The Expanding Threat Landscape: *How* Cyberattacks *Are* Targeting Telecom Networks

Cybercriminals, hacktivists, and nation-state actors are all targeting telecommunications operators with more sophisticated and AI-augmented threats.

This article is part of the **Safeguarding the Digital Backbone: Building Resilient Telecom Infrastructure in Emerging Economies** series, produced by the International Finance Corporation (IFC, Note 1). Drawing on original IFC research into the cyber-readiness of telecom operators across Africa, Asia-Pacific, Europe, Latin America, and the Middle East, the series examines why cybersecurity has become a strategic imperative for the sector, and what operators, regulators, and development finance institutions (DFIs) can do to close the gaps. Each article stands alone and builds toward a practical picture of what resilient telecommunications infrastructure looks like in emerging economies.

- Article 1: From Connectivity to Critical Infrastructure: Why Cybersecurity is Now a Telecom Imperative
- **Article 2: The Expanding Threat Landscape: How Cyberattacks Are Targeting Telecom Networks**
- Article 3: Breaking Through Barriers: Cybersecurity Challenges Facing Telecom Operators in Emerging Markets
- Article 4: What Good Looks Like: Building a Cyber-Resilient Telecom Operator
- Article 5: Securing the Ecosystem: The Role of Regulators, Industry and Investors in Telecom Cyber Resilience

Cyberattacks against telecom operators have expanded in scope, sophistication, and frequency.

In April 2025, mobile operator MTN Group, which serves more than 300 million customers in 19 markets across Africa and the Middle East, reported that a threat actor had gained unauthorized access to customer data across multiple markets. MTN immediately activated its incident response processes, notified law enforcement, and warned affected customers (MTN Group 2025; Note 2). The company released few details on the breach, but according to its Ghana subsidiary, at least 5,700 customer records may have leaked.

Cybercriminals continue to deploy ransomware against enterprises, use phishing attacks powered by artificial intelligence (AI) against customers, and compromise telecommunications supply chains to expand their reach. Cybercriminals and nation-state operators are also increasingly using telecom-specific techniques to target networks and infrastructure, including compromising the signaling protocols used to exchange subscriber information, installing malware to intercept calls and data, and disrupting mobile financial services.

While the cyberthreat group behind the MTN breach is still unknown, the company is not alone in being targeted by cybercriminals. In February 2025, the HellCat ransomware group stole 380,000 records from a Romanian branch of the telecom giant Orange (Ilascu 2025). The Salt Typhoon nation-state cyberespionage group targeted telecommunications operators in Myanmar, South Africa, and Thailand (Insikt Group 2025). Additionally, in Latin America, hacktivists targeted a wide swath of the telecommunications industry in 2025, including providers in Brazil, Colombia, and Mexico (Intel471 2026).

Because telecom networks play a central role in the economies and digitalization of emerging markets, cyberattackers will continue to target these systems. As such, **network operators need to stay up-to-date with threat intelligence on their adversaries, especially the latest tactics, techniques, and procedures used against the industry**.

Two tiers of threat: Enterprise and Service-based

The two broad categories of threats include enterprise threats—such as ransomware, social engineering, and malware—and service-based threats, such as attacks on the signaling systems.

Enterprise threats are a broad class of attacks and compromises that affect all businesses and their information technology systems, including ransomware attacks, phishing attacks, zero-day exploits against edge devices, abuse of legitimate credentials, and malware (Figure 1). In October 2023, the Telecommunications Services of Trinidad and Tobago lost control of some of its service after an administrator's legitimate credentials were stolen, eventually leading to a ransomware attack (Julien 2024).

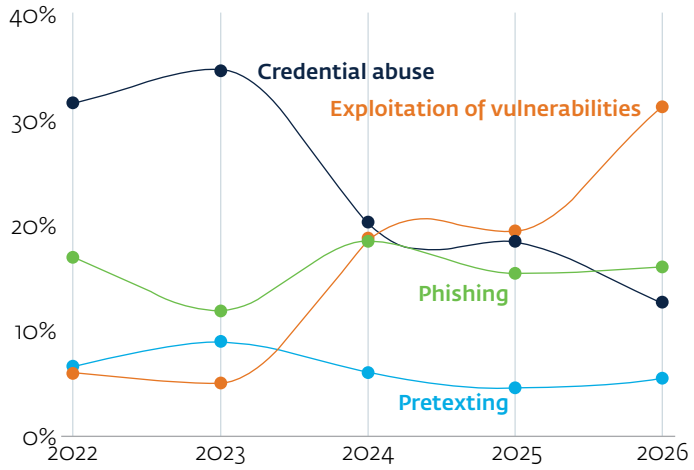
Credential abuse continues to be a major, if less common, threat, with both exploitation of vulnerabilities and phishing becoming more common (Figure 1).

Such incidents highlight the main threats to telecommunications firms. Ransomware and extortion have become an increasingly significant class of cyberattacks, involved in 48 percent of all breaches in 2026, up from 32 percent in 2024 (Verizon DBIR Team 2026, 11).

"Ransomware, cyber availability hindrance, and user access control [are] the triad of risks in the digital age that require vigilant governance," said Stephen Stryker, managing director and chief information officer for DigitalBridge, a global investor in digital infrastructure.

Figure 1

The Prevalence of Known Initial Access Vectors over Time



Source: Verizon DBIR Team 2026.

Telecommunication firms must also contend with service-based threats, specific to the industry, that can disrupt the communications networks underpinning critical functions such as mobile finance and government operations. For example, the Signaling System 7 (SS7) protocol for routing phone calls and exchanging information between different telecommunications providers is widely used in 2G and 3G networks. However, it lacks authentication, which enables threat actors to hijack numbers and intercept messages (Marczak and others 2020, 1–2). Even the newer Diameter protocol, which added authentication for 4G and 5G networks, is often run in a backward compatibility mode that retains the weaknesses of SS7 (Saalim Wani and others 2024).

> Ransomware, cyber availability hindrance, and user access control [are] the triad of risks in the digital age that require vigilant governance.
>
> — **STEPHEN STRYKER**
> Managing Director and Chief Information Officer
> *DigitalBridge*

The distinction between enterprise and service-based threats is collapsing. Attackers increasingly use corporate entry points, such as phishing, credential theft, and third-party access, to bridge to network-layer exploitation. The multistage approach defeats defenses designed for single-vector attacks and is widely used by state-sponsored actors, who prioritize telecoms alongside public administration and transportation (ENISA 2025a).

Cyberattacks surge irrespective of region

In late 2024, Telecom Namibia in Southern Africa was struck by ransomware, resulting in the leak of more than 400,000 customer records, including sensitive data on government officials (Lemos 2025). The telecommunications firm refused to pay the ransom (refusal is widely considered a best practice), and the ransomware group Hunters International published the stolen information on the dark web (Khaitan 2024). Data leaks typically do not hobble operations, but do have real costs: reputational damage can be significant, costing firms in potential compliance penalties, investigation and response fees, and the expenses required to retain customers.

While ransomware is a major threat to the telecommunications sector, other types of attacks from a diverse group of sources continue to target digital-network providers in emerging markets. No region, operator type, or architecture has been spared.

Salt Typhoon appears to have compromised dozens of telecommunication providers since 2024. While many of the breached organizations are in North America and Europe, the group also targeted firms in Argentina, Bangladesh, Indonesia, Malaysia, Mexico, Thailand, and Viet Nam (Insikt Group 2025).

In a similar attack, a cyberthreat group disrupted the Viasat KA-SAT telecommunications service for weeks in an attack that coincided with Russia's invasion of Ukraine, demonstrating how telecom infrastructure can be targeted as an instrument of geopolitical disruption without attribution to any single actor (Viasat 2022).

As geopolitics grows more polarized, hacktivism has become increasingly common, with many groups targeting a variety of businesses, including telecommunications firms. For example, in 2025, a group of self-described North African hacktivists calling themselves Keymous+ claimed attacks against hundreds of organizations in emerging markets, including in India and several African nations, such as Egypt and Morocco. About 10 percent of their targeted victims were telecommunications firms (Meidan 2025).

AI and the evolving attack toolkit

The cyberthreat landscape continues to evolve and shift in response to the latest technologies and common defenses. The as-a-service approach to productizing complex offensive hacking and cyber operations capabilities into easy-to-use services continues to be popular, with distributed denial-of-service and ransomware-as-a-service offerings already widespread.

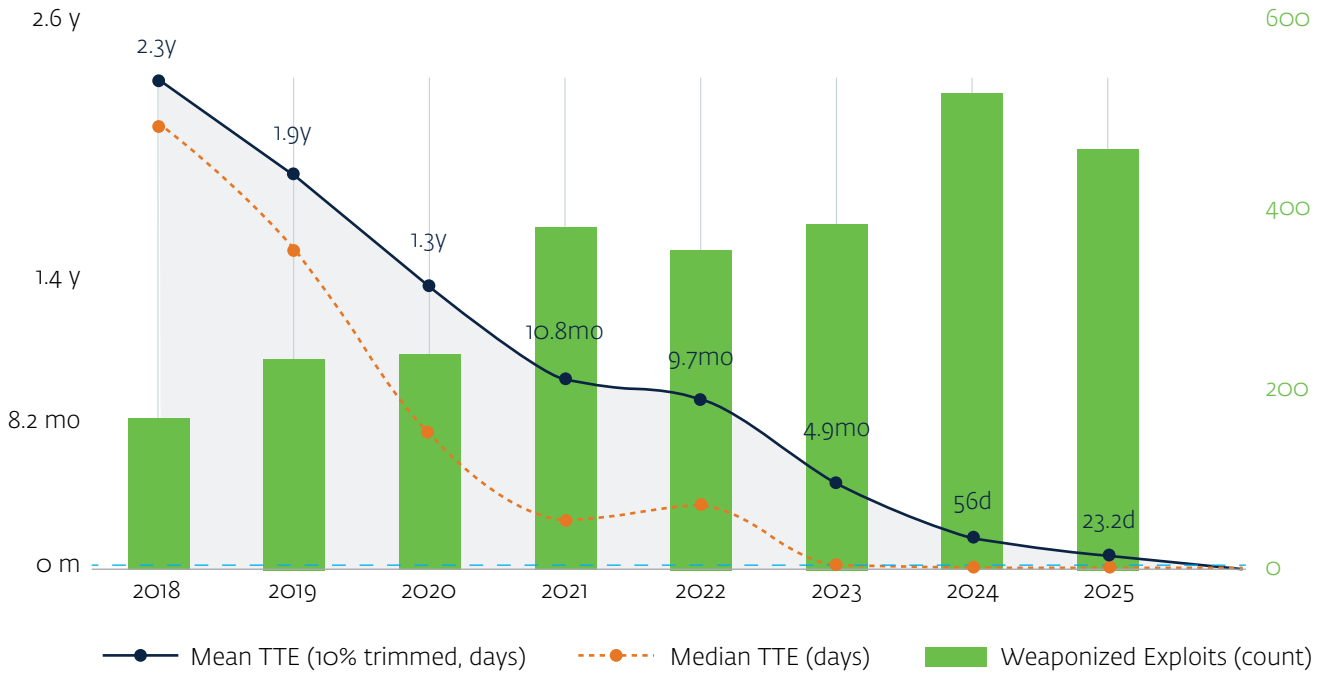
The two most popular methods that attackers use to gain initial access to businesses' networks continue to be phishing and software exploitation. In Q4 2025, exploitation of public-facing applications accounted for 40 percent of one cybersecurity firm's incident-response engagements, while phishing accounted for about 33 percent (Liebenberg 2026).

AI has impacted both. With the November 2022 release of ChatGPT, cybercriminals have quickly adopted a variety of AI techniques to augment their expertise and create more sophisticated attacks. For example, language barriers used to be a major problem for fraudsters, which enabled most potential victims of phishing to easily discern any non-native messages. With AI, that is no longer the case: users now click malicious links in phishing emails 54 percent of the time, up from 12 percent prior to the adoption of AI (DeGrippo 2026).

AI has also accelerated the discovery of software vulnerabilities and the development of attacks—or "exploits"—for those vulnerabilities (Figure 2). In 2022, attackers needed about 10 months to create an exploit from a vulnerability report, typically as the disclosure of an issue when assigned a Common Vulnerabilities and Exposures identifier. That time has now dropped to 20 hours in 2026 (Evron, Mogull, and Lee 2026, 8). Overall, the ability to quickly go from vulnerability disclosure to working exploit means cybercriminals effectively operate at the

Figure 2

AI-Driven Decline in Mean Time to Exploit



Source: Evron, Mogull, and Lee 2026.

Note: TTE = time to exploit.

same level as nation-state actors.

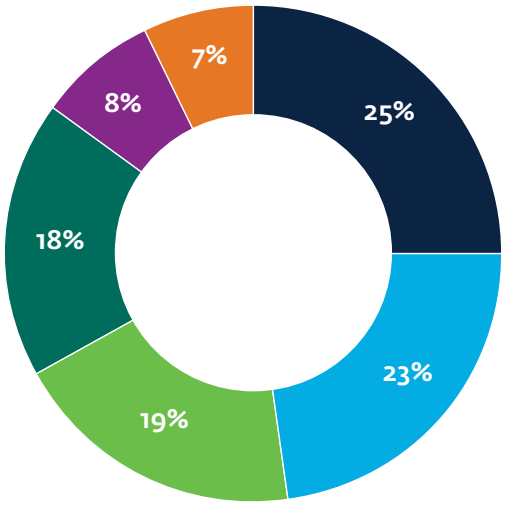
Finally, AI is also being used directly in cyberattack operations. In April 2026, the United Kingdom's AI Security Institute found that two advanced models, Anthropic's Mythos and Open AI's GPT-5.5, could complete a 32-step attack chain without human intervention (AISI 2026). Attackers have experimented as well. For example, an attack on nine Mexican government agencies earlier this year made widespread use of popular AI models, creating a playbook in the form of a long prompt that implemented their attack using both Anthropic's Claude and OpenAI's ChatGPT systems (Nelson 2026).

The solution for defenders such as cybersecurity teams is to integrate AI detection, analysis, and response into their own infrastructure. "Defenders need to adopt AI to keep up," said Ismail Faiz, head of cloud, architecture, and cybersecurity at Dhiraagu, a Maldivian telecommunications company. "AI and machine learning are both assets and risks, requiring us to strengthen our defenses and stay alert against the constantly changing threats of ransomware and phishing."

The top potential uses of AI in cybersecurity are automated response and remediation, fraud detection, network anomaly detection, and attack and risk prediction using real-time data, according to a 2025 survey of telecom operators conducted by GSMA Intelligence (GSMA 2025) (Figure 3).

Figure 3

Potential Cybersecurity Benefits of AI Applications



Source: GSMA Intelligence Operators in Focus Security Survey, July 2025.

Telecom-specific vulnerabilities

While ransomware, AI-powered attacks, and cybercrime-as-a-service affect all organizations globally, some threats are more concerning to telecommunications companies in emerging markets, including supply-chain and vendor compromises, SS7 and Diameter protocol attacks, cloud misconfigurations, and insider threats.

Supply-chain risks

Telecom operators in emerging markets, with limited in-house security capacity, rely heavily on international equipment vendors and regional managed service providers. While each relationship adds expert services and operations, they also extend the cybersecurity perimeter that needs to be defended. The average company in the information sector had 25 third-party relationships detectable externally, which are typical software-as-a-service subscriptions or cloud services (Cyentia 2023; Note 3). All vendor and third-party relationships are typically many times that number.

Network-service vulnerabilities

On the network side, the Signaling System 7 (SS7) and Diameter legacy signaling protocols were originally designed for a trusted community of interconnected operators and lack the basic authentication and validation mechanisms of Internet Protocol networks. Operators in emerging markets still widely use 2G and 3G networks that rely on these protocols, placing them at risk from vulnerabilities. A single threat actor conducted more than 1,700 SS7 attacks between October 2023 and April 2025, with 92 percent of that traffic linked to location-tracking operations (Miller and Lange 2026).

Growing attacks surface area

The rapid digitization and adoption of cloud services in emerging markets have resulted in a growing attack surface area that is often misconfigured. Stolen but still legitimate credentials can often be leveraged to gain access to cloud services used for telecom operations. Even limited access to misconfigured or unsecured cloud assets and capabilities can result in the leak of consumer data (GSMA 2026).

Misconfiguration and insider errors

Finally, inadvertent insider errors and malicious insider activity continue to be major problems for companies. End users and developers are common parts of the attack chain, contributing to more than 75 percent of breaches (54 and 22 percent, respectively). Insider errors, such as misconfiguration or the leak of credentials or development secrets, can lead to wider breaches. Malicious insider attacks are far less common, but when they do take place, the impact can be significantly more damaging (Verizon DBIR Team 2026, 58).

> Defenders need to adopt AI to keep up.

— **ISMAIL FAIZ**
Head of Cloud, Architecture and Cybersecurity
Dhiraagu

The investment gap and lack of collaboration

Cyberthreat actors experiment and adopt new technologies quickly. Telecommunications providers in emerging markets need to take a similar approach in adopting the latest cybersecurity technologies to close the gap between attackers and defenders. Globally, telecommunications, media, and technology companies have already begun closing the gaps, raising cybersecurity investments by 125 percent over five years, compared to a doubling of investments (+100 percent) for all global companies, according to risk-rating firm Moody's (Kapko 2024).

More visibility into attackers' tactics is also needed. Like many regulated industries, incident reporting in the telecom sector is constrained by real or perceived compliance and reputational consequences. For example, the European Union Agency for Cybersecurity's annual telecom incident reports capture only major incidents—those with significant impacts—while smaller, more frequent incidents are not systematically counted (ENISA 2025b). Regional telecoms should cooperate with others in their industry to collect intelligence on attacks and attackers' tactics.

Cross-border cooperation continues to face complex technology and geopolitical issues, especially as different regions—Asia, Europe, and North America—pursue different regulatory cybersecurity frameworks for telecommunications companies and other businesses (Geller 2026). Despite the different approaches, operators must shift from siloed defense to collective threat intelligence sharing. This structural change, which requires both regulatory mandate and industry collaboration, can help them be better prepared for future attacks.

"Future-proofing cybersecurity means embracing advanced threat intelligence with mature processes, broad risk management integration, and active industry collaboration to stay ahead of evolving threats," said Suresh Sankaran Srinivasan group head for cybersecurity and data privacy at Axiata, a Malaysian telecommunications provider.

Telecom operators should assess the threats that currently pose the greatest risk to their business. Part of this effort should be to collect the latest information on the types of threats and attacks that target their industry. While some threat actors are opportunistic, others will focus on specific industries and particular regions, making the well-informed organization the best defended.

NEXT IN THE SERIES: ***ARTICLE 3 | BREAKING THROUGH BARRIERS***
The next article explores the structural barriers that make these threats harder to address in emerging markets, including legacy infrastructure, cybersecurity talent gaps, regulatory fragmentation, budget constraints, and geopolitical supply-chain risks.

Endnotes

1. The development of this series was financially supported by the World Bank Cybersecurity Multi-Donor Trust Fund and guided by German Cufre, Director of Access & Affordability. It was delivered as a team effort led by Charlotte Kaheru, with key contributions from Maurice Kaleek Isaac, Massiel Lopez, and Morshed Haque. Significant contributions from Lemos Associates LLC are gratefully acknowledged. The series was informed by a foundational study conducted by IFC in collaboration with Ernst & Young LLP (EY), with appreciation extended to Kunal Bhatia, Partner – TMT Consulting, EY, Ashrut Mahajan, and the broader EY working team. Special thanks are extended to the customers, partners, and stakeholders who contributed to the study and this series, including external peer reviewers. Acknowledgment is also extended to IFC and World Bank colleagues, as well as the Communications teams—including Chris Vellacott, Rob Wright, and Brian Beary—whose feedback helped shape the study and this series.
2. MTN Group's business statistics come from the About Us page, MTN Group, Johannesburg, South Africa (accessed June 1, 2026), https://www.mtn.com/about/.
3. The Cyentia Institute report did not break out data for the telecommunications sector. The closest matching category is the information sector.

References

AISI (AI Security Institute). 2026. "Our Evaluation of OpenAI's GPT-5.5 Cyber Capabilities." AISI Blog, April 30, 2026. https://www.aisi.gov.uk/blog/our-evaluation-of-openais-gpt-5-5-cyber-capabilities.

Cyentia Institute. 2023. *Close Encounters of the Third (and Fourth) Party Kind*. SecurityScorecard, New York. https://securityscorecard.com/resources/research/cyentia-close-encounters-of-the-third-and-fourth-party-kind/.

DeGrippo, Sherrod. 2026. "Threat Actor Abuse of AI Accelerates from Tool to Cyberattack Surface." Microsoft Security Blog, April 2, 2026. https://www.microsoft.com/en-us/security/blog/2026/04/02/threat-actor-abuse-of-ai-accelerates-from-tool-to-cyberattack-surface/.

ENISA (European Union Agency for Cybersecurity). 2025a. *ENISA Threat Landscape 2025*. ENISA, Athens. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

ENISA (European Union Agency for Cybersecurity). 2025b. *Telecom Security Incidents 2024*. ENISA, Athens. https://www.enisa.europa.eu/publications/telecom-security-incidents-2024.

Evron, Gadi, Rich Mogull, and Robert T. Lee. 2026. The *'AI Vulnerability Storm': Building a 'Mythos-Ready' Security Program*. Cloud Security Alliance, Seattle. https://labs.cloudsecurityalliance.org/wp-content/uploads/2026/04/mythosreadyv92.pdf.

Geller, Eric. 2026. "Moody's Forecasts Growing AI Threats, Regulatory Friction for 2026." *Cybersecurity Dive*, January 8, 2026. https://www.cybersecuritydive.com/news/moodys-cyber-outlook-forecast-2026/809101/.

GSMA (Global System for Mobile Communications Association). 2026. *GSMA Mobile Telecommunications Security Landscape 2026*. GSMA, London. https://www.gsma.com/solutions-and-impact/technologies/security/gsma-mobile-telecommunications-security-landscape-2026/.

Ilascu, Ionut. 2025. "Orange Group Confirms Breach After Hacker Leaks Company Documents." *Bleeping Computer*, February 25, 2025. https://www.bleepingcomputer.com/news/security/orange-group-confirms-breach-after-hacker-leaks-company-documents/.

Insikt Group. 2025. "RedMike (Salt Typhoon) Exploits Cisco Vulnerabilities for Cyber Espionage." Recorded Future, February 13, 2025. https://www.recordedfuture.com/research/redmike-salt-typhoon-exploits-vulnerable-devices.

Intel471. 2026. *Latin America's Cyber Threat Landscape Report*. Intel471, Wilmington. https://www.intel471.com/resources/whitepapers/region-report-latin-america-2025.

Julien, Joel. 2024. "Report: Hackers Accessed TSTT Using Admin's Credentials." *Daily Express*, February 24, 2024. https://trinidadexpress.com/business/local/report-hackers-accessed-tstt-using-admin-s-credentials/article_41215060-d38d-11ee-8bdd-ab92c0ffcc5d.html.

Kapko, Matt. 2024. "Telecom, Media and Tech Companies Are Cyber Defense Standouts: Moody's." *Cybersecurity Dive*, June 7, 2024. https://www.cybersecuritydive.com/news/tmt-sector-defense-standouts/718380/.

Khaitan, Ashish. 2024. "Telecom Namibia Hit by Massive Cyberattack: Over 400,000 Files Leaked." *The Cyber Express*, December 16, 2024. https://thecyberexpress.com/telecom-namibia-cyberattack/.

Lemos, Robert. 2025. "Ransomware Targeting Infrastructure Hits Telecom Namibia." *Dark Reading*, January 8, 2025. https://www.darkreading.com/cyberattacks-data-breaches/ransomware-targeting-infrastructure-telecom-namibia.

Liebenberg, Dave. 2026. "IR Trends Q4 2025: Exploitation Remains Dominant, Phishing Campaign Targets Native American Tribal Organizations." Cisco Talos Blog, January 29, 2026. https://blog.talosintelligence.com/ir-trends-q4-2025/.

Marczak, Bill, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert. 2020. *Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles*. University of Toronto, Toronto. https://utoronto.scholaris.ca/items/a6e38e89-ffe3-4bc1-9ebf-3e8177ad7039.

Meidan, Ori. 2025. "Keymous+: A New Hacktivist Collective or a DDoS-as-a-Service Brand in Disguise?" Radware Research Blog, July 2, 2025. https://www.radware.com/blog/threat-intelligence/keymous-plus-a-new-hacktivist-collective-or-a-ddos-as-a-service-brand/.

Miller, Gary, and Swantje Lange. 2026. "Bad Connection: Uncovering Global Telecom Exploitation by Covert Surveillance Actors." Citizen Lab, April 23, 2026. https://citizenlab.ca/research/uncovering-global-telecom-exploitation-by-covert-surveillance-actors/.

MTN Group. 2025. "MTN Cybersecurity Incident, but Critical Infrastructure Secure." Press Release, April 24, 2025. https://www.mtn.com/mtn-cybersecurity-incident-but-critical-infrastructure-secure/.

Nelson, Nate. 2026. "AI-Driven Cyberattack on Mexico Couldn't Breach OT Systems." *Dark Reading*, May 7, 2026. https://www.darkreading.com/ics-ot-security/worlds-first-ai-driven-cyberattack-couldnt-breach-ot-systems.

Saalim Wani, Mohamad, Michael Rademacher, Thorsten Horstmann, and Mathias Kretschmer. 2024. "Security Vulnerabilities in 5G Non-Stand-Alone Networks: A Systematic Analysis and Attack Taxonomy." *Journal of Cybersecurity and Privacy* 4 (1). https://mc-lab.de/publications/2024-01-attack-taxonomy-5g-nsa/paper.pdf.

Verizon DBIR Team. 2026. 2026 *Data Breach Investigations Report*. Verizon, New York. https://www.verizon.com/business/resources/reports/dbir/.

Viasat. 2022. "KA-SAT Network Cyber Attack Overview." Viasat, March 30, 2022. https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/.