority which have been established in 2021 (ANSSI, 2025). Chad codified cybersecurity and cybercrime in 2015 (Law 009/PR/2015) and set up ANSICE by the same law (Council of Europe, 2025). Sudan repealed its older Computer Crime Act (2007) with a comprehensive Cybercrimes Act in 2018, which criminalizes online defamation and fake news as well as typical cybercrimes. Sudan also has a National Intelligence and a Computer Training Center noted in its laws (Council of Europe, 2025). Mali annunciated a Cybercrime law in 2015 and has a draft of an updated national cybersecurity strategy, although it is still in the development phase, it is expected to be approved this year. (Kassouwi, 2025) Recently, after its 2021 coup, the Malian military regime has shut down some media and internet access as a form of information warfare to control the narrative.

In summary, the Central Sahel has begun to build the legal and institutional pillars of cyber defense, but enforcement is still inefficient. Despite new laws, low prosecutions and lack of technical expertise, it undermines deterrence. Many countries still need to implement regulations and capacity (judges trained in cyber law, forensic experts, etc.) to make these laws effective. Recent advances include Nigeria's 2023 data protection regime, Niger's new cybersecurity center, and regional cooperation projects, such as EU and UN development programs to train CERT staff. However, the pace of regulatory and defensive development remains slower than the pace of threats.

Security Policy Implications

The limited and uneven digital development of these states poses specific security risks. The continuously growing and unmanaged – at least from a security point of view – telecommunications infrastructure and limited cybersecurity capacities lead to significant security gaps. Governments or armed actors sometimes deliberately restrict the internet to create an information vacuum. Online crime is also growing sharply; in West Africa, for example, more than 30% of registered crimes are now cybercrime. (INTERPOL, 2025) Meanwhile, the spread of disinformation and online propaganda poses a new threat. External actors, particularly Russia, are actively waging information warfare in the region, aiming to destabilize societies and weaken Western influence. In Mali, Russian disinformation campaigns have amplified anti-Western narratives, contributing to the government's expulsion of UN peacekeepers and its turn to Russian mercenaries. (Wright, 2025) Terrorist groups also use social media for recruitment and propaganda, further fueling violence and making conflict management more difficult. The lack of a digital sector, coupled with malicious online activities, is creating new types of security threats in the region. Limited access and manipulated information both undermine stability and pose a serious challenge to both affected governments and international security actors.

Conclusion

The Central Sahel region faces growing cybersecurity challenges as sudden digitalization outpaces cybersecurity measures. While the use of mobile devices and internet spread widely, most countries still lack strong cybersecurity systems and well-funded response teams. While Nigeria and Niger have made recent progress with national cybersecurity strategies and legal frameworks, many others are still building the basics. Countries like Sudan and Chad have laws and agencies, but political instability and resource limits hinder their effectiveness.

As cyberattacks targeting the region are increasing, Nigeria have become one of the most attacked countries in Africa, with thousands of incidents against banks, government offices, and schools every week. Although other countries in the Sahel region are generally not reporting detailed information about cyber attacks, global trends suggest they also face similar threats like data breaches, cyber espionage or denial of service attacks. If a large, well-orchestrated attack occurs on a governmental system or infrastructure, it could cause serious damage. The limited capacity of local Computer Emergency Response Teams (CERTs) shows that defensive efforts are still developing.

Social media is playing an increasing role in cyberspace activities in the Sahel. Extremist groups, like Boko Haram and ISWAP use encrypted apps and social media platforms to spread propaganda, recruit and raise funds. In addition, foreign-state supported disinformation campaigns, especially linked to Russia, have targeted countries like Mali, Burkina Faso, and Niger. These campaigns support military juntas and

propagate anti-Western messages in order to destabilize the region's volatile political environment.

The cyber activities related to terrorist groups in the Sahel currently still focus on propaganda and misinformation, rather than major disruptive or intelligence-focused operations. Groups in Nigeria and Mali use social media and encrypted messaging to coordinate and spread their narratives but lack the technical skills for offensive cyber operations. Meanwhile, hacktivist groups, like "Anonymous Sudan" have launched multiple attacks in the region, but their direct links to Sahel insurgents are unclear.

On the legal side, countries are updating laws or at a legislative phase to address the emerging risks of digitalization. Nigeria already has updated cybercrime and data protection laws, while Niger and Burkina Faso have recent strategies aligned with regional standards. However, enforcement remains weak due to lack of trained personnel, cybersecurity capability, and consistent prosecution.

Recent incidents like cyberattacks on financial institutions in Burkina Faso, Mali's Bank of Africa, and Senegalese government websites show the growing threat of both politically motivated and financially driven cyberattacks. Groups like Mysterious Team and Anonymous Sudan have targeted government systems with denial of service attacks during times of political tension.

In summary, the Central Sahel has a very fragile digital environment as cybersecurity defenses and legal frameworks are still catching up to the recent trends in cyber threats. The region faces a wide variety of criminal, terrorist, and foreign state-supported cyber threats, all of which are exploiting weak infrastructure and political instability at some degree among other factors. Building capability and capacity in national CERTs, improving laws and regulations and investing in cyber awareness are some of the urgent steps needed to protect the Sahel's growing digital economy and fragile security environment.

Conflict of Interest

The authors hereby declare that they have no financial interest in this manuscript.

Notes on Contributors

Gyula Vörös is a dedicated professional in the fields of information security and cyber operations, holding degrees in Information Security Management and Military Systems Operation from the University of Public Service in Hungary. His academic and professional interests center around the complexity of cyberspace and the interactions between state and non-state actors within it. He is currently preparing to apply for doctoral studies, where he intends to conduct research on the strategic dimensions of cyber operations, with a particular focus on the assertion of state interests in the digital domain. Over the years, he has compiled a comprehensive database of several thousand articles and analyses documenting cyber incidents, operations, and campaigns from around the world. This resource forms the foundation for his planned research, through

which he aims to perform a systematic evaluation of cyberspace activity. His analysis will go beyond the traditional criminal perspective, focusing instead on the geopolitical, strategic, and policy-related implications of state-driven cyber operations.

Viktor Szulcsányi holds a Master's degree in Computer Science Engineering and is currently a doctoral student at the Doctoral School on Safety and Security Sciences at Óbuda University. He has nearly a decade of work experience in the field of cybersecurity. His doctoral research investigates "The Modeling of Attack Group Activities: Opportunities and Challenges in Attribution," with a focus on the theoretical and practical aspects of cyber threat actor identification. His area of research lie at the intersection of cybersecurity, cyber law, and security policy, aiming to contribute to the development of systematic frameworks for understanding and attributing hostile cyber operations. In addition to his academic pursuits, Viktor Szulcsanyi holds several widely recognized professional certifications, including CISSP, SecurityX, and OSCP, reflecting a strong foundation in both strategic and technical aspects of cybersecurity. His work is aiming to bridge research and practice, supporting evidence-based decision-making in national and organizational cybersecurity contexts.

References

Africa Center for Strategic Studies. (2024). *Mapping a Surge of Disinformation in Africa*. Retrieved July 10, 2025 from https://africacenter.org/spotlight/mapping-a-surge-of-disinformation-in-africa/

Agence Nationale de la Sécurité des Systèmes d'information (ANSSI). (2025). *National Cybersecurity Agency of Burkina Faso*. Retrieved July 10, 2025 from https://anssi.bf/

Besenyő, J., & Gulyas, A. (2021). The Effect of the Dark Web on the Security. *Journal of Security and Sustainability Issues*, *11*(1), 103-121. DOI: https://doi.org/10.47459/jssi.2021.11.7

Bezborodko, A. (2024). *Cybersecurity threatscape for African countries Q1 2023 – Q3 2024*. Retrieved July 12, 2025 from https://global.ptsecurity.com/en/research/analytics/cybersecurity-threatscape-for-african-countries-q1-2023-q3-2024/

Cinini, S. F., Ehiane, S. O., Osaye, F. J., & Irewunmi, B. A. (2023). The Trends of Cybersecurity and Its Emerging Challenges in Africa. In S. O. Ehiane, S. A. Olofinbiyi, & S. M. Mkhize (Eds.), *Cybercrime and Challenges in South Africa* (pp. 75-106). Springer Nature Singapore. DOI: https://doi.org/10.1007/978-981-99-3057-9_4

Council of Europe. (2025). *Octopus Cybercrime Community*. Retrieved July 10, 2025 from https://www.coe.int/en/web/octopus/

Cox, K., Marcellino, W., Bellasio, J., Ward, A., Galai, K., Meranto, S., & Paoli, G. P. (2018). *Social Media in Africa: A double-edged sword for security and development*. Retrieved July 12, 2025 from

https://www.undp.org/sites/g/files/zskgke326/files/migration/africa/UNDP-RAND-Social-Media-Africa-Executive-Summary_final_3-Oct.pdf

DarkReading. (2024). *Anonymous Sudan Launches Cyberattack on Chad Telco*. Retrieved July 12, 2025 from https://www.darkreading.com/cyberattacks-data-breaches/anonymous-sudan-launches-cyberattack-on-chad-telco

Global Forum on Cyber Expertise. (2025). *Chad*. Retrieved July 10, 2025 from https://thegfce.org/member-and-partner/chad/

Hassan, I. (2024). *Outlaws Are Weaponizing Disinformation in Northern Nigeria*. Retrieved July 12, 2025 from https://www.cigionline.org/articles/outlaws-are-weaponizing-disinformation-in-northern-nigeria/

Interpol Africa Cybercrime Operations Desk. (2025). *INTERPOL AFRICA CYBERTHREAT ASSESSMENT REPORT 2025, 4th edition*. Retrieved July 10, 2025 from https://www.interpol.int/en/content/download/23094/file/Cybercrime_Africa%20Cyberthreat%20Assessment%20Report_Design_FINAL.pdf

Kassouwi, I. K. (2025). *Mali to Launch National Cybersecurity Strategy This Year*. Retrieved July 10, 2025 from https://www.wearetech.africa/en/fils-uk/news/public-management/mali-to-launch-national-cybersecurity-strategy-this-year

Kemp, S. (2025). *Digital 2025: Global Overview Report*. Retrieved July 12, 2025 from https://datareportal.com/reports/digital-2025-global-overview-report

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77-81. DOI: https://doi.org/10.1080/1097198X.2019.1603527

L'Economiste. (2023). *La BOA Mali victime d'une cyberattaque*. Retrieved July 12, 2025 from https://www.leconomiste.com/flash-infos/la-boa-mali-victime-d-une-cyberattaque

Lakshmanan, R. (2022). *OPERA1ER APT Hackers Targeted Dozens of Financial Organizations in Africa*. Retrieved July 12, 2025 from https://thehackernews.com/2022/11/researchers-detail-opera1er-apt-attacks.html

Maleh, Y., & Maleh, Y. (2022). The African View on Cybersecurity. In Y. Maleh & Y. Maleh (Eds.), *Cybersecurity in Morocco* (pp. 29-40). Springer International Publishing. DOI: https://doi.org/10.1007/978-3-031-18475-8_3

Onyido, J. C., Okoro, F., Abdulsalam, M., & Adeyeye, P. (2024). *ICLG - Cybersecurity Laws and Regulations - Nigeria Chapter*. Retrieved July 12, 2025 from https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/nigeria

Pantserev, K. A. (2022). Malicious Use of Artificial Intelligence in Sub-Saharan Africa: Challenges for Pan-African Cybersecurity. *Vestnik RUDN. International Relations*, *22*(2), 288-302. DOI: https://doi.org/10.22363/2313-0660-2022-22-2-288-302

Reuters. (2023). *Senegalese government websites hit with cyber attack*. Retrieved July 12, 2025 from https://www.reuters.com/world/africa/senegalese-government-websites-hit-with-cyberattack-2023-05-27/

Vermeersch, E., Coleman, J., Demuynck, M., & Dal Santo, E. (2020). *The Role of Social Media in Mali and its Relation to Violent Extremism: A Youth Perspective*. Retrieved July 12, 2025 from https://icct.nl/sites/default/files/import/publication/Social-Media-in-Mali-and-Its-Relation-to-Violent-Extremism-A-Youth-Perspective.pdf

Wright, G. (2025). *Bending the Baobab: AI's Erosion of Security in the Sahel*. Retrieved July 12, 2025 from https://georgetownsecuritystudiesreview.org/2025/01/03/bending-the-baobab-ais-erosion-of-security-in-the-sahel/