Analysis of cyber incidents in Senegal from 2005 to 2023

Ciré Sall
Professor of Computer Networks and Cybersecurity, and Supervisor of Information Technology programme, Centre de Formation Africain du Sénégal (CEFAS), Dakar
https://orcid.org/0009-0005-1376-440X

Abstract
This article presents findings from a review of cyber incidents that occurred in Senegal between 2005 and 2023. Twenty-six incidents were identified, and they were analysed in terms of their frequency, incident type, perpetrator type, and victim type. The study found that cyber incidents are increasing in frequency in the country; that the most common incident types are cybercrimes and compromised websites; that the most frequent perpetrators are cybercriminals and hackers; that state/political organisations are slightly more likely than non-state/political entities to be attacked; that the most common incident type experienced by state/political entities is a compromised website; that the most frequent incident type for non-state/political organisations is cybercrime; and that insider attacks are much less common than external attacks, but still occur at a level that is a cause for concern. Based on the findings, the author recommends, inter alia, improved Senegalese government monitoring and reporting of cyber threats, with an emphasis on cooperation between the state's Computer Security Incident Response Team (CSIRT-Senegal, or SNCSIRT) and the CSIRT-Universitaire established by tertiary institutions in the country.

Keywords
cybersecurity, cyber incidents, cyberattacks, cybercrimes, compromised websites, data exposure, denial-of-service (DoS), ransomware, Senegal

DOI: https://doi.org/10.23962/ajic.i34.17851

Recommended citation
Sall, C. (2024). Analysis of cyber incidents in Senegal from 2005 to 2023. *The African Journal of Information and Communication (AJIC), 34,* 1-19. https://doi.org/10.23962/ajic.i34.17851

1. Introduction

As of January 2024, Senegal had an internet penetration of approximately 60% (Statista, 2024). Given Kshetri's (2013) determination that 10–15% internet penetration is the threshold level for the generation of significant hacking activities, it is unsurprising that Senegal has, in recent years, experienced numerous cyber incidents. The aim of this study was to provide insight into the cybersecurity and cyber-threat landscapes in Senegal.

According to Kaspersky (2023), Africa was, in early 2023, among the regions experiencing the largest number of cyberattacks on industrial control system (ICS) computers, with the energy sector experiencing the most ICS attacks. This finding of energy-sector vulnerability is relevant to Senegal, which began oil production, for the first time, in mid-2024 (Rukanga, 2024).

One difficulty with studying cyber incidents in African nations is that many incidents are not reported. According to Allen (2021), 96% of cybersecurity incidents in Africa go unreported or unresolved, meaning that the scale of cyber threats in Africa, including Senegal, is probably much worse than officially documented.

This study identified 26 incidents in Senegal between 2005 and 2023. Data was gathered by reviewing online media reports from, inter alia, *Africa Cybersecurity Magazine*, *Agence de Presse Sénégalaise (APS)*, *L'As*, *Dakaractu*, *ITmag*, *Seneweb*, *Senenews*, *Le Soleil*, and cybersecurity alert bulletins. I used research terms including "*cyberattaques*" (cyberattacks), "*cybermenaces*" (cyber threats), *stratégie nationale de cybersécurité* (national cybersecurity strategy), along with "*Senegal*", to identify incidents that occurred in the country and to gather data about the national cybersecurity space. I also used targeted online searches, typing, for example, the name of a specific malware involved in an attack, in order to gather more information. I could not find any peer-reviewed publications that focused on Senegalese cyber incidents.

When an incident involved an actor targeting many websites of the same type, or targeting the same site multiple times, I considered this to be a single incident. This was the case for the 2023 Mysterious Team attack against several Senegalese government websites; and for the threat actor with the alias Yunus Incredibl, whose 2014 targeting of Senegal's Ministry of Economy and Finance was in fact the actor's third attack on this Ministry.

2. Senegal's cybersecurity landscape

Senegal's core cybersecurity statute is its Law No. 2008-11 on Cybercrime (Republic of Senegal, 2008). In 2016, Senegal acceded to the Convention on Cybercrime (Budapest Convention) and the African Union (AU) Convention on Cybersecurity and Personal Data Protection (Malabo Convention) (AU, 2014; Council of Europe,

2001). However, Senegal ratified the Malabo Convention two years after the Convention was adopted in 2014. Furthermore, the Malabo Convention entered into force only in June 2023, i.e., nine years after its adoption. This indicates that African countries are, to some extent, lagging behind in dealing with cybersecurity concerns.

In 2017, Senegal published the Senegalese National Cybersecurity Strategy (SNC2022), which envisioned, by 2022, a Senegalese "cyberspace of confidence, secure and robust for all" (Ministry of Communications, Telecommunications, Post and the Digital Economy, 2017). The SNC2022 sets out the following five strategic aims:

1. Strategic aim 1: strengthen the legal and institutional framework for cybersecurity in Senegal;
2. Strategic aim 2: protect critical information infrastructure (CII) and government information systems in Senegal;
3. Strategic aim 3: promote a cybersecurity culture in Senegal;
4. Strategic aim 4: strengthen our cybersecurity resources and technical knowhow in all sectors;
5. Strategic aim 5: be involved in regional and international cybersecurity work. (Ministry of Communications, Telecommunications, Post and the Digital Economy, 2017, p. 5)

In 2018, Senegal partnered with France to establish a National Cybersecurity School with a Regional Focus (École Nationale de Cybersécurité à Vocation Régionale, ENCVR) in Dakar. The ENCVR aims to build cybersecurity policy and practical expertise in Senegal and other West African nations (EU Cyber Direct, 2018). In 2021, the Directorate General of Code and Security of Information Systems (Direction Générale du Chiffre et de la Sécurité des Systèmes d'Information, DCSSI) was established, replacing an evolving entity that had been created in 1962. The DCSSI belongs to the General Secretariat in the Office of the Presidency, and is considered to be Senegal's national cybersecurity authority (DCSSI, n.d.-a).

Recent research conducted by cybersecurity firm Indusface found that Senegal was the most cyber-secure African country with respect to businesses allowing their employees to work remotely (*Ventureburn*, 2023). The study, which analysed various cybersecurity metrics including distributed denial-of-service (DDoS) attacks, phishing sites, malware hosting sites, and compromised computers, assigned a cybersecurity index score to countries around the world. Senegal secured the top African spot with an index score of 78.09 out of 100.

All this suggests that Senegalese authorities have understood, to some extent, the challenge and the urgent need to deal with cyber threats at a national level, and have

adopted many initiatives to ensure a more secure cyberspace. As stated above, one area of apparent weakness in Senegal is the low rate of incident reporting. Among the dozens of incidents that have occurred in the country, only one seems to have been formally reported online on the DCSSI website. That sole warning concerned the DDoS attack by the Mysterious Team group targeting government websites in May 2023 (DCSSI, 2023).

In April 2023, it was reported that a workshop took place to prepare for the beginning of operations of Senegal's Computer Security Incident Response Team (CSIRT-Senegal, or SNCSIRT), and, in 2024, the DCSSI began issuing SNCSIRT Alert Bulletins (DCSSI, n.d.-b). Another initiative is CSIRT-Universitaire, which is focused on protecting university cyberspace and Senegal's cyberspace more generally (CSIRT- Universitaire, n.d.). The platform, an initiative by young cybersecurity experts, releases a monthly bulletin to build awareness of international cybersecurity matters. The platform has the merit of allowing the reporting of incidents online. However, not all the data gathered is made public, which can prevent the cybersecurity community in Senegal from having a clear overview of the country's actual cyber-threat landscape.

3. Findings: Cyber incidents, 2005 to 2023

This study identified the following 26 cyber incidents in Senegal between 2005 and 2023:

2005 (two incidents)

In 2005, an operation called "Cyclone in Internet" was launched by the Cybercrime Brigade and ended with the arrest of Nigerian citizens (Gueye, 2005a). These people had sent phishing emails, claiming to be dignitaries from fallen regimes in Africa and seeking help to launder large amounts of money. Victims were asked to fund the purchase of a solution that would supposedly allow them to launder the money. The victims lost a total of more than F.CFA300 million (USD496,000).[1] This type of attack is widely known as the "Nigerian scam" or the "419 scam", with the number referring to section 419 of the Nigerian legal code, which deals with fraud.

In the same year, Senegalese Urban Security arrested a group of Nigerian citizens involved in an attempted scam, similar to the one above, targeting a Senegalese citizen living in the US (Gueye, 2005b). The citizen received an email message from

1 In this article, all USD estimates for amounts in F.CFA (West African CFA franc; currency code XOF) are based on the exchange rate on 31 October 2024.

a woman asking for his help in transferring a large sum of money to the US, with the promise of a large commission. However, the individual was asked to send a certain amount to the account of a legal adviser who would ensure the legality of the transfer. The scam was discovered before the target paid over any money, and the group was arrested.

No incidents were identified for the years 2006 or 2007.

2008 (one incident)
In 2008, the website of a Senegalese newspaper, *Nettali*, was attacked by Trojan horse malware that made the site unavailable (Guissé, 2008; Mbengue, 2008). According to the administrator, the breach came from a forum where a malicious message was sent and, as soon as the message was validated, the website went down.

No incidents were identified for the years 2009 or 2010.

2011 (one incident)
In 2011, the website of Société Générale de Banques au Sénégal (SGBS), the Senegalese arm of French bank Société Générale, was hacked and the home page was defaced with the message: "Hacked by Islamic Ghosts Team" (*Seneweb*, 2011).

2012 (one incident)
In 2012, Wari, which offers a money transfer service, was the victim of an intrusion by a former employee (who had been dismissed) who hacked into the money transfer system to steal F.CFA16 million (USD26,000). When arrested, the guilty individual justified his act as vengeance (*APS*, 2012).

No incidents were identified for the year 2013.

2014 (three incidents)
In 2014, 13 Nigerian nationals based in Senegal were arrested for compromising the email account of a senior official in the Presidency of the Republic and impersonating him. According to *ITmag* (2014), the fraudsters would identify people who wished to emigrate, and would offer to find them a visa for any country in the world, but for a large fee. Then they would ask for a digital version of the person's passport and, using the comprised account, would contact the senior official's friends in the consulates of US or European countries, asking for help in obtaining visas, supposedly for the official's relatives.

In the same year, the home page of the Ministry of Economy and Finance (Ministère de l'Economie et des Finances, MEF) was defaced with the following message:

> This site has been h@cked by somebody. This is just a warning and no data has been deleted or modified (except the current page, obviously) and it is exactly to show you to what extent your systems were vulnerable. If you need some info about your security weaknesses, contact me at piscomputer0101@gmail.com. (author's translation from the original French). (*Dakaractu*, 2014)

Also in 2014, a hacker based in Algeria, with the alias Yunus Incredibl, launched an attack on six Senegalese government websites (*Senenews*, 2014). The attacker altered the websites with pictures, the message "Catch me if you can", and audio messages.

2015 (one incident)

In January 2015, the State Information Agency (Agence de l'Informatique de l'Etat, ADIE), which has since been renamed Sénégal Numérique SA (SENUM),[2] released a communiqué stating that its website had fallen victim to a series of attacks but that its teams had been able to deal with infiltrations (ADIE, 2015). Responsibility for the attack was claimed by the group Anonymous, and according to the message used to deface the website, the attack was in reprisal for Senegal's ban on the publication of the French satirical magazine *Charlie Hebdo* (Fama, 2015).

2016 (one incident)

In 2016, intruders hacked into the financial transfer system of the Post Office (La Poste Sénégal) using the account of an insider agent. The incident cost the Post Office more than F.CFA411 million (USD680,000) (*Leral.net*, 2016).

2017 (one incident)

In 2017, the MalwareTech site reported, using a map, that many African countries, among them Senegal, had been targeted by the ransomware WannaCry (Hutchins, 2017). However, there was no formal report in Senegal regarding WannaCry incidents. The US Cybersecurity and Infrastructure Security Agency (CISA) attributed WannaCry to the North Korean government and stated that the ransomware campaign had resulted in tens of thousands of malware infections in over 150 countries (CISA, 2018).

2 https://www.adie.sn

2018 (one incident)
In 2018, Campusen, an online platform allowing students that passed the baccalaureate to request enrolment in courses in Senegalese universities, was the victim of a denial-of-service (DoS) attack that affected its availability (Ba, 2018).

2019 (two incidents)
In 2019, the Bank of Dakar's server was hacked by intruders. Using malware, the hackers, who were a mix of Nigerian and Senegalese nationals, made withdrawals of amounts ranging from F.CFA2,000 (USD3) to F.CFA50,000 (USD83) by manipulating account balances in the server's database. The total value of the withdrawals was estimated at F.CFA18 million (USD30,000) (OSIRIS, 2020).

Also in 2019, an intruder using the alias "el profesor" launched an attack on the website of the Multinational Higher School of Telecommunications (École Supérieure Multinationale des Télécommunications, ESMT), which is based in Dakar. The website was unavailable for users, who were instead welcomed with the following message: "The website is not correctly configured on this server. If you are the owner of this website, contact your web hosting provider" (author's translation from the original French). The hacker requested USD200 to reestablish the website (*Dakaractu*, 2019). However, there is no evidence that any ransom was paid.

2020 (two incidents)
In 2020, a hacker launched an attack on the corporate system of the attacker's former employer, Transpay, which specialises in electronic ticketing. The attack caused thousands of euros of loss (*PressAfrik*, 2020).

Also in 2020, a group of hackers from Cameroon, who had duplicated the credit cards of 572 clients of the Housing Bank of Senegal (Banque de l'Habitat du Sénégal, BHS), were able to withdraw F.CFA20.776 million (USD34,000) through 117 transactions. They had obtained the credit card numbers by "skimming", i.e., putting an electronic device on an automated teller machine (ATM) in Dakar that allowed them to copy financial information from clients' cards (*Africa Cybersecurity Magazine*, 2020).

2021 (one incident)
In 2021, *PressAfrik*, an online newspaper, fell victim to a DDoS attack that disrupted the availability of its website (Diouf, 2021).

Also in 2021, 13 members of a scamming group were arrested. They had targeted clients of mobile-money applications such as Wave, in complicity with a Wave employee, eventually arrested in Dakar, who had provided them with confidential information about the targeted customers. They had called each victim and claimed that there was a fraud attempt on their account, tricking them into revealing their access code. Upon obtaining the code, they emptied the victim's account. The total theft was estimated at F.CFA150 million (USD248,000) (*Seneweb*, 2021).

2022 (three incidents)

In 2022, the Agency for the Safety of Air Navigation in Africa and Madagascar (Agence pour la Sécurité de la Navigation Aérienne en Afrique et à Madagascar, ASECNA), which is headquartered in Dakar, was the victim of a LockBit ransomware attack. The hackers requested USD25,000 as a ransom (Koné, 2021). There is no indication that a ransom was paid, and a counterattack against the hacking group resulted in the identification of the tool that they used for encryption (*Africa Cybersecurity Magazine*, 2022a). According to a joint report by CISA and international partners, LockBit was, in 2022, the most-deployed ransomware variant across the world, functioning as a ransomware-as-a-service (RaaS) model whereby affiliates are recruited to conduct attacks (CISA et al., 2022).

Also in 2022, the Telecommunications and Posts Regulatory Authority (Autorité de Régulation des Télécommunications et des Postes, ARTP) was the victim of an attack by the Karakurt extortion group, which claimed to have stolen 149GB of data and requested a ransom of USD70,000 or they would release publicly sensitive data (*Africa Cybersecurity Magazine*, 2022b). No ransom was paid, and the data was released (*Africa Cybersecurity Magazine*, 2022c).

Also in 2022, according to CSIRT-Universitaire, a victim reported an Nqhd ransomware attack. The attack resulted in all the victim's files being encrypted with the .nqhd format—with a README file, added to each directory, that requested a ransom of USD980 for recovery of the files (Diallo, 2022).

2023 (five incidents)

In May 2023, Mysterious Team, an international hacktivist group with links to Anonymous, launched a DDoS attack on the website of the Presidency of the Republic, along with other gouv.sn websites (DCSSI, 2023; Ndoye, 2023; Ngom, 2023). On X (formerly Twitter), the hacktivists stated the following, in English, on 27 May 2023:

> Greetings,
> @Macky_Sall
> We've heard that your IT infrastructure is facing some outages. We stand in solidarity with the citizens of #Senegal who are determined to exercise their right to freely choose their next leader. We are #Anonymous.
> @MysteriousTeamO
> #OpSN #FreeSenegal

This May 2023 incident occurred at the same time as many protest marches against the government of then-President Macky Sall, who was accused of seeking to prevent the then-leader of the opposition, Ousmane Sonko, from participating in the future presidential election. (At present, in late 2024, Sonko is Senegal's Prime Minister.) It should be noted that this attack was the only one, among the 26 cyber incidents that I identified in this study, that was reported by the DCSSI via a bulletin on its website (DCSSI, 2023).

Also in May 2023, at the same time as the Mysterious Team's attack on government websites, the same hacktivist group also took down the website of Air Senegal with a DDoS attack (Ndiaye, 2023).

In August 2023, the National Agency for Civil Aviation and Meteorology (Agence Nationale de l'Aviation Civile et de la Météorologie, ANACIM) was the target of hacktivists who defaced the home page of its website with the message "Libérez Juan Branco" ("Free Juan Branco"). According to ANACIM managers, the attack did not have any impact on the website's data (Souaibou, 2023). (Juan Branco, a French-Spanish national who was one of Ousmane Sonko's lawyers, had been arrested earlier in August 2023 in Mauritania and handed over to Senegalese authorities, who were pursuing numerous charges against Branco at the time of this hacktivist incident. Branco was ultimately released and deported to France.)

In September 2023, the Facebook page of the National Programme of Community Agricultural Domains (Programme National des Domaines Agricoles Communautaires, PRODAC) was hacked and altered by Anonymous, which posted pornographic images (Niasse, 2023).

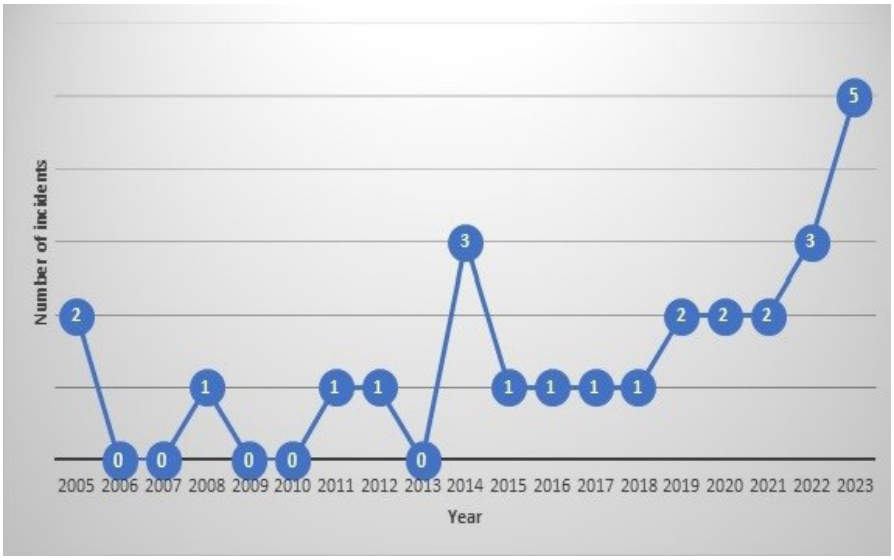
Finally, in November 2023, the Roads Management Agency (Agence de Gestion des Routes, AGEROUTE) was the victim of a LockBit attack, and a ransom was requested. When no ransom was paid, about 18GB of the agency's data was publicly released (Houeto, 2023).

4. Analysis

Figure 1 shows the annual cyber-incident trend, demonstrating the following:

- incidents occurring at least once a year from 2014 onwards;
- incidents occurring at least twice a year from 2019 onwards; and
- the final year studied, 2023, featuring five incidents, the highest number among the years studied.

Figure 1: Annual cyber-incident totals



To analyse the gathered data on the 26 cyber incidents, I used the three classifications established by Van Niekerk (2017) and Pieterse (2021): incident type, perpetrator type, and victim type. I also added a fourth classification: perpetrator position. Table 1 summarises the elements in each classification.

Table 1: Cyber-incident classification taxonomy

Incident type	Perpetrator type	Victim type	Perpetrator position
One of the following: • compromised website • cybercrime • data exposure • denial of service • ransomware	One of the following: • hacktivist • hacker • cybercriminal • nation state	Either of the following: • state/political organisations • other	Either of the following: • external • insider

Note. Source: Derived from Van Niekerk (2017); Pieterse (2021).

Figure 2 shows the share of each incident type. The most prevalent was cybercrime (35%), followed by compromised websites (27%), denials of service (19%), ransomware (15%), and, finally, data exposure (4%). It should be noted that even though data exposure has the lowest share of the incident types, it should not be underestimated because it is often the outcome of a ransomware attack.

Figure 2: Cyber incidents by type

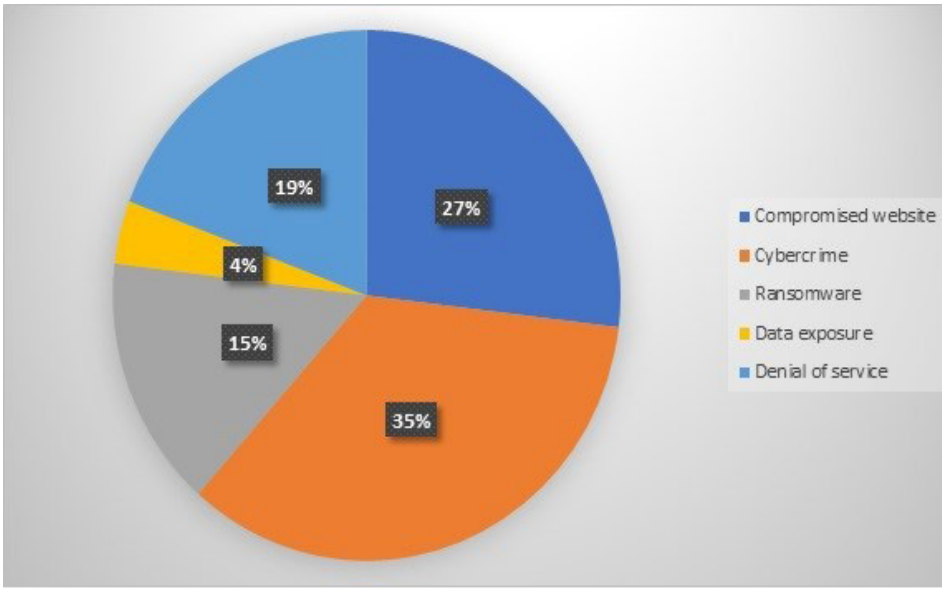


Figure 3 presents the percentage distribution of the perpetrator types, with cybercriminals (46%) and hackers (35%) being the most common perpetrators, followed by hacktivists (15%) and nation states (4%).

Figure 3: Perpetrators by type

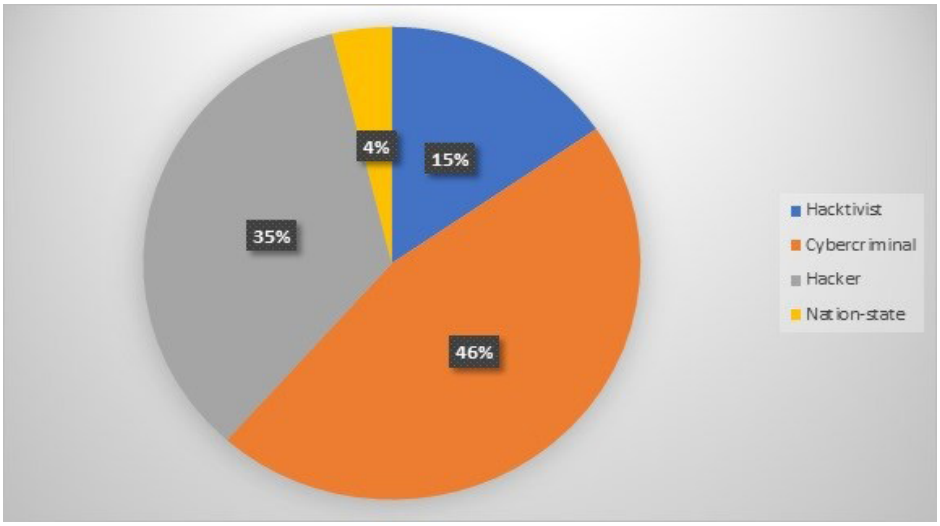


Figure 4 shows the trends in perpetrator type, indicating that cybercriminals and hackers were generally active across the years of study, with a stronger presence from 2018 to 2023. The year 2023 witnessed an abrupt emergence of incidents related to hacktivists, whose actions were closely related to the strained political situation in the country. Meanwhile, only one incident was attributed to a nation-state actor.

Figure 4: Trends in perpetrator type

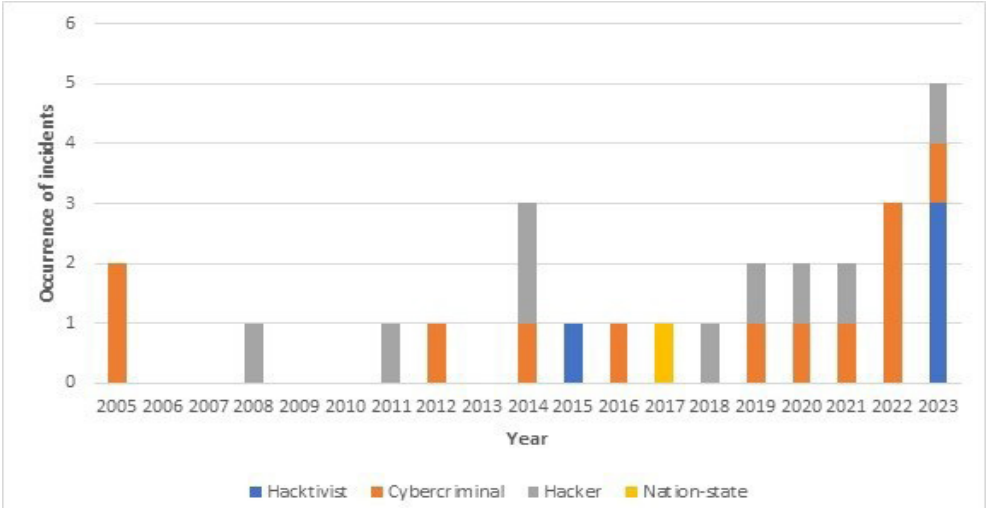


Table 2 is a pivot table that links the incident types to the perpetrator types. As expected, there is a strong correlation between cybercrime and cybercriminal actors, followed by a strong association between hackers and compromised websites, and between hacktivists and compromised websites.

Table 2: Incident type by perpetrator type

	Compromised website	Cybercrime	Ransomware	Data exposure	Denial of service
Hacktivist	4				
Cybercriminal		9	3		
Hacker	5	1			3
Nation state			1		

Figure 5 depicts the distribution of victim types as state/political entities or other. Attacks targeting state/political entities are more prevalent than those targeting other entities.

Figure 5: Distribution by victim type

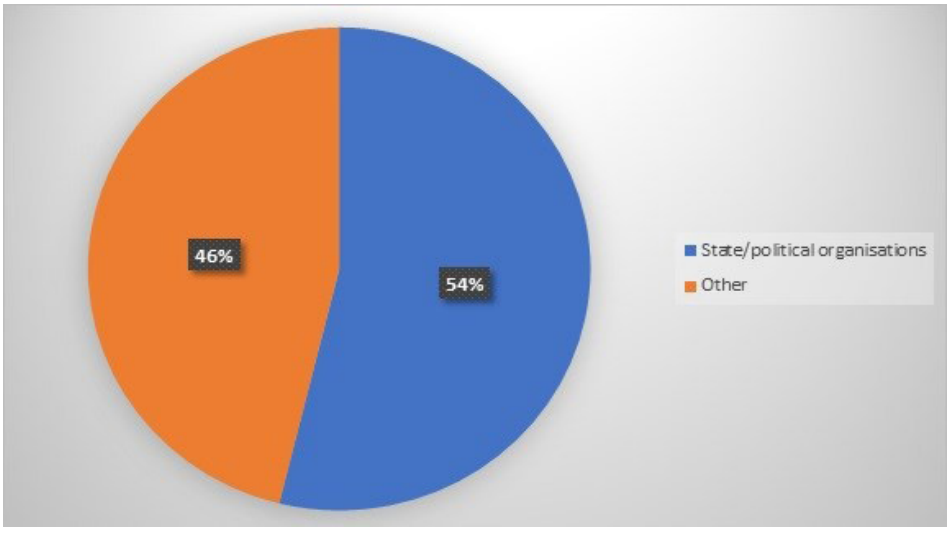


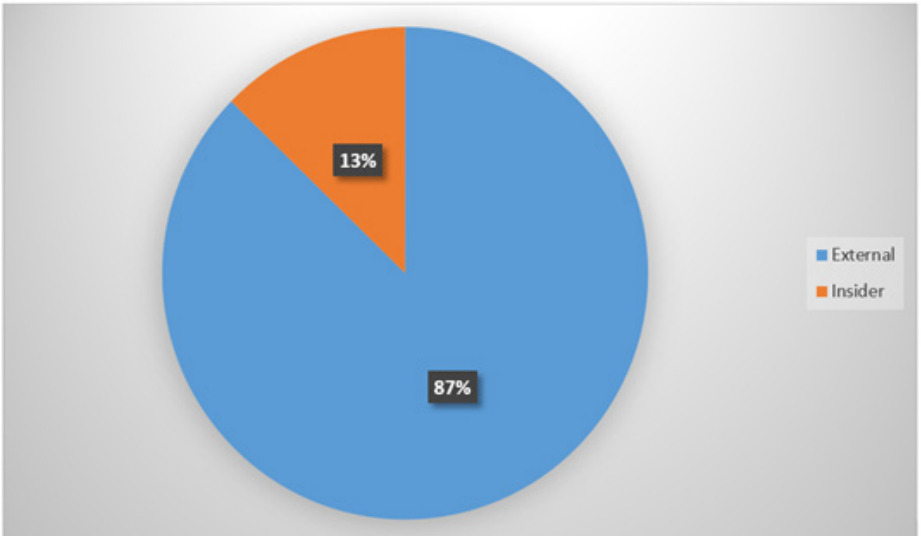
Table 3 is a pivot table that associates incident types with victim types. It shows that the most frequent incident type for state/political organisations was a compromised website, while the most frequent incident type for non-state/political organisations was cybercrime.

Table 3: Incident type by victim type

	Compromised website	Cybercrime	Ransomware	Data exposure	Denial of service
State/political organisations	6	2	2	1	3
Other	1	7	2		2

Finally, I considered incident distribution based on the perpetrator position. While external attacks often receive more attention, insider threats pose a significant risk that must not be overlooked. Insider threats are threats from an insider who, according to CISA, can be any person who has or had authorised access to, or knowledge of, an organisation's resources, including personnel, facilities, information, equipment, networks, and systems (CISA, 2020). Figure 6 shows the percentage distribution of perpetrators between externals and insiders. Incidents involving insiders represented 13% of the 26 cyber incidents identified, an indication that Senegalese entities must pay close attention to this kind of threat.

Figure 6: Perpetrators by position



5. Conclusions

The key findings from this study are that cyber incidents are increasing in frequency in Senegal; that incidents most often take the form of cybercrimes or compromised websites; that the most frequent perpetrators are cybercriminals and hackers; that state/political organisations are more likely to be victims than non-state/political organisations; and that the most frequent incident type for state/political organisations is a compromised website.

The frequency of incidents can be expected to continue to increase, or at least to remain at their currently high level (five incidents in 2023), for the foreseeable future due to, inter alia, increasing internet penetration in Senegal and thus an expanding attack surface. Also, there should be a real concern about the potential vulnerabilities arising from Senegal's commencement of oil production, given Kaspersky's (2023) finding that industrial systems in the oil and gas sector are key cyber-incident targets in Africa.

Senegalese authorities should be aware that the inadequate reporting of cyber incidents, occurring in both the public and private sectors, will limit their understanding of the country's cyber-threat landscape. Hence, there is a need for improved collaboration for the reporting, collection, and analysis of incidents, under the supervision of the DCSSI or CSIRT-Senegal. The DCSSI and CSIRT-Senegal should collaborate with CSIRT-Universitaire in efforts to achieve general cybersecurity awareness at a national level. One element of this cooperation should be the publication of cyber-threat and cyber-incident information not only in French but also in national languages such as Puular, Wolof, and Serer. The French-language literacy rate in Senegal was only 51.8% in 2021, according to the National Agency of Statistic and Demography (Agence Nationale de la Statistique et de la Démographie, ANSD) (ANSD, 2021). Moreover, cyber-incident bulletins should focus more on reporting based on incidents reported by users, while continuing to provide information on global trends. Finally, the option of making cyber-incident reporting mandatory, for both state/political entities and non-state/political entities, should be explored.

Funding
No funding was received for this study.

Data availability
The data supporting the results of this study is available upon written request to the author at sallcire@gmail.com.

AI declaration
No AI tools were used in the research or in the preparation of this article.

Competing interests

The author has no competing interests to declare.

References

Africa Cybersecurity Magazine. (2020, September 25). Cybersécurité au Sénégal: Le Sénégal victime d'une attaque cybercriminelle venue du Cameroun. https://cybersecuritymag.africa/cybersecurite-au-senegal-le-senegal-victime-dune-attaque-cybercriminelle-venue-du-cameroun

Africa Cybersecurity Magazine. (2022a, September 22). Attaques Lockbit 3: La récupération des données possibles [et] envisables. https://cybersecuritymag.africa/attaques-lockbit-3-recuperation-des-donnees-possibles-envisageables

Africa Cybersecurity Magazine. (2022b, October 12). L'ARTP Sénégal touchée par le groupe de ransomwares Karakurt. https://cybersecuritymag.africa/artp-senegal-touchee-par-groupe-ransomwares-karakurt

Africa Cybersecurity Magazine. (2022c, October 17). Les cybercriminels du groupe Karakurt divulguent les données de la cyberattaque de l'ARTP Sénégal. https://cybersecuritymag.africa/cybercriminels-groupe-karakurt-divulguent-donnees-cyberattaque-artp-senegal

African Union (AU). (2014). African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

AU. (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-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf

Agence de l'Informatique de l'Etat (ADIE). (2015, January 18). Communique de l'ADIE suite à l'attaque de son site web. *Seneweb*. https://www.seneweb.com/news/Technologie/communique-de-l-adie-suite-a-l-attaque- d_n_145419.html

Agence de Presse Sénégalaise (APS). (2012, April 17). L'ingénieur financier risque trois ans de prison ferme pour escroquerie. https://www.osiris.sn/L-ingenieur-financier-risque-trois.html

Agence Nationale de la Statistique et de la Démographie (ANSD). (2021). *Enquête harmonisée sur les conditions de vie des ménages (EHCVM) au Sénégal: Rapport final*. https://www.ansd.sn/sites/default/files/2022-11/Rapport-final-EHCVM-vf-Senegal.pdf

Allen, N. (2021, January 19). *Africa's evolving cyber threats*. Africa Center for Strategic Studies. https://africacenter.org/spotlight/africa-evolving-cyber-threats

Ba, D. (2018, August 30). Cyber-attaque: Le site Campusen ciblé par des pirates. *Seneweb*. https://www.osiris.sn/Cyber-attaque-Le-site-Campusen.html

Computer Security Incident Response Team (CSIRT-Universitaire). (n.d.). Fonctions. https://csirt-universitaire.org/fonctions

Cybersecurity and Infrastructure Security Agency (CISA). (2018, June 7). *Indicators associated with WannaCry ransomware*. https://www.cisa.gov/news-events/alerts/2017/05/12/indicators-associated-wannacry-ransomware

CISA. (2020). *Insider threat mitigation guide*. https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf

CISA, with FBI, MS-ISAC, ACSC, NCSC-UK, CCCS, ANSSI, BSI, CERT NZ, NCSC-NZ. (2023). Understanding ransomware threat actors: LockBit. https://www.cisa.gov/sites/default/files/2023-06/aa23-165a_understanding_TA_LockBit_0.pdf

Council of Europe. (2001). The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Dakaractu. (2014, July 20). Le site web du MEF tout comme quatre autres sites officiels ont été piratés. https://www.dakaractu.com/Le-site-Web-du-MEF-tout-comme-quatre-autres-sites-officiels-ont-ete-pirates_a71100.html

Dakaractu. (2019, August 7). Le site de l'École supérieure multinationale des télécommunications piraté: la rançon dérisoire exigée par le hacker «El Profesor». https://www.dakaractu.com/Le-site-de-l-Ecole-superieure-multinationale-des-telecommunications-pirate-la-rancon-derisoire-exigee-par-le-hacker-El_a174670.html

Diallo, C. (2022, May 9). Prendre des fichiers en otage: un acte cybercriminel à l'aide de ransomware ou rançongiciel. CSIRT-Universitaire Bulletin Mensuel de Sécurité, n°2022-01.https://csirt-universitaire.org/media/BulletinMensuel/PDF/BMS1_Bulletin_mensuel_de_securite_no1__v1_2POwnQ4.pdf

Diouf, A. (2021, February 23). Tentative de piratage du site PressAfrik: Appel condamne et tire la sonnette d'alarme. *PressAfrik*. https://www.pressafrik.com/Tentative-de-piratage-du-site-PressAfrik-Appel-condamne-et-tire-la-sonnette-d-alarme_a228311.htmlv

Direction Générale du Chiffre et de la Sécurité des Systèmes d'Information (DCSSI). (n.d.-a). Présentation. http://stcc-ssi.sn/presentation

DCSSI. (n.d.-b). Bulletins d'alerte. http://stcc-ssi.sn/bulletins-dalerte

DCSSI. (2023). Attaques de type DDoS par le groupe «Mysterious Team». https://www.stcc-ssi.sn/2023/06/07/bulletin-dalerte

EU Cyber Direct. (2018). École nationale de cybersécurité à vocation régionale. https://eucyberdirect.eu/good-cyber-story/ecole-nationale-de-cybersecurite-a-vocation-regionale

Fama, A. (2015, January 20). Anonymous a piraté le site de l'Adie en représailles à l'interdiction de Charlie Hebdo. https://senego.com/anonymous-a-pirate-le-site-de-ladie-en-represailles-a-linterdiction-de-charlie-hebdo_211716.html

Federal Bureau of Investigation (FBI), CISA, Treasury & FinCEN. (2022). Karakurt data extortion group. https://www.cisa.gov/sites/default/files/2023-12/aa22-152a-karakurt-data-extortion-group.pdf

Global Cyber Security Capacity Centre. (2016). *Cybersecurity capacity review of the Republic of Senegal*. University of Oxford. https://gcscc.web.ox.ac.uk/files/senegal-report-v4pdf

Gueye, P. (2005a, May 4). Coup de filet de la S.U.: La bande de cyber-escrocs avait engrangé plus de 300 millions. *Le Soleil*. https://osiris.sn/Coup-de-filet-de-la-S-U-la-bande.html

Gueye, P. (2005b, August 17). HLM Grand-Médine: Une bande de cyber-escrocs démantelée. *Le Soleil*. http://osiris.sn/HLM-Grand-Medine-Une-bande-de.html

Guissé, C. M. (2008, January 26). Sabotage et destruction du site Nettali.com: Le parquet aux trousses d'un « cheval de Troie ». *L'As*. https://www.osiris.sn/sabotage-et-destruction-du-site-nettali-com-le-parquet-aux-trousses-d-un-cheval.html

Houeto, C. (2023, November 24). Cyberattaque contre l'Ageroute au Sénégal: Environ 18 gigaoctets de données sensibles publiées. *Africa Cybersecurity Magazine*. https://cybersecuritymag.africa/cyberattaque-contre-lageroute-au-senegal

Hutchins, M. (2017, May 16). *Note on WannaCrypt infection count accuracy*. MalwareTech. https://www.malwaretech.com/tag/wannacry

ITmag. (2014, February 22). Sénégal: 13 Nigérians arrêtés pour avoir piraté le compte mail d'un haut responsable de la Présidence. http://www.itmag.sn/news/senegal-13-nigerians-arretes-pour-avoir-pirate-le-compte-mail-dun-haut-responsable-de-la-presidence

Jones, C. & Chebla, J. (2023). African cyberthreat assessment report 2023. Interpol. https://www.interpol.int/content/download/19174/file/2023_03%20CYBER_African%20Cyberthreat%20Assessment%20Report%202022_EN.pdf

Kaspersky. (2023, September 21). Africa among regions with highest number of industrial systems under attack in the first half of 2023. https://kaspersky.africa-newsroom.com/press/africa-among-regions-with-highest-number-of-industrial-systems-under-attack-in-the-first-half-of-2023?lang=en

Koné, M. (2022, September 20). Sécurité aérienne: le site de l'ASECNA piraté par le groupe de hackers Lockbit. Le360 Afrique. https://afrique.le360.ma/autres- pays/societe/2022/09/20/39358-securite-aerienne-le-site-de-lasecna-pirate-par-le-groupe-de-hackers-lockbit-39358

KPMG. (2022). *Africa cyber security outlook*. https://assets.kpmg.com/content/dam/kpmg/ke/pdf/thought-leaderships/2022/KPMG%20Africa%20Cyber%20Security%20Outlook%202022.pdf

Kshetri, N. (2013). *Cybercrime and cybersecurity in the Global South*. Palgrave Macmillan.

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

Leral.net. (2016, October 17). Piraterie: La Poste délestée de plus de 400 millions. https://www.leral.net/Piraterie-La-Poste-delestee-de-plus-de-400-millions_a182765.html

Mbengue, A. R. (2008, January 26). Un cheval de Troie fait des ravages sur Nettali: L'administration du site porte plainte contre X.

Ministry of Communications, Telecommunications, Post and the Digital Economy. (2017). Senegalese National Cybersecurity Strategy (SNC2022). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SNC2022-Senegal-NCS-Jan-2018_eng.pdf

Ndiaye, T. (2023, May 27). Cyberattaque au Sénégal: Après la présidence de la République et le gouvernement, Air Sénégal touché. *Seneweb*. https://www.seneweb.com/news/Societe/cyberattaque-au-senegal-apres-la- preside_n_410935.html

Ndoye, K. (2023, May 26). Plusieurs sites internet du Gouvernement, dont celui de la Présidence, attaqués. *Seneweb*. https://www.seneweb.com/news/Societe/plusieurs-sites- internet-du-gouvernement_n_410896.html

Ngom, M. (2023, May 29). Sénégal: une « Mysterious Team » derrière les cyberattaques contre l'Etat. *Le Monde Afrique*. https://www.lemonde.fr/afrique/article/2023/05/29/senegal-une-mysterious-team-derriere-les-cyberattaques-contre-l-etat_6175339_3212.html

Niasse, F. (2023, September 7). Victime d'attaques de groupe de hackers Anonymous, le Prodac porte plainte à la Division de la Cybersécurité. Le Grand Panel Citoyen. https://www.grandpanel.sn/victime-dattaques-de-groupe-de-hackers-anonymous-le-prodac-porte-plainte-a-la-division-de-la-cybersecurite

Observatoire sur les systèmes d'information, les réseaux et les inforoutes au Sénégal (OSIRIS). (2020, January 23). Accès frauduleux dans le système de la Banque de Dakar (Bdk): Des cyber délinquants nigérians et sénégalais risquent 4 ans de prison. http://www.osiris.sn/Acces-frauduleux-dans-le-systeme.html

Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. *The African Journal of Information and Communication (AJIC)*, *28*, 1–21. https://doi.org/10.23962/10539/32213

Republic of Senegal. (2008). Law No. 2008-11 (25 January 2008) on Cybercrime.

Rukanga, B. (2024, June 12). Senegal starts producing oil as president promises benefits. *BBC*. https://www.bbc.com/news/articles/c722n9g5w22o

PressAfrik. (2020, December 17). Après avoir attaqué les systèmes de la police et de la gendarmerie: le jeune hacker Souleymane accusé d'avoir bloqué le système de Transpay. https://www.pressafrik.com/Apres-avoir-attaque-les-systemes-de-la-police-et-de-la-gendarmerie-le-jeune-hacker-Souleymane-accuse-d-avoir-bloque-le_a225211.html

Senenews. (2014, November 27). 6 sites du gouvernement sénégalais en gouv.sn hackés par Yunus Incredibl. https://www.senenews.com/actualites/6-sites-du-gouvernement-senegalais-hackes-par-yunus-incredibl_76736.html

Seneweb. (2011, March 30). Banque: Le site web de la Sgbs piraté. https://www.seneweb.com/news/News/medinatoul-salam-les-partisans-de-sokhna_n_43167.html

Seneweb. (2021, November 3). 60 plaintes et 13 arrestations: 150 millions détournés via Wave et Orange Money, la DSC sur la brèche. https://www.seneweb.com/news/Societe/60-plaintes-et-13-arrestations-150-milli_n_362921.html

Souaibou, M. (2023, August 7). ANACIM: la cyberattaque n'a pas atteint les données (responsables). *Agence de Presse Sénégalaise (APS)*. https://baobab7.com/actualites/anacim-la-cyberattaque-na-pas-atteint-les-donnees-responsables

Statista. (2024). Share of internet users in Africa as of January 2024, by country. https://www.statista.com/statistics/1124283/internet-penetration-in-africa-by-country

Symantec. (2016). *Cyber crime and cyber security trends in Africa*. https://securitydelta.nl/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf

Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication (AJIC)*, *20*, 113–132. https://doi.org/10.23962/10539/23573

Ventureburn. (2023, June 20). Senegal tops African countries in cybersecurity – Indusface. https://ventureburn.com/2023/06/senegal-tops-african-countries-in-cybersecurity-indusface