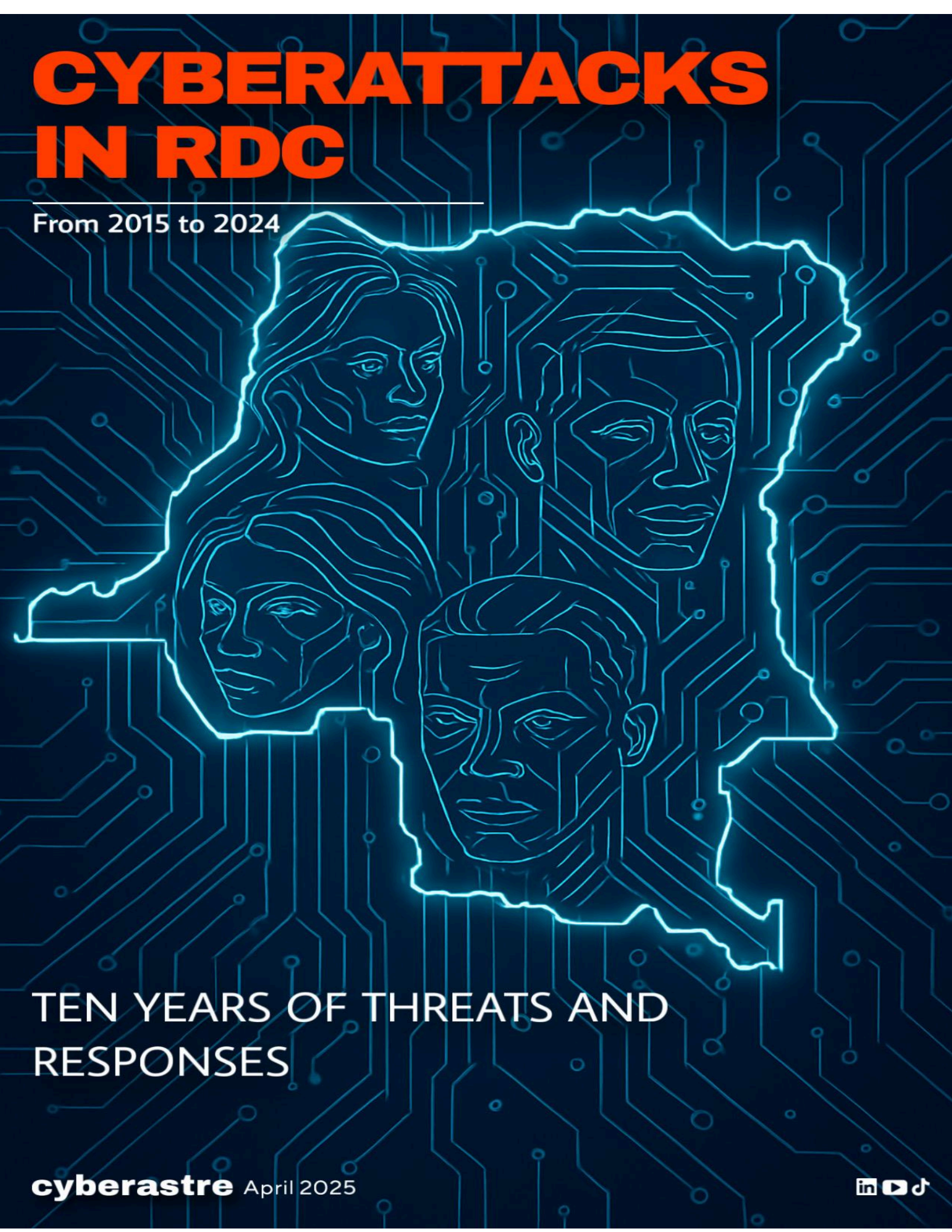
CYBERATTACKS IN RDC

From 2015 to 2024



TEN YEARS OF THREATS AND RESPONSES

cyberastre April 2025

Cyberattacks in the DRC (2015-2024): Review of ten years of threats and responses

General context and issues in the DRC

The Democratic Republic of Congo (DRC) has been experiencing an expansion of its digital ecosystem for a decade, accompanied by new IT threats. If the country had already been confronted with acts of piracy since the 2000s (government and business websites hacked in 2001, 2004, 2005, etc. HABARIDRC.NET), the scale and frequency of cyberattacks have increased over the past ten years. **Ransomware**, **intrusions into official sites**, **online scams** and attacks against **critical infrastructure** are now among the risks that the DRC must face in its journey towards digital transformation.

Several factors contribute to the vulnerability of Congolese cyberspace: increasing computerization of services (governance, finances, communications), often without sufficient security measures, a legal and institutional framework still under construction, and limited user awareness. This report provides a detailed overview of significant cyberattacks in the DRC over the last ten years, highlighting the targets, operating methods, consequences, alleged perpetrators and measures taken. An analysis of trends then makes it possible to identify recommendations to strengthen the **cybersecurity in the DRC**.

NB: The facts cited are supported by sources cited in this research: recognized media, reports and official statements.

Attacks on government sites and public institutions



Extract from an announcement on Twitter by a hacktivist Anonymous (operation #OpCongo) claiming responsibility in November 2018 for attacks against Congolese government sites. These attacks aim to denounce the regime in place TRESORKALONJI.PRO HABARIDRC.NET.

The websites of DRC institutions have been repeatedly targeted by **spectacular hacks**, often motivated by political issues. The most memorable episode comes at the end **2018**, in the middle of the pre-electoral period: a collective claiming to**Anonymous** announces having attacked eight government websites, including those of the Presidency, the Prime Minister's Office and several key ministries (Budget, Planning, Foreign Affairs, Civil Service, etc.) TRESORKALONJI.PRO TRESORKALONJI.PRO. At first, the impact seemed limited – several sites were still online immediately after the announcement – but the attackers intensified their actions. Around

8 p.m. (Kinshasa time) on November 25, 2018, all portals in *.gouv.cd* became inaccessible for a few hours TRESORKALONJI.PRO. These were probably attacks of the type **DDoS** (distributed denial of service) combined with **removals** of web pages, as part of the operation entitled *#OpCongo*. Pirates, linked to groups *Nulld3vice* And *Ghost Squad*, clearly displayed their motivation: "to fight against the oppressive and dictatorial regimes of which the Congolese government is a part" HABARIRDC.NET. They thus intended to protest against the power in place and in particular against the introduction of the controversial **voting machines** electronics planned for the December 2018 elections HABARIRDC.NET . In an interview, the hacktivist **Lorian Synaro** – alleged coordinator of these attacks – confirmed his opposition to voting machines, joining part of the Congolese opposition HABARIRDC.NET . Public calls have even been made to Anonymous to directly target the Independent National Electoral Commission (CENI) and render its systems inoperable before the vote TRESORKALONJI.PRO.

Indeed, the **APPRECIATE** was the subject of intrusion attempts. At the end of 2018, the CENI website and electoral database were attacked, undoubtedly with the aim of sabotaging or discrediting the electoral process. Anonymous claimed responsibility for these actions and promised to "bring the CENI to its knees" if possible. TRESORKALONJI.PRO. However, no major disruption to the centralization of results was attributed to hacking at this time – the main communications outage in January 2019 being the work of the authorities themselves (see below). The goal of the hacktivists was above all symbolic: in **disfiguring** official sites or by making them temporarily inaccessible, they sought to convey a message of protest HABARIRDC.NET. This type of attack, if it lasts only a few hours, does not deeply damage the systems but exposes the vulnerability of the State and can sow confusion (for example by disseminating false information via hacked sites).

Beyond 2018, other institutions have been targeted. More recently, in **June 2024**, the website of **Ministry of Higher and University Education (ESU)** suffered significant hacking. Discovered on the morning of June 8, the attack made the ministry portal inaccessible all weekend, disrupting access to essential information and services for students, teachers and administrators. DIGITALCONGO.ORG. Although the site was restored the following Monday, this incident sparked a **worry** regarding the security of academic and personal data managed online DIGITALCONGO.ORG. He also highlights the **fragility of government digital infrastructures** : even outside tense electoral periods, ministries can be paralyzed by a relatively simple intrusion, due to lack of sufficient protections.

Finally, it is worth mentioning the attempted attacks during the local elections in December **2023**. According to the president of the CENI, Denis Kadima, the computer system of the Electoral Commission resisted attacks "of unprecedented scale" on the day of the vote (December 15, 2023) RADIOGOFM.NET. In the space of 24 hours, no less than *1,303 cyberattacks* were detected and blocked by CENI teams, coming from various countries (United States, Hong Kong, France) RADIOGOFM.NET. Kadima assured that none of these intrusions compromised the integrity of electoral data, the systems having remained secure RADIOGOFM.NET. The CENI therefore seems to have learned lessons from the past by equipping itself with better defense

systems, succeeding in thwarting these attempts to digitally sabotage the electoral process. This episode shows that **Congolese institutions become privileged targets** during major political issues, and that they must expect sophisticated attacks from abroad as well as from within.

With: Attacks on government sites in the DRC have mainly taken the form of actions **hacktivists** (aimed at sending a political message, e.g. #OpCongo 2018) an **opportunistic intrusion** exploiting weak web security. The immediate consequences are often limited (sites temporarily offline, pages displaying protest slogans), but these acts have a strong symbolic impact and can create a climate of uncertainty. The identified or presumed perpetrators are mostly groups **Anonymous** or affiliates, generally based outside the country (which complicates any prosecution). In response, targeted authorities and institutions have gradually improved their resilience: strengthening firewalls and surveillance systems, cooperation with cybersecurity experts, and public communication to reassure data integrity (as did the CENI in 2023). RADIOGOFM.NET). Nevertheless, the need for more robust structural measures remains a central issue (see recommendations section).

Ransomware and financial cyberattacks against businesses

Beyond the public sector, the DRC has not been spared by the global wave of **ransomware** and other financially motivated attacks. Companies and organizations operating in the DRC – whether local or subsidiaries of international groups – have suffered intrusions in recent years aimed at **extorting money** or to steal sensitive data with a view to blackmail.

An emblematic case is that of **Bolloré Transport & Logistics DRC**, the Congolese subsidiary of the French logistics giant. May 14 **2020**, this company was the target of a ransomware-type cyberattack on part of its servers LEMAGIT.FR LEMAGIT.FR. The malware used belongs to the family **NetWalker**, active at the time in numerous attacks around the world. Bolloré RDC confirmed the incident in an official press release dated May 19, 2020: the group indicates that it has **immediately took protective measures** to stop the spread of ransomware, calls on cybercrime experts available 24 hours a day, and launches investigations to assess potentially compromised data LEMAGIT.FR LEMAGIT.FR.



Screenshot from the NetWalker ransomware operators' site in May 2020, showing the list of victims including "Bollore". Cybercriminals displayed a countdown timer threatening to publish the stolen data if the ransom was not paid LEMAGIT.FR.

In the case of Bolloré, the attackers did not just encrypt the files: they also exfiltrated a significant amount of internal data (human resources documents, databases, invoices, password lists, etc.) as proof of their intrusion ZATAZ.COM ZATAZ.COM. Screenshots posted on the *blog* hackers show files from 2009 until May 13, 2020 LEMAGIT.FR, suggesting prolonged access to the company's network before the ransomware was triggered. The criminals demanded a ransom (exact amount not public) in exchange for non-disclosure of this stolen information, setting an ultimatum of May 31, 2020 LEMAGIT.FR. At the same time, they began to publish extracts of data on their leak site to increase pressure, in particular lists of named files (paid leave, financial reports, etc.) and even a countdown before full disclosure ZATAZ.COM ZATAZ.COM. This operating mode – said to be **double extortion** – has become common: it is no longer enough to restore backups to resolve the incident, because the threat also concerns data confidentiality. Bolloré has not communicated publicly on whether or not the ransom was paid, but it filed a complaint in the DRC and promised to be transparent with its partners on the results of the investigation. LEMAGIT.FR LEMAGIT.FR. This episode highlighted the vulnerability of players in the sector **logistics and transport**, considered vital infrastructure (supply chains), and the exposure of their African subsidiaries to the same cyber threats as Western headquarters.

The sector **banking** Congolese was also targeted. In June **2023**, rumors indicate a large-scale cyberattack against the DRC subsidiary of the pan-African bank **BGFI**. According to security researchers (notably expert Clément Domingo), clues on the dark web suggest that a group of ransomware has compromised BGFI RDC, is demanding a ransom of 55 Bitcoin (more than $1.5 million) and has already shared a list of supposedly stolen files. CYBERSECURITYMAG.AFRICA CYBERSECURITYMAG.AFRICA. However, the banking group has officially *denied* having suffered any attack, in a press release dated June 29, 2023 CYBERSECURITYMAG.AFRICA CYBERSECURITYMAG.AFRICA. BGFI says these allegations are "malicious, unfounded and defamatory", after verification with its security teams CYBERSECURITYMAG.AFRICA. Two possibilities remain: either the bank actually escaped an attack and the information was incorrect, or an intrusion took place but the institution chose to deny it publicly to preserve its reputation, having perhaps been able to contain it in time. Regardless, this incident (even if unconfirmed) demonstrates that **banks in the DRC** are targets for international cybercriminals, just like in the rest of the world. Already in 2019-2020, a group of hackers named **"Silence"**, originally from Eastern Europe, had led phishing campaigns targeting several banks in sub-Saharan Africa to infiltrate their systems CYBERSECURITYMAG.AFRICA. Attacks of this type – booby-trapped emails installing banking malware – have likely targeted Congolese establishments in the group, although few cases have been made public.

Furthermore, many smaller companies in the DRC may have been hit by ransomware or other malicious programs in recent years, without the matter necessarily emerging in the press. For example, the global wave of **WannaCry** in 2017 and other malware (Emotet, Trickbot, etc.) affected hundreds of thousands of systems around the world, including in Africa. According to statistics from Kaspersky Lab, the African continent recorded tens of millions of malware attacks in the first half of 2020 alone CYBERSECURITYMAG.AFRICA. It is therefore likely that Congolese companies or administrations using outdated Windows systems have been affected by these epidemics, suffering data encryption or disruptions, but without always reporting it publicly.

With: Financially motivated attacks are increasing in the DRC. The targets range from large logistics groups to banks, including SMEs. The dominant operating mode is **ransomware**, often introduced via **phishing** (phishing email containing a booby-trapped attachment or link) or exploiting vulnerabilities on unprotected servers. The consequences for victims are serious: business interruption, financial losses (either through ransom payment or restoration costs), damage to their image, and legal risks in the event of a leak of sensitive data. The authors are generally **organized cybercriminals**, operating from abroad (Eastern Europe, Asia, etc.) and affiliated with known ransomware gangs (NetWalker, Hive, LockBit, etc.). In the DRC, the response of affected companies consisted of calling on **security experts** to stem the attack, file a complaint, and communicate in a measured manner to avoid panic. However, the Bolloré incident shows that it is crucial to raise the level of preventive protection: security patches applied quickly, network segmentation, offline backups, and staff awareness of phishing attempts. BGFI's denial of attack also highlights the issue of *transparency* : Recognizing a cyberattack to mobilize appropriate response resources, while informing customers honestly, is preferable to leaking information through unofficial channels.

Online scams, account takeovers and digital fraud

The **cybercrime** in the DRC is also expressed through less visible attacks but just as pernicious for citizens and organizations: these are **online scams**, hacking of personal accounts and scams on digital networks. These practices often exploit the **user confidence** and the relative naivety of new Internet users who are not very aware of the risks.

A phenomenon that has been on the rise since the mid-2010s is that of **fake job offers on the Internet**. In the DRC, more and more fraudulent job advertisements are published online by individuals posing as recruiters or HR managers, with the aim of extracting money and personal data from job seekers. RADIOOKAPI.NET. For example, in 2017, Radio Okapi reported the resurgence of these scams: candidates apply for an attractive offer, then they are asked to pay "application fees" or training before hiring, only to ultimately discover that no position existed and that the "employer" was a scammer. This type of scam has claimed many victims among young Congolese graduates and unemployed people in recent years, taking advantage of high unemployment and the desperation of certain candidates willing to pay for a promise of employment.

In the same vein, impostors have usurped the identity of personalities or structures to deceive the public. We can cite the case that occurred in 2019 involving a **UDPS party executive** (presidential party): this individual defrauded citizens by promising them false recruitments in the public service, monetizing forms and induced costs, before being arrested RADIOOKAPI.NET. If the scam took place partly physically (via the delivery of documents against payment), it also relied on social networks to recruit victims, propagating the announcement of a "special hiring operation" in the name of the authorities. This case illustrates the porosity between cyber-scam and classic scam: the Internet offers an echo and apparent credibility (Facebook page, WhatsApp announcements) to scams then finalized in the real world.

Another common threat is **online account hacking** – in particular social network accounts (Facebook, WhatsApp) or messaging – with the aim of usurping the identity of the person and soliciting their contacts. The Congolese media related edifying testimonies: for example, a couple from Lubumbashi saw their Facebook account hijacked by a stranger who was sending messages to their friends claiming to be in urgent need of money. HABARIRDC.NET HABARIRDC.NET. Likewise, students have discovered fake profiles in their name, created to defraud acquaintances. This type of hacking, relatively simple (often via password theft or social engineering), causes direct harm to individuals and those around them: loss of money for those who fall into the trap, damage to the reputation of the victim whose image is misused, not to mention the violation of their privacy if messages or photos are exposed. There **mobile fraud** is also present: false SMS or WhatsApp messages pose as telephone operators or mobile money services (such as M-Pesa, Airtel Money), encouraging the user to communicate a code or call back a premium rate number, resulting in the theft of credit or funds. Although few official

statistics are available, these everyday digital scams probably constitute the most widespread form of cybercrime affecting the population in the DRC.

THE **consequences** of these online frauds are mainly financial and psychological: households sometimes lose substantial sums (employment scams can extort the equivalent of several months of local salary), and confidence in online services is eroded. In addition, these criminal acts are difficult to prosecute: they often involve isolated offenders or small, mobile and anonymous networks on the Internet. The Congolese law enforcement agencies, via specialized units (for example within the Judicial Police), have carried out some **operations** against this type of delinquency. We can cite the dismantling of networks of "grazers" (online scammers) operating from Kinshasa and Lubumbashi, sometimes in collaboration with accomplices abroad – although these cases are less publicized than large-scale attacks. On the preventive side, awareness campaigns are starting to emerge: local media publishing precautionary advice, NGOs and experts organizing workshops on digital security for the general public, etc.

With: Cybercrime scams take advantage of **human factors** and low general awareness. In the DRC, as elsewhere, cyber scams use social engineering more than technicality: false promises (employment, lottery winning, emergency aid), identity theft, romance scam, etc. Typical victims are unsuspecting Internet users or those in a situation of economic vulnerability. The amounts stolen, taken individually, may seem modest, but cumulatively they represent significant damage - difficult to quantify in the absence of official reports, but experts estimate that these frauds cost millions every year. **million dollars** to African citizens. The necessary response comes through a **digital education** reinforced: teach users to check job offers (contact the company directly, be wary of requests for money RADIOOKAPI.NET), to protect their accounts (robust passwords, two-factor authentication) and to never share sensitive information upon simple request. Several local initiatives, often supported by international organizations, aim to instill these good practices (see recommendations below).

Critical infrastructure attacks and technological fraud

Critical infrastructure – telecommunications, energy, transport, health – is a prime target for malicious actors, whether criminal groups seeking profit or acts of sabotage. In the DRC, over the last decade, there have been a few notable incidents falling into this category, although fewer than the attacks previously mentioned.

A significant case is the **telecom fraud by SIMBOX** revealed in **October 2018**. The Congolese National Police dismantled a network in Kinshasa involving several Chinese nationals, who had sophisticated equipment (*SIM box* and telephone equipment) to divert international telephone traffic TRESORKALONJI.PRO.



One of the Chinese subjects apprehended

Concretely, these boxes made it possible to *re-route* international calls entering the DRC, by routing them as if they were local communications, thus escaping official international pricing. This ploy, also known as **SIM boxing fraud**, causes a huge loss of income for the State and operators, because taxes and interconnection fees are not collected. In the Congolese case, the cumulative damage was estimated at nearly **120 million dollars USD** loss of income for the tax authorities TRESORKALONJI.PRO. Investigators found that fraudsters were even able to manufacture fake SIM cards locally, illustrating a well-established criminal supply chain. The 2018 police operation resulted in the arrest of the individuals involved and the seizure of equipment – a success in the fight against financial cybercrime. It highlights the importance of **monitoring the routing of telecom traffic** and the need to provide the Regulatory Authority (ARPTC) with technical means to detect this type of anomaly (for example, an unusual volume of local calls emanating from the same point). It was one of the first cases of this scale in the DRC linked to the **phreaking** (telephone hacking), showing that foreign actors can exploit flaws in the Congolese system on a large scale.

The infrastructure of **transport and logistics** have also indirectly suffered cyberattacks. An example is the cyberattack on the South African port company Transnet in July 2021, which paralyzed the port of Durban – the largest port in sub-Saharan Africa – for several days. This incident, although not specifically targeting the DRC, had repercussions on Congolese trade: Durban is a hub for the transport of goods to or from the DRC (a landlocked country for part of its territory) INTERPOLINT INTERPOLINT. Thus, a computer attack abroad may have delayed essential

shipments for the DRC, highlighting the interdependence of regional logistics chains. This makes the Congolese authorities aware of the fact that **cybersecurity of critical infrastructures** is not just an isolated national issue, but also depends on the robustness of international partners.

In the field of **health**, no major cyberattack was officially reported in the DRC during the period considered. Nevertheless, experts warn of the vulnerability of the sector. A report devoted to cyber threats in the health sector in the DRC highlights that the country's hospitals and clinics, in the process of digitization, could suffer serious consequences in the event of an attack: blocking of services, disclosure of confidential medical data, potential harm to human lives if vital systems are disrupted IJISRT.COM. This same report notes that cyber threats in the DRC are not *not taken very seriously* in the health sector for the moment, due to lack of awareness and resources. However, elsewhere in the world (including South Africa, Morocco, etc.), **ransomware** has already targeted hospitals, sometimes forcing the cancellation of surgeries or the postponement of urgent care. The DRC must therefore anticipate such eventualities by securing its hospital systems in advance and by having manual continuity plans.

Another critical aspect concerns the **energy and mining sector**. As the DRC is rich in natural resources (cobalt mines, coltan, gold, etc.), we can fear cyberattacks aimed either at spying on these industries (industrial cyber-espionage) or at disrupting production. No publicly documented attacks targeted, for example, the national electricity company (SNEL) or large mining companies during 2015-2024. However, the past saw a symbolic operation in 2012: *Operation Coltan*, claimed by Anonymous, which targeted the sites of companies exploiting Congolese coltan TRESORKALONJI.PRO. The stated aim was to denounce the conditions of mineral exploitation and the link between mining resources and armed conflicts in the DRC. This operation was part of a logic of **environmental hacktivism** and anti-capitalist (#OperationGreenRights), but did not have devastating technical consequences apart from a few disruptions to websites. She nevertheless recalls that the **multinationals linked to Congolese resources** can become targets – either of activists, competitors or states seeking access to strategic data (mining contracts, etc.). Vigilance is required, especially as many of these companies rely on SCADA systems, IoT sensors and digital tools that are potentially vulnerable if not properly secured.

With: The DRC's critical infrastructure has not yet experienced a public "catastrophic" attack, but several warning signs exist. The 2018 SIMBOX fraud revealed a **flaw in telecom monitoring** exploited on a large scale, depriving the State of significant resources TRESORKALONJI.PRO**.** Attacks in neighboring countries have had a **domino effect** on the Congolese economy (port of Durban 2021). The energy, transport and health sectors remain potentially exposed, often due to recent computerization without an integrated security strategy. It is crucial for the DRC to **inventory your sensitive infrastructure** and apply appropriate cybersecurity measures: segmentation of industrial networks, access control, updates of control systems, offline backups, emergency plans in the event of an incident, etc. Regional and international cooperation is also a key factor, because the disruption of one link can have cross-border consequences.

Measures taken and responses provided in the DRC

Faced with the rise of these multifaceted cyber threats, the DRC has gradually begun to deploy **response and reinforcement measures** cybersecurity, both at the government level and in the private sector and civil society. However, these efforts remain embryonic and fall short of the scale of the challenges to be met.

On **the institutional and regulatory levels**, the end of the 2010 decade marked an awakening at the top of the State. In September 2018, a few weeks before the elections, a **national summit** was organized in Kinshasa to consider the creation of a national computer incident response team (CERT or CIRT) HABARIRDC.NET. This initiative, encouraged by international recommendations (ITU, African Union), aimed to provide the country with a public structure for monitoring and rapid intervention in the event of a cyber attack. However, the project came up against bureaucratic rivalries: disagreements between the Ministry of Posts, Telecoms and New Information Technologies (initiator of the meeting), the Telecoms Regulatory Authority (ARPTC) and the Ministry of the Interior over the supervision of the future CERT HABARIRDC.NET HABARIRDC.NET. In the absence of clarification on institutional support and the legal framework, the national CERT did not see the light of day at that time – which has been compared to "putting the cart before the horse" without a solid legislative basis. HABARIRDC.NET.

At the legislative level, the DRC was falling behind. During the past decade, there was no **specific law on cybersecurity or modern cybercrime** in the DRC. Online offenses were prosecuted under the general provisions of the Penal Code (fraud, scam, sabotage) or telecoms laws, which are often unsuitable for new digital realities. Aware of this legal void, the community of experts recommended in 2018 that the government ratify the *African Union Convention on Cyber Security* (adopted in Malabo) and above all that it promulgates a law dedicated to cybersecurity HABARIRDC.NET. This involves providing the country with legal tools to define computer crimes, the penalties incurred, digital investigation procedures, the protection of personal data, etc. To date (2024), the specific law is still not in force, although a draft *"Digital code"* was mentioned. The DRC, however, created in 2021 a **Ministry of Digital**, proof of a desire to structure the country's digital development. This ministry, led by Minister Désiré-Cashmir Kolongele, has the mission of developing a national digital strategy integrating cybersecurity.

A notable advance took place in **2022** at the level of the Presidency of the Republic: a Congolese expert from the diaspora, **Nathalie Kienga**, was appointed Advisor in charge of cybersecurity and new technologies to President Félix Tshisekedi ID4AFRICA.COM ID4AFRICA.COM. She also serves as deputy head of the National Cyber Defense Council ID4AFRICA.COM ID4AFRICA.COM. The arrival of this specialist (with experience in Europe and initiator of an African Cybersecurity Institute in Kinshasa) within the governing bodies is a positive signal: there is now a **coordinating body** at the highest level of government to address cyber defense issues. We can expect this National Cyber Defense Council to contribute to finalizing the strategic framework (national cybersecurity

policy, clarification of roles between agencies) and to stimulating the creation of the national CERT.

On the side of **law enforcement**, the DRC has started to strengthen its capacities. The Police created **specialized cells** in cybercrime (attached to the Judicial Police and Intelligence) who collaborate with Interpol and regional police networks. Successes like the SIMBOX case of 2018 are partly attributable to these training efforts. Furthermore, the authorities are increasingly collaborating with independent experts: during major cyber incidents (e.g. Bolloré 2020 attack), private cybersecurity companies were called in to provide support. LEMAGIT.FR. The Congolese justice system has also started to deal with cases of cyber delinquency, relying on magistrates trained in these new issues (often thanks to workshops with the OIF or other partners). However, without specific law, prosecutions remain complex and require generic qualifications.

Measurement **techniques** were also taken by the targeted entities to protect themselves. For example, after the 2018 attacks, webmasters of government sites migrated certain portals to more robust and standardized hosting (previously scattered in various countries, cf. sites hosted in the USA, Germany, etc.). TRESORKALONJI.PRO). The CENI, for 2023, has clearly invested in high-performance firewalls and intrusion detection systems, which enabled it to block more than a thousand attacks on D-Day. RADIOGOFM.NET. We also note a change in mentality: the idea that *"this can happen to us too"* has established itself in Congolese business and administrative circles, especially after concrete incidents. Consequently, some Congolese companies are starting to subscribe to **assurances cyber** and to include IT risk management in their corporate governance.

Finally, the **civil society and the local tech community** play an increasing role in the response. Congolese organizations and experts are mobilizing for cybersecurity awareness and training. Let us cite the initiative **"Cyber Rebel"** launched in 2024 by the Africa Cyber Education foundation: a digital education program intended for young Congolese women, who during one-week workshops learn to identify online threats and adopt good security practices CIO MAGCOM CIO MAGCOM. During these sessions, key messages are transmitted, such as the importance of thinking before each digital action – *"Before each click, you have to ask yourself the question: does this action expose me to a cyber risk? »*, insists Nathalie Kienga, organizer of the event CIO MAGCOM. Likewise, tech communities (e.g. meet-ups *Google Developers Group* or *Tech Hub* in Kinshasa) integrate modules on cybersecurity into their meetings. The Congolese online press (Actualité.cd, Zoom Eco, Habari RDC, etc.) is publishing more and more popular articles on cyber threats and how to protect against them HABARIRDC.NET HABARIRDC.NET. This mobilization of citizens and the private sector is an essential complement to State action, by creating a breeding ground for local skills and collective vigilance.

Summary table of major incidents (2015-2024):

Date / Period	Target / Event	Type of attack	Main consequences
October 2018	Telecom fraud network in Kinshasa (SIMBOX)	**Phreaking** (SIMBOX, call diversion)	Network dismantled by the police, arrest of Chinese nationals; avoided tax losses estimated at **120 millions USD** TRESORKALONJI.PRO TRESORKALONJI.PRO.
Nov–Dec 2018	Government websites (Presidency, ministries, etc.)	**Defaçage/DDoS** for *Anonymous* (#OpCongo)	Approximately **8 official sites were hacked** or saturated for a few hours TRESORKALONJI.PRO. Anti-diet message displayed; domain vulnerability *.gouv.cd* exposed TRESORKALONJI.PRO. Calls to target **APPRECIATE** also launched TRESORKALONJI.PRO.
December 14, 2018	Electoral Commission (CENI)	**Hacking attempt** (DDoS, intrusion)	Attack announced by hacktivists opposed to voting machines HABARIRDC.NET HABARIRDC.NET. Some possible disturbances to the site, but no proven impact on the counting; internet cut as a precaution by the authorities after the vote (tense post-election context).
May 2020	Bolloré Logistics RDC (Logistics)	**Ransomware** (NetWalker)	Servers encrypted, operations disrupted. **Theft of sensitive data** (accounts, internal documents) partly disclosed online LEMAGIT.FR . Threat of massive publication if ransom not paid;

			complaint filed and investigation underway LEMAGIT.FR.
June 2023	BGFI Bank (DRC subsidiary)	**Ransomware** (unconfirmed, denied)	Hackers claim to have encrypted data and demanded **55 BTC** ransom CYBERSECURITYMAG.AFRICA. The bank **demented** publicly any attack CYBERSECURITYMAG.AFRICA. Incident reported but disputed, illustrating the difficulty of obtaining information on attacks suffered by banks.
December 15, 2023	CENI computer system	**Massive cyberattacks** (1,303 attempts)	Foreign intrusion attempts during partial legislative elections RADIOGOFM.NET RADIOGOFM.NET. **No success** : all attacks blocked, no disruption of voting or data leak. CENI was praised for its resilience.
June 2024	Website of the Ministry of ESU	**Website hacking** (indefinite)	Website rendered **inaccessible** a whole weekend DIGITALCONGO.ORG, disrupting student services. Return to normal in 48 hours. Incident highlighting the weakness of ministerial web security and the fear of academic data being compromised.

(Source: compilation of press articles and official press releases, see references)

Observed trends and recommendations to strengthen cybersecurity in the DRC

Examining these incidents over ten years reveals several **key trends** in the DRC:

- **Diversification of attacks** : threats are no longer limited to simple defacing of sites as in the 2000s. We observe a range ranging from political sabotage (hacktivism) to economic espionage (data theft), including purely financial extortion (ransomware) and scams targeting the general public. This diversification requires an equally versatile response from the authorities: technical, legal and educational.

- **More and more targets** : initially, it was mainly visible government sites that were targeted. Now any connected organization can become a target. THE **state institutions**, obviously, remain on the front line during sensitive periods (e.g. the CENI during elections), but the **private companies** (logistics, finance, mines, etc.) are just as threatened. Even individuals are affected through their accounts or their uses (scams). No one is “too small” to be attacked, which requires awareness at all levels.

- **Often transnational threats** : a striking feature is that many attacks involve foreign actors or infrastructure outside Congo. Anonymous hacktivists operate via Twitter and international hosting TRESORKALONJI.PRO, ransomware groups and telecom fraudsters come from other countries (Eastern Europe, Asia). This complicates attribution and repression, and highlights the importance of **international cooperation**. The DRC must work hand in hand with Interpol, the African Union and partner countries to track down cybercriminals who target it and exchange threat intelligence.

- **Awareness in progress but still incomplete** : the recent period shows an improvement in the defensive posture (e.g. the CENI has drastically improved its security between 2018 and 2023 RADIOGOFM.NET). The government has initiated some initiatives (Ministry of Digital, cyber defense council, bills), and the media are talking about the subject more than before. However, large parts of the public and private sector remain **underprepared** : few organizations have **an incident response plan** or a dedicated team, security audits are rare, and the idea that “cybersecurity is a priority” is not yet anchored everywhere. You only need to look at the ease with which a ministry was hacked in 2024 to be convinced.

In view of these findings, here are some **recommendations and areas for improvement** to strengthen cybersecurity in the DRC:

- **Strengthen the legal and institutional framework** : It is imperative to **adopt a cybersecurity law** and cybercrime. This text should clearly define offenses (intrusion, sabotage, cyber-fraud, etc.), provide dissuasive sanctions, and establish procedures for collecting digital

evidence. At the same time, the DRC should ratify international legal instruments such as the AU Convention on Cyber Security (Malabo) or even consider joining the Budapest Convention on Cybercrime. On the institutional level, the effective creation of a **CERT/R** (Computer Emergency Response Team) is a national emergency. Whether this CERT is attached to the Ministry of Digital, the ARPTC or the Presidency, it does not matter – it must be decided and put in place. This center would act as threat monitoring and technical support in the event of a major incident, in coordination with the CERTs of other countries. Without this structure, the response will remain ad hoc and scattered.

- **Increase resources and training** : The government must allocate **budgetary resources** specific to cybersecurity. This involves the equipment (network monitoring tools, malware analysis systems, forensic laboratories) but above all through the **human resources training**. It is recommended to train a core group of local experts: engineers and technicians capable of securing networks, testing the vulnerability of systems (pentests), detecting intrusions and responding to them. Law enforcement and magistrates also need capacity building in digital investigations (hard drive analyses, IP address tracing, etc.). Partnerships with friendly countries or international organizations could help organize these high-level training courses. Internally, each ministry and large company should appoint a **RSSI** (Information Systems Security Manager) or equivalent, to address these topics continuously.

- **Protect critical infrastructure** : Develop and implement **sectoral cybersecurity plans** for energy, mines, transport, health, finance. For example, auditing the security of SCADA networks of SNEL (electricity) and mining companies, imposing minimum standards on telecom operators for securing switches and gateways (in order to prevent new SIMBOX-type fraud). Update outdated hardware and software in these areas (some infrastructure may still be running Windows XP or unpatched systems, which is critical). Regularly simulate **cyber crisis exercises** involving these operators, to verify resilience and coordination in the event of a real attack. Furthermore, require strategic companies to have **continuity plans** to continue operating in degraded mode if their systems fail (e.g. hospitals with paper backup procedures, transport companies with radio communication in the event of an IT failure).

- **Raising awareness among the general public and organizations** : User education is the best shield against many attacks. It is necessary to multiply the **awareness campaigns** on good digital practices. This can take the form of TV/radio shows dedicated to cybersecurity (for example spots explaining how to spot phishing, how to choose a good password, the importance of not paying for a job offer, etc.), practical guides broadcast on social networks in French and local languages, or workshops in universities and schools. Companies should also train their employees (internal awareness programs) because a single human error can open the door to a hacker. Initiatives like *Rebel Cyber* must be encouraged and extended to other audiences (young people, entrepreneurs, civil servants, etc.). As a Congolese expert points out: *"Online insecurity seriously harms the privacy of users [...] However, there are always ways to protect yourself and limit the nuisance of cybercriminals"* HABARIRDC.NET HABARIRDC.NET– this message must be hammered home until basic digital hygiene becomes a reflex for everyone.

- **Development of a local cybersecurity ecosystem** : The DRC would benefit from stimulating the **birth of local cybersecurity companies** (consulting, auditing, software solutions) and to promote academic research in this area. For example, integrating cybersecurity modules into university computer science courses, supporting ethical hacking competitions (*hackathons*) to identify talents, creating a label or an association of Congolese cybersecurity professionals in order to share information on emerging threats. A solid ecosystem would make it possible to no longer depend solely on expensive foreign experts and to build strategic autonomy. Note that Congolese already play an international role (Nathalie Kienga and others), it is a question of using these skills to supervise the next generation on site.

- **Improve cooperation and transparency** : It is important that victims of attacks (whether institutions or companies) **report incidents quickly** to the relevant authorities, rather than hiding them. This allows the CERT/police to, in turn, alert other potential targets, trace channels, or even prevent an attack in progress on a third party. To encourage this, an anonymous or confidential reporting system could be put in place. In addition, the DRC should insert itself into information sharing networks (for example, join the AFRIPOL cyber network for Africa, or establish agreements with the CERTs of neighboring countries). The fight against cybercrime has no borders: an investigation into fraud in the DRC may require collaboration with Ivory Coast (for a "browser"), with China (for a pirate order server) or with the USA (for data hosted on an American cloud). It is therefore recommended to **establish international assistance protocols** specific to cyber (rapid mutual legal assistance to seize servers, exchange of data between CERTs, etc.).

- **Avoid counterproductive measures** : Finally, it should be noted that in response to the unrest linked to the elections, the Congolese authorities have in the past cut off access to the Internet or social networks (notably in 2016 and 2018). While these outages can temporarily prevent the spread of false news or make the task of remote hackers more difficult, they also heavily penalize the digital economy and freedom of expression. Organizations like Access Now have called on the DRC to **keep the internet open during the 2023 elections** and favor targeted cybersecurity solutions rather than widespread outages ACCESSNOW.ORG. The recommendation is to invest in the capacity to **filter malicious content** (e.g. remove fake profiles, counter bots, etc.) rather than using the "kill switch". A resilient and secure Internet must remain functional even in times of crisis.

In conclusion, the DRC is at a **digital turning point** : the past ten years have shown the reality and seriousness of cyberattacks that can hit it. The incidents caused notable damage but also served as **salutary warnings**. The country still has a **window of opportunity** to make up for delays in cybersecurity before a major attack occurs with potentially severe consequences (for example, massive sabotage of infrastructure or a leak of strategic state data). Efforts already initiated – whether governmental, private or citizen – must be intensified and coordinated. By prioritizing digital security in its agenda, the DRC will not only be able to protect its vital interests and its population, but also create a climate of trust conducive to the development of its emerging digital economy. As a local expert says, *"there is no point in having technical teams*

when the criminal and regulatory provisions are still lacking" HABARIRDC.NET: it is by conjugating **political will**, **adequate legal framework**, **human skills** And **technologies** that the DRC will succeed in significantly improving its cybersecurity for the coming decade.

Sources : Congolese and international press articles, reports from cybersecurity experts, official press releases and interviews (see references cited throughout the text). Each significant fact reported is based on at least one verifiable source, indicated in brackets in the body of the text.

Table of contents

General context and issues in the DRC....1
Attacks on government sites and public institutions....2
Ransomware and financial cyberattacks against businesses....4
Online scams, account takeovers and digital fraud....7
Critical infrastructure attacks and technological fraud....9
Measures taken and responses provided in the DRC....11
Summary table of major incidents (2015-2024):....14
Observed trends and recommendations to strengthen cybersecurity in the DRC....16

office@cyberastre.com © 2025