DARKTRACE

The State of Cybersecurity

in the Global Telecommunications Sector

Disclaimer

This report is for informational purposes only. While every effort has been made to ensure the accuracy and completeness of the findings, the conclusions are based on available data, which may change over time.

The information does not constitute legal, financial, or professional advice, and readers should consult relevant experts for specific guidance.

The views expressed in this report are those of the authors and do not necessarily reflect the views of any specific organization or governmental entity. The report does not guarantee the security of any systems, and ongoing vigilance and adaptive strategies are required to address emerging threats. This report is provided "as is," without warranties or representations, express or implied, regarding accuracy or completeness.

No liability is accepted for any damages or losses arising from the use or reliance on the content.

Acknowledgements

This report is intended to highlight the current challenges the telecommunications sector faces, particularly in the Europe, the Middle East and Africa (EMEA), Americas (AMS) and Asia-Pacific (APAC) regions.

Telecommunications infrastructure, including mobile networks, internet service providers, satellite communications, and undersea cables, forms the backbone of modern digital society.

As nations and industries become increasingly interconnected, the resilience of these systems is paramount.

A successful cyber-attack on telecommunications networks could disrupt critical communications, compromise sensitive data, and destabilize national security and economic operations.

This report explores some of the key threat actor groups, emerging threats, and strategic imperatives for safeguarding the telecommunications ecosystem.

We would like to extend our sincere appreciation to the telecommunications professionals, cybersecurity experts, and industry stakeholders who generously shared their time, insights, and experiences with us throughout this research.

Their openness and depth of knowledge have been instrumental in shaping our understanding of the complex and rapidly evolving cyber landscape within the telecommunications sector. We are also grateful to the Darktrace Analyst and Incident Response teams for their invaluable support and collaboration during the course of this study.

Authors:

Emily Megan Lim, Justin Torres, and Qing Hong Kwa

Thank you to the following of their contributions:

Emma Foulger, Nathaniel Jones, and Nicole Wong.

And a special thank you to

Jack Pearson

Contents

Executive Summary

The telecommunications industry, at the epicenter of today's digital revolution, faces an increasing array of cyber threats.

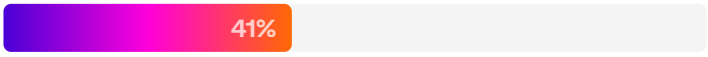
This report provides a comprehensive overview on the cybersecurity challenges with 5G adoption, the perspectives of Chief Information Security Officers (CISOs) on these critical issues, an overview of the current threat landscape, major threat actors, and Darktrace observations across this sector.

The advent of 5G technology has brought about unprecedented speed and connectivity, but with it comes enhanced cybersecurity risks. The vast number of connected devices, the introduction of network virtualization, and the increased complexity of 5G networks have expanded the attack surface for potential cyber threats.

The legacy of first generation (1G), second generation (2G), third generation (3G), and fourth generation (4G) networks has accumulated significant technical debt, due to rapid advancements in technology and the pressure to quickly roll out new capabilities. This debt, in the form of outdated infrastructure, inefficient processes, and patchwork solutions, often leads to vulnerabilities in the system. These vulnerabilities, combined with the complexity of integrating new technology with old systems, provide potential entry points for intrusions.

CISOs' perspectives and risk management toward security and new emerging technologies illustrate the business challenges of constant uptime delivery while maintaining and managing legacy infrastructure, but also highlight risks in supply chain management, adoption of AI, and how geopolitical drivers can impact their security posture.

Despite strong consensus that AI-powered security defenses will significantly improve cyber resiliency, only 41% of security leaders agreed that their existing security capabilities are adequate to defend against these threats, which is lower than the average across other Critical National Infrastructure (CNI) organizations.



Furthermore, at the start of 2025 most telecommunications organizations were still discussing formal policies on the safe and secure usage of AI. A key priority was implementing security controls to prevent the unwanted exposure of corporate data.

Commonly observed attacks across the telecommunications sector were:

- data breaches, phishing
- SIM swapping
- SIM cloning
- ransomware
- and protocol targeting.

These attacks were highlighted via the Confidentiality, Integrity, and Availability (CIA) Triad often applied in cybersecurity risk management. The initial access vectors associated with these attacks involved entry via edge infrastructure such as virtual private networks (VPNs) and firewalls, and the exploitation of older vulnerabilities, legacy infrastructure and dormant accounts.

The Darktrace Threat Research team observed activity across the EMEA region that is assessed with varying levels of confidence to be linked to Chinese nation-state threat actors, most likely Liminal Panda.

While existing research has mainly associated Liminal Panda victimology with telecommunications organizations, the close interconnection between the energy and telecommunications sectors suggests a potential broader impact.

The telecommunications industry, being the backbone of the digital revolution, has a crucial role in safeguarding the digital space. In the AI era, it is incumbent upon all stakeholders in this industry to collaborate and create a safe and secure digital environment.

Objectives and Methodology

Research Objectives

This research analyzes the historical and current threat landscape for the telecommunications sector across EMEA, the AMS and APAC.

It does so by exploring:

- The cybersecurity implications of digital transformation within the sector, particularly in relation to 5G technology
- Key security considerations for CISOs in the sector
- The main threat groups and attack vectors targeting the sector
- Darktrace incident observations involving telecommunications customers

Methodology

This research focuses on the EMEA, AMS and APAC telecommunications sectors. Open-source intelligence (OSINT), Darktrace incident data and alert metadata were analyzed to identify attacker tactics, techniques, and procedures (TTPs).

The findings were applied to threat hunting frameworks, namely the Diamond Model of Intrusion Analysis [1] and Mandiant's A4 Framework [2], to craft four hypotheses for hypothesis-driven threat hunts. Based on these, hypothesis-driven threat hunts were conducted, and AI-driven experimental anomaly detection models were created to test the hypotheses across the telecommunications customer base.

Definitions

Critical National Infrastructure (CNI) is defined by UK National Cyber Security Centre (NCSC) as national assets that are essential for the functioning of society, such as those associated with energy supply, water supply, transportation, health and telecommunications [3].

In the U.S., 16 sectors are currently designated as CNI. In the UK, there are 14, with "Data Centers" newly added in September 2024—marking the first new designation in a decade, following "Space" and "Defense" in 2015 [4].

In this research, organizations are classified using the UK Standard Industrial Classification (SIC) codes [5]. These codes are grouped into broader industry sections, such as Information and Communication or Manufacturing. Telecommunications is a division within the Information and Communication section.

In this report, the term "sector" generally refers to these section-level classifications. However, in the case of the Telecommunications sector, it specifically denotes the division under the Information and Communication section.

For this report, the term "telecommunications sector" refers to any company that contributes to the production, distribution, or consumption of telecommunications resources.

These resources include various types of equipment and hardware, network software and infrastructure, and the personnel responsible for maintaining and operating these systems. In addition, we include Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs) within the scope of the telecommunications sector, as their roles in delivering, securing, and managing network services are closely aligned with the broader ecosystem of telecommunications.

Darktrace models leverage anomaly detection and integrate outputs from Darktrace Deep Packet Inspection, telemetry inputs, and additional modules, creating tailored threat detection.

Darktrace applies Self-Learning AI to an organization's data to understand and identify anomalies specific to them. The research in this report leverages insights gained from Darktrace's model alerts, which are raised when observed activity is deemed to be anomalous. Each alert contains metadata such as timestamps, source and destination IP addresses, and the protocols used.

Understanding Technical Debt

in Current Telecommunications Security

The fifth generation of mobile network technology (5G) represents a transformative leap in the telecommunications sector, reshaping both its infrastructure and strategic direction. With global investments in 5G infrastructure projected to exceed USD 1 trillion between 2020 and 2025 [6], 5G is not merely an upgrade—it is the foundation for next-generation connectivity.

Its capabilities, including ultra-low latency, high-speed data transfer, and massive device connectivity, are enabling innovations across industries such as healthcare, manufacturing, and transportation.

As telecommunications providers pivot toward 5G to unlock new revenue streams and support digital transformation, the technology is becoming the backbone of modern communication systems. However, this rapid evolution also introduces a broader and more complex cyber threat landscape. To understand the current state of the security challenge in the telecommunications sector, it is helpful first to understand how security has evolved alongside technological progression.

1G to 2G: The Era of Minimal Security

The first generation (1G) of mobile networks, launched in the 1980s, relied on analog transmission with no built-in security mechanisms. This left communications vulnerable to eavesdropping and device cloning. A notable example was the widespread cloning of analog mobile phones in the 1990s, where attackers intercepted analog signals to duplicate phone identities and make fraudulent calls [7].

The transition to the second generation (2G) introduced digital encryption and Subscriber Identity Module (SIM)-based authentication, marking the beginning of mobile security. However, early encryption standards such as A5/1 and A5/2 were later found to be weak. International Mobile Subscriber Identity (IMSI) catchers—also known as Stingrays—became a common surveillance tool, exploiting 2G's lack of mutual authentication to intercept calls and messages [8].

3G: Strengthening Authentication and Encryption

With the advent of the third generation (3G), mobile networks adopted stronger encryption algorithms and mutual authentication protocols. These improvements significantly reduced the risk of unauthorized access and man-in-the-middle attacks. However, rogue base stations and downgrade attacks remained a threat. Attackers could force devices to fall back to 2G or 3G from 4G, exploiting weaker security protocols [9].

In 2010, researchers demonstrated how fake base stations could be used to intercept 3G traffic by exploiting protocol downgrades, highlighting the persistent vulnerabilities in transitional network environments [10].

4G: IP-Based Architecture and Internet-Style Threats

The fourth generation (4G) marked a shift to Internet Protocol (IP)-based architecture, enabling high-speed data transmission and advanced services such as Voice over Internet Protocol (VoIP) and high-definition (HD) video streaming. While 4G networks implemented stronger security mechanisms than their predecessors, the move to IP-based infrastructure also introduced new vulnerabilities—particularly those resembling traditional internet threats.

One prominent area of concern involves the Diameter signaling protocol, which replaced SS7 in 4G networks.

Although designed to be more secure, Diameter has been shown to suffer from misconfigurations and trust-based vulnerabilities. These weaknesses can be exploited to launch signaling storms—a form of denial-of-service (DoS) attack where excessive or malformed signaling messages overwhelm the network.

Real-world incidents have demonstrated how such storms can lead to subscriber service disruptions and network instability, even though specific operators are rarely named publicly. For example, EXFO and GSMA have both documented how signaling storms can arise from device reconnection loops or malicious traffic patterns, causing widespread degradation of service [11] [12].

Additionally, legacy SS7 vulnerabilities persist in 4G environments due to continued reliance on fallback services like SMS and voice. These inherited flaws allow attackers to track users, intercept messages, and manipulate signaling traffic, even on modern LTE networks.

5G: Expanding the Attack Surface

Security in 5G is significantly enhanced through features such as network slicing, zero-trust architecture, and improved encryption. However, the complexity and virtualization of 5G infrastructure introduce new risks. In 2022, researchers from the U.S. National Security Agency, Cybersecurity and Infrastructure Security Agency (CISA), and Office of the Director of National Intelligence (ODNI) identified vulnerabilities in 5G core network slicing that could allow attackers to access or disrupt services across slices if misconfigured [13]. Moreover, early 5G deployments often relied on non-standalone (NSA) architectures that interoperated with legacy 3G and 4G systems, inheriting their vulnerabilities such as General Packet Radio Service Tunneling Protocol (GTP) flaws and exposure to spoofing and DoS attacks [14].

As telecommunications companies strive to stay at the forefront of technology, there is often a race to deploy the latest networks, like 5G, sometimes at the expense of fully addressing inherent systemic issues. The legacy of 1G, 2G, 3G, and 4G networks has accumulated significant technical debt, due to rapid advancements in technology and the pressure to quickly roll out new capabilities. This debt, in the form of outdated infrastructure, inefficient processes, and patchwork solutions, often leads to vulnerabilities in the system. These vulnerabilities, combined with the complexity of integrating new technology with old systems, provide potential entry points for attackers.

However, despite the associated risks, telecommunications providers cannot simply switch off these older networks. Many devices and systems, including some emergency services and rural areas, still rely on these older networks due to compatibility issues or lack of access to newer technology.

Furthermore, each generation of technology comes with its own set of security protocols, and integrating these disparate systems can lead to gaps in security.

Hence, while striving for advancement with 5G, it is crucial for telecommunications companies to address the technical debt and security issues from previous generations, to fortify their systems against potential cyber threats.

This technical debt in the current 5G telecommunications environment poses a significant challenge for security teams and CISOs who are left managing this risk.

Generation	Key Features	Security Capabilities	Common Threats	Notes
1G 1980s	Analog voice only	No encryption or authentication	Eavesdropping, cloning	Extremely insecure; no built-in security
2G 1990s	Digital voice, SMS, basic data	Basic encryption (A5/1, A5/2), SIM authentication	SMS spoofing, IMSI catching (Stingrays), weak encryption	Introduced digital security, but easily broken today
3G 2000s	Mobile internet, video calls	Stronger encryption (KASUMI), mutual authentication	Man-in-the-middle (MITM), rogue base stations	Improved security, but still vulnerable to downgrade attacks
4G 2010s	High-speed data, VoIP, HD streaming	IP-based security (IPSec, LTE security), mutual authentication	Signaling storms, DDoS, SS7 vulnerabilities	More secure, but exposed to internet-based threats
5G 2020s	Ultra-low latency, IoT, massive connectivity	Enhanced encryption, network slicing, zero-trust architecture	Supply chain attacks, IoT botnets, slicing misconfigurations	Most secure yet, but broader attack surface due to IoT and virtualization

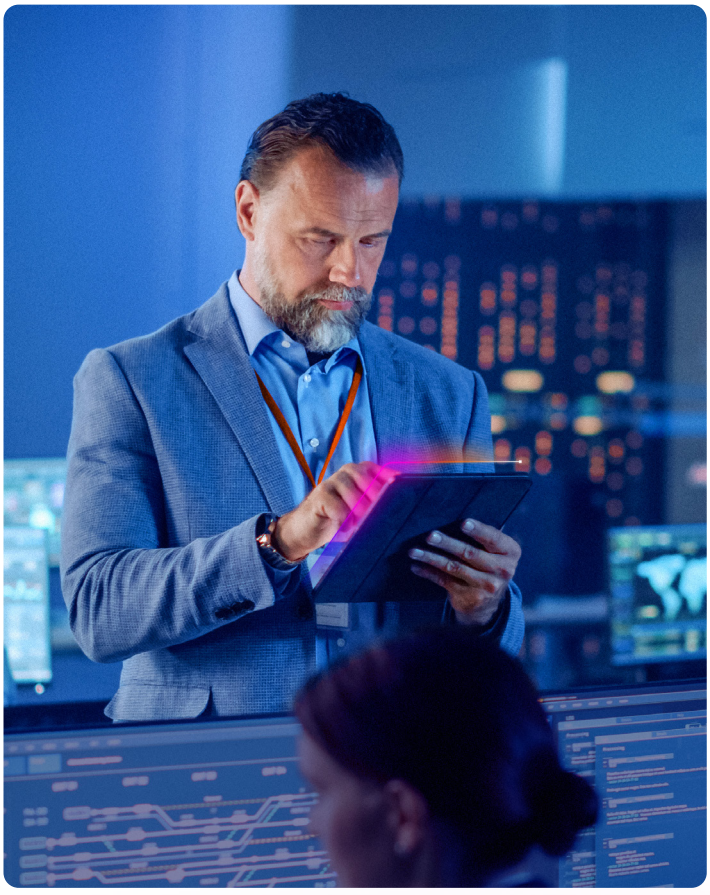
CISO Perspective

On Assessing Risks in the Telecommunications Sector

While nation-state threat actors are a key threat across the telecommunications industry, CISOs must also understand and assess a wide range of risks as part of their business function.

As part of this research, Darktrace conducted interviews with security leaders from telecommunications organizations at the start of 2025. Below are four main themes that CISOs in the telecommunications sector expressed concern about:

01	The impact of AI on privacy, security, and trust
02	Security management in the 5G Era
03	Supply chain and technical debt
04	Geopolitical drivers increasing business risk



Risk 1: The impact of AI on privacy, security, and trust

As organizations embrace AI tools, benefiting from their ability to streamline workflows, reduce false positives, and enable the detection of never-before-seen threats, the need for AI will only become more urgent.

Threat actors are racing to take advantage of the transformative potential of AI, and leading SecOps programs, including those in the telecommunications sector, are doing the same [15]. AI adoption within the sector places the trustworthiness of telecommunications companies under further scrutiny. Yet, as of the start of 2025, most organizations were still discussing formal policies on the safe and secure use of AI.

A key priority for security leaders was implementing security controls to prevent the exposure of corporate data. In contrast, organizational readiness to use AI to defend against today's cyber threats generally falls behind this appetite to adopt AI for operational growth.

Darktrace found that:

- Most security leaders in telecommunications organizations agree that AI-powered cyber threats already significantly impact and will continue to have a significant impact on their organization in the next few years.
- Despite strong consensus that AI-powered security defenses will significantly improve cyber resiliency, only 41% of security leaders believe their existing security capabilities are sufficient to defend against these threats, which is lower than the average across other CNI organizations.
- The most commonly used type of AI reported by security leaders in their current security stack is generative AI. It also appears to be the most widely understood type of AI among security leaders, compared to other types (supervised/unsupervised, deep learning and neural networks, generative adversarial networks, natural language processing, etc.).
- Security leaders are optimistic about the benefits of AI, strongly agreeing that AI is critical to freeing up time for their security teams to become more proactive. To reap the benefits of AI in securing growth, telecommunications organizations must deepen their understanding of AI application in security beyond generative AI and recognize the importance of security as an enabler of digital transformation.

Risk 2: Security management in the 5G era

As organizations move towards rolling out 5G technologies, they are, in turn, introducing new security risks. One of the most critical risks introduced by 5G is network slicing. Network slicing brings several advantages to the telecommunications sector. It enables providers to allocate resources dynamically, optimizing performance for diverse use cases, such as autonomous vehicles, smart cities, or industrial Internet of Things (IoT) environments. Although network slicing is still an emerging technology, research and industry observations have already highlighted its potential as a cybersecurity attack vector [16].

A 2022 survey by GlobalData and Nokia revealed that up to 75% of telecommunications providers had experienced security breaches in their 5G networks, with many incidents linked to misconfigured network slices [17].

These misconfigurations exposed slices to threats such as DoS attacks, man-in-the-middle attacks, and unauthorized access. While specific breach details remain confidential, industry experts believe such attacks are already occurring, especially as standalone 5G infrastructure becomes more widely deployed.

These examples underscore the urgent need for telecommunications operators to implement zero-trust architectures, enforce strict slice isolation, and adopt continuous monitoring to secure the dynamic and complex environment introduced by network slicing [18].

Risk 3: Supply chain and technical debt

telecommunications operators rely on hardware, software and services from third-party vendors, introducing additional cybersecurity risks. While most CISOs conduct thorough risk assessments of their suppliers, scrutinizing their security protocols, compliance with industry standards, there is still only so much that any single operator can control.

In a notable campaign, Chinese state-sponsored group Salt Typhoon exploited unpatched vulnerabilities in Cisco IOS XE software to compromise internet-facing devices used by global telecommunications providers that were over five to eight years old. This underscores the importance of implementing "Secure by Design" principles, such as not having hard-coded credentials in an array of network management products. It also emphasizes the need for substantive vendor risk management practices including vulnerability scans and patch management, while highlighting the challenge that telecommunications organizations have maintaining and managing legacy infrastructure [19].

Risk 4: Escalation in geopolitical conflicts

According to the World Economic Forum's Global Cybersecurity Outlook 2025, escalating geopolitical tensions are significantly influencing the cyber threat landscape.

The report highlights that nearly 60% of organizations have adjusted their cybersecurity strategies in response to geopolitical risks, and a third of CEOs are specifically concerned about cyber espionage and the loss of sensitive information due to global conflicts [20].

With current economic headwinds and regional conflicts, escalating geopolitical conflicts can significantly disrupt the telecommunications industry by causing supply chain issues, increased costs, and challenges in meeting consumer demand.

These tensions are driving more strategic and destructive cyber operations, especially against critical infrastructure sectors like telecommunications. This shift is further supported by the International Monetary Fund (IMF), which notes that cyberattacks—particularly ransomware—are increasingly used to disrupt essential services, with some incidents causing widespread outages across critical infrastructure systems [21].

Threat Landscape and Attack Trends

in Telecommunications

Overview of the threat landscape

The telecommunications industry continues to face a rapidly evolving threat landscape, with cyberattacks often targeting the confidentiality of customer data and the availability and integrity of telecommunications services.

As telecommunications providers handle large volumes of sensitive information and operate critical infrastructure, they are frequent targets for financially motivated cybercriminals and state-sponsored threat actors. Notable among these are Evasive Panda [22], Salt Typhoon [23], and Liminal Panda [24], which have been linked to cyber espionage campaigns aimed at intercepting sensitive communications, compromising infrastructure, and exfiltrating data from telecommunications operators.

In recent years, the frequency and severity of these attacks have escalated, driven by the expansion of 5G networks, the prevalence of IoT devices, and the growing geopolitical significance of telecommunications infrastructure [25].

Notable recent attacks in the telecommunications sector

In February 2022, a cyberattack targeted Viasat's KA-SAT satellite network, disrupting communications across Ukraine and parts of Europe.

The attack, attributed to the Russian military intelligence (GRU), aimed to cripple Ukraine military command and control systems as Russian forces launched their invasion. This act of cyber warfare highlights the strategic role of digital infrastructure in modern conflicts [26].

In December 2023, Ukrainian's largest telecommunications provider, Kyivstar, experienced a massive cyberattack that disrupted services for millions of customers. The attack also affected businesses, including banks and Ukraine's air raid warning system [27].

In 2024, CISA discovered that Salt Typhoon had infiltrated the networks of several major U.S. telecommunications companies to conduct surveillance and espionage activities [28].

CIA Triad Framework

The CIA triad—Confidentiality, Integrity, and Availability—provides a useful framework for understanding the different cyber threats to the telecommunications sector and their impact on telecommunications organizations [29].

Each of these principles needs to be upheld to ensure secure and reliable operations of telecommunications networks and services. Understanding this framework in the context of telecommunications provides a structured lens through which to assess cyber risks.

CIA Triad applied to telecommunications sector:

	Role in Telecommunications	Targets/Attack Types
Confidentiality	▪ Protect sensitive customer data and communications ▪ Ensure privacy and compliance with data protection regulations	▪ Data breaches via phishing or malware ▪ Espionage targeting call records and surveillance data
Integrity	▪ Maintain accuracy of transmitted data ▪ Ensure trust in billing, routing, and delivery service	▪ Data tampering to disrupt services ▪ Man-in-the-middle attacks altering communications
Availability	▪ Guarantee continuous access to telecommunications services ▪ Support emergency communications and national infrastructure	▪ Distributed Denial of Service (DDoS) attacks causing service outages ▪ Ransomware disabling critical systems

Confidentiality

Confidentiality of data remains a primary target, with data breaches being one of the most common outcomes of cyber-attacks on telecommunications companies.

Data Breaches

In the past two years, a significant proportion of cyber incidents in the sector have resulted in the theft of customer data, including personally identifiable information and account credentials [30]. This stolen data is often sold on the dark web, where it can be used to facilitate further attacks such as SIM swapping.

In most cases, threat actors did not need to employ advanced techniques to gain unauthorized access and merely exploited basic security gaps in their targets' infrastructure. This included using stolen usernames and passwords to get into systems [31], or taking advantage of known software vulnerabilities that had not been patched [32] [33].

Phishing

In 2024, Darktrace detected phishing attacks targeting telecommunications companies that involved credential harvesting, adversary-in-the-middle (AitM) techniques, and fake invoice scams. Some of these campaigns also abused legitimate services such as ClickUp and Dropbox Sign (formerly known as HelloSign). However, in addition to targeting telecommunications employees, phishing campaigns also frequently impersonate telecommunications brands themselves.

In early 2024, **over 15,000 phishing campaigns** were themed around the telecommunications and media industry, with companies like AT&T among the most impersonated brands [34]. Ultimately, this shows how threat actors are also exploiting brand trust to deceive users and harvest credentials.

■ Darktrace case study

VIP phishing of a technology and software provider to telecommunications organizations

The Microsoft 365 account of a VIP user from a technology and software supplier to telecommunications organizations was compromised in an attacker-in-the-middle attack. The attacker used an e-signature service to send a phishing email spoofing the company's HR department. The email directed the user to enter their credentials and MFA tokens if required into a fake human resources (HR) website, which the attacker used to log into the VIP's Microsoft account. The attacker proceeded to view sensitive files on SharePoint that appear to contain Intellectual Property (IP).

This case exemplifies how telecommunications organizations are also vulnerable to supply chain risks.

The targeting of a VIP of a supplier demonstrates clear motives; to collect sensitive data from one organization that has access to multiple, critical organizations. For defenders, the exploitation of legitimate services and possible bypass of MFA emphasizes the importance of moving away from signature-based detections and adopting a multi-layered, cross-domain platform approach to threat detection and response.

Integrity

The integrity of telecommunications networks refers to the trustworthiness and accuracy of data and services, ensuring that communications are not tampered with and that users are who they claim to be. Threat actors have abused the integrity of telecommunications networks during identity-based attacks that manipulate or impersonate subscriber information. Two prominent examples are SIM swapping and SIM cloning attacks, which allow attackers to hijack or duplicate a user's mobile identity.

SIM swapping and SIM cloning

SIM swapping, or SIM hijacking, is a social engineering attack in which a threat actor convinces a telecommunications provider's customer service representative to transfer a victim's phone number to a SIM card under the attacker's control. Once the number is ported, the attacker gains control over the victim's calls and text messages, allowing them to intercept one-time passwords (OTPs) and bypass two-factor authentication (2FA) on banking, email, and other sensitive [35]. This compromises the integrity of telecommunications services by allowing unauthorized access to personal communications and services that rely on mobile verification [36].

SIM cloning involves duplicating a legitimate SIM card by extracting its unique identifiers, such as the International Mobile Subscriber Identity (IMSI) and the authentication key (Ki) [37].

Once cloned, the attacker can use the duplicated SIM to impersonate the victim on the mobile network and, like SIM swapping attacks, it allows the attacker to intercept communications, including OTPs that can be used to bypass 2FA. In some cases, both the original and cloned SIMs can operate simultaneously, making detection more difficult and increasing the risk of prolonged unauthorized access.

This undermines the integrity of telecommunications networks by allowing multiple devices to operate under the same subscriber identity, leading to unauthorized access and potential data leakage.

These types of successful attacks are particularly concerning given the prolific nature and impact of ransomware groups like Scattered Spider [36], which have targeted critical infrastructure using these tactics.

Availability

Telecommunications networks are frequently targeted by ransomware campaigns and DDoS attacks, which could impact the availability of telecommunications services.

Ransomware

Ransomware incidents in the telecommunications industry have been particularly notable, with a reported 177% increase of such incidents in the first half of 2024 [38] [39]. These attacks often encrypt critical systems and demand payment for decryption, disrupting services and placing immense pressure on operators to restore functionality quickly.

■ Darktrace case study

Ransomware attack on African Communications Services Provider (CSP)

Darktrace detected Crytox ransomware in an African CSP. Unlike other more prominent ransomware groups, this group does not typically employ double extortion attacks and drops the uTox messenger application on affected devices to enable the victim to communicate with them [40]. In this case, the attacker gained initial access to the network through exploiting a VPN.

The attacker then exploited a legacy service account, 'monitor', to move laterally through the telecommunications organization's environment. The username suggests the service account is used for network monitoring and thus has high levels of privilege and access across the network, likely to be bypassed on security tools too.

Over two million files were encrypted over SMB and the attackers deployed uTox on an FTP server that had external connectivity enabled. The time to escalate from the mid-stages of the attack, reconnaissance, to encryption and impact, was merely 36 minutes, demonstrating the speed at which the attackers operated.

This case highlights the importance of securing edge infrastructure in telecommunications organizations, and ensuring continuous monitoring of all credentials, including service credentials that attackers leverage for easy access across the network.

It also emphasizes the importance of implementing basic security best practices around account management.

■ Darktrace case study

Internal denial of service on African Mobile Network Operator

Darktrace detected what was likely a compromise involving multiple intrusion sets that rendered an African mobile network operator's application server inaccessible. In a similar initial access vector to the case of Crytox ransomware, an attacker gained access to another African telecommunications organization's internal network via their corporate VPN.

Once inside, the attacker also exploited a dormant domain admin account for lateral movement via RDP. However, the attacker exhibited different techniques and objectives during this multiple intrusion set attack with longer dwell time than the aforementioned case, to impact the Availability and Integrity of the network.

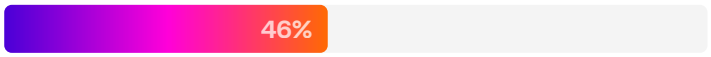
A Linux privilege escalation vulnerability, namely CVE-2016-5195, that has reportedly existed since 2007 and actively exploited from 2016, was used to delete the root accounts on an application server and create an attacker-controlled account named 'firefart' [47] [48]. No indicators of data exfiltration were observed; however, data exfiltration may have already occurred as indicators of a Raccoon Stealer 2.0 infection were detected in the organization's network months prior to this.

Raccoon Stealer 2.0 is a Malware-as-a-Service (MaaS) information stealer known to steal credentials saved in browsers, but also has keylogging capabilities. The likely involvement of multiple threat actors in different but potentially interconnected compromises underlines the interest that groups with various underlying motivations have in targeting telecommunications organizations, and the value of access to these organizations.

The techniques leveraged in this attack also highlight the challenges of managing legacy infrastructure within telecommunications organizations and emphasizes the importance of maintaining good cyber hygiene and continuous monitoring of privileged accounts, particularly within these legacy environments.

DDoS attacks

DDoS attacks, which aim to overwhelm network infrastructure and cause service outages, also saw a 46% increase during the same period [41].



These attacks are often carried out using a botnet and some botnet owners may even advertise DDoS-as-a-service on the Dark Web [42] [43]. Botnets rely on a large number of infected devices rather than centralized command-and-control (C2) servers, making it harder to detect and mitigate using traditional signature-based defense methods.

Malware infections can enable large-scale control of devices, potentially for use in botnet-driven attacks. While not a botnet itself, the Lumma Stealer malware illustrates the scale reached by certain malware strains and the efforts required to take down infrastructure: **between March and May 2025, over 394,000 Windows devices were compromised globally.**

In May 2025, Microsoft, in collaboration with law enforcement and industry partners, disrupted Lumma's infrastructure by seizing or redirecting **over 1,300 domains** [44].

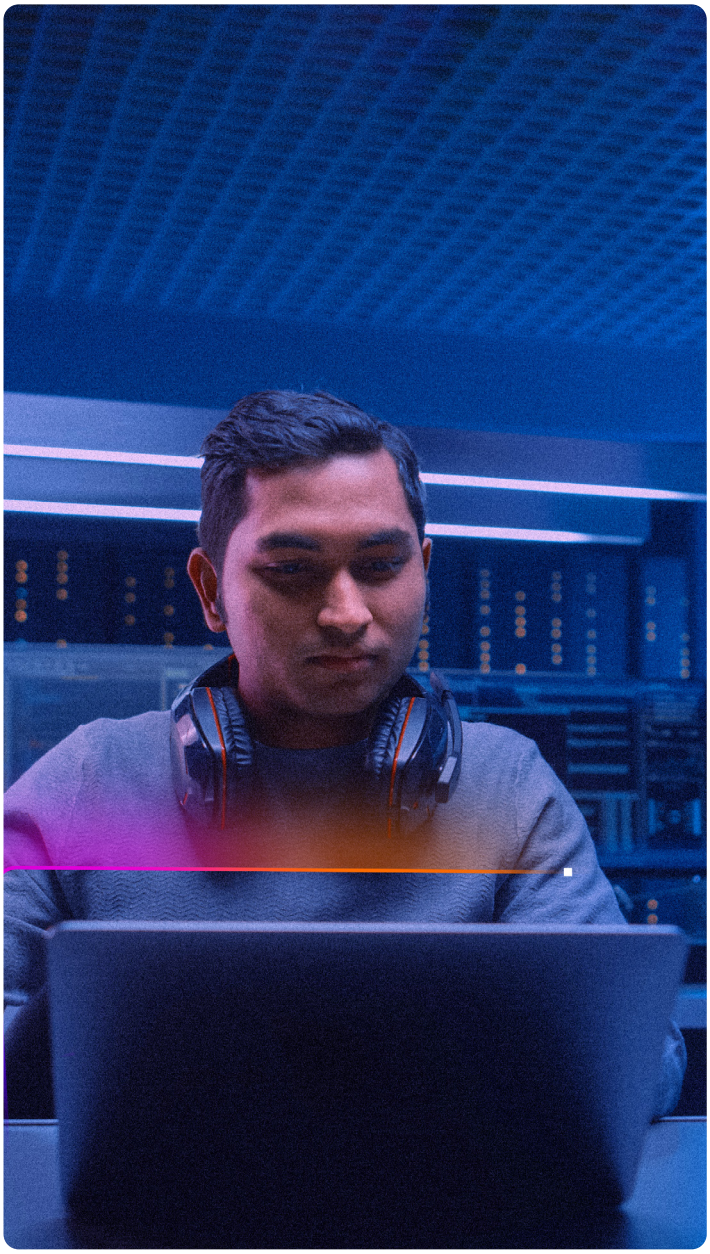
DDoS attacks on telecommunications providers can cause major disruptions to phone and internet services, which could potentially have an impact on hotlines for emergency services and banks as well [45]. In May 2025, a regional telecommunications provider in the US was forced to take its network offline after facing a cyberattack, resulting in widespread outages for mobile services. While the company did not confirm the exact nature of the attack, the sudden and widespread outage raised strong suspicions of a DDoS attack [46]

Protocol Targeting

Besides the CIA framework, another useful way to understand the threat landscape in the telecommunications sector is knowing what protocols are commonly used and their associated vulnerabilities which can be targeted in various attacks.

Telecommunications protocols are used to transmit a variety of sensitive information. By targeting these protocols, threat actors can gain unauthorized access to this information, which can include everything from personal data to state secrets.

SS7 and Diameter-based attacks demonstrate how threats faced by the telecommunications industry can stem from weaknesses in the underlying signaling protocols that manage voice, messaging, and data services. These protocols were often designed and developed decades ago, with little consideration for modern cybersecurity threats.



As telecommunications networks continue to evolve to support 4G, 5G and beyond, weaknesses in protocols will continue to be a target for attackers. Some of the most commonly targeted protocols in telecommunications networks include:

SIGTRAN: SIGTRAN is used for transporting SS7 signaling over IP networks. It inherits many of the vulnerabilities of SS7, making it a target for similar types of attacks, such as eavesdropping and fraud.

GTP: GTP is used in 3G, 4G, and 5G networks for data transfer. It can be exploited for attacks like fake GTP packets, leading to unauthorized access and disruption of network services.

Session Initiation Protocol (SIP): SIP is used for initiating, maintaining, and terminating real-time sessions in IP networks, including voice and video calls. Common attacks include SIP flooding (DoS attacks) and SIP spoofing, which can lead to unauthorized access and call interception.

Stream Control Transmission Protocol (SCTP): SCTP is used for signaling in IP networks. It can be targeted for DoS attacks and other exploits that disrupt communication.

Mobile Application Part (MAP): MAP is a protocol which enables real time communication between nodes in a mobile cellular network. It is used in GSM networks for various signaling tasks. It can be exploited for attacks similar to those targeting SS7, such as location tracking and intercepting communications.

Remote Authentication Dial-In User Service (RADIUS): RADIUS is used for authentication and accounting in network access. It can be targeted for attacks that aim to gain unauthorized access to network resources.

Home Location Register (HLR) and Visitor Location Register (VLR): These are databases used in mobile networks to store subscriber information. Attacks on HLR and VLR can lead to unauthorized access to subscriber data and manipulation of network operations.

IP Multimedia Subsystem (IMS): IMS is used in 4G and 5G networks to deliver multimedia services. It can be targeted for attacks that disrupt service delivery and gain unauthorized access to multimedia content.

Threat Profile Spotlight

Salt Typhoon

Note: Salt Typhoon is noted to have overlaps in tactics, techniques and procedures (TTPs) and tooling with other threat groups such as GhostEmperor, FamousSparrow, and Earth Estries. In this research, Darktrace has treated these groups as aliases or closely affiliated entities under the broader designation of Salt Typhoon for the purpose of analysis and attribution.

Salt Typhoon is a Chinese-nexus advanced persistent threat (APT) group known for its sophisticated cyber espionage activities, active since at least 2019 [49]. The group demonstrates a high level of operational maturity, leveraging both advanced malware and legitimate tools to conduct long-term espionage. Their previous targets include government organizations, critical infrastructure sectors such as energy and telecommunications, as well as educational institutions.

The group has been observed leveraging exploits, typically used to gain initial access through vulnerabilities in internet-facing devices such as Microsoft Exchange and VPN solution servers [50]. There have also been recent reports on Salt Typhoon exploiting vulnerabilities in Cisco software [19].

Salt Typhoon's arsenal consists of custom malware such as GHOSTSPIDER, MASOL RAT, SNAPPYBEE (Deed RAT), and DEMODEX rootkit. They also frequently use living-off-the-land binaries (LOLBINs) and legitimate administrative tools such as WMIExec, PsExec [51].

Liminal Panda

Note: Liminal Panda is noted to have overlaps in TTPs and tooling with other groups such as LightBasin, UNC1945 and Decisive Architect. In this research, Darktrace has treated these groups as aliases of Liminal Panda for the purpose of analysis and attribution.

Liminal Panda is a Chinese-nexus APT group also known for its sophisticated cyber espionage activities and has been active since at least 2016. While they have an exceptionally advanced skill level, they typically leverage external Domain Name System (eDNS) servers, which are part of GPRS network and play a role in roaming between different mobile operators, to connect directly to and from other compromised telecommunications companies' GPRS networks via Secure Shell (SSH) and through previously established implants.

They also incorporate robust research and development capabilities to target vendor-specific infrastructure commonly seen in telecommunications environments (including the ability to fingerprint various brands of network hardware).

Attack vectors include the exploitation of external-facing devices such as routers and gateways, accessing eDNS server via SSH from another compromised telecommunications company by password spraying extremely weak and third-party-focused passwords, leveraging SGSN emulation software with TinyShell. SGSNs are GPRS network access points, emulation software allows adversary to tunnel traffic via telecommunications networks [52].

Threat Hunting

The formation and utilization of hypotheses can be instrumental in directing threat hunting efforts. Hypotheses help to give focus to the threat hunting process by predicting the types of threats that might be present and suggesting where to look for them.

The Darktrace observed incidents, OSINT findings, and APT spotlights informed hypotheses-driven threat hunts across the telecommunications sector customer base. In this case, Darktrace focused on threat actor TTPs that have been observed and attributed to Liminal Panda and Salt Typhoon.

Hypotheses

The hypotheses crafted and tested were:

01 Chinese-nexus threat actors will target internet-facing servers and exploit vulnerabilities such as ProxyLogon to gain initial access, deploy web shells for long-term persistence, and enable lateral movement within the network.

02 Chinese-nexus threat actors will leverage Living off the Land (LOTL) Techniques, targeting Windows endpoints and servers, leveraging built-in Windows utilities like PSExec and WMIC to execute malicious payloads while evading detection.

03 Salt Typhoon will establish Generic Routing Encapsulation (GRE) tunnels between compromised devices and their infrastructure for C2 communications and data exfiltration, while potentially bypassing network monitoring.

04 Liminal Panda will target the telecommunications sector/related systems in the GPRS network via eDNS servers. Initial access with the eDNS server via SSH will typically occur via password spraying attacks. Liminal Panda will aim to return access to several eDNS servers from one of the compromised telecommunications entities while deploying a range of different types of malware and backdoor tools.

Key Findings

Darktrace Global Observations: A Spotlight on indicators of likely Liminal Panda activity

The geopolitical significance of cyberattacks in the telecommunications sector is reflected by findings from a threat hunt conducted by Darktrace's Threat Research team, using metadata associated with Liminal Panda activity from across the customer base. The hunt revealed moderate-confidence activity from organizations of geopolitical significance to China-nexus threat actors.

Darktrace observed with moderate confidence:

Inbound DNS requests and outbound external activity to various IPs and ports attributed to Liminal Panda
Outbound anomalous external connections, including with a Liminal Panda subnet
Password spraying of multiple Software-as-a-Service (SaaS) accounts from a Liminal Panda IP, used to compromise eDNS servers
Unusual outbound external connections, including SSH, to a likely Chinese target of interest in the telecommunications sector

Case 1:

Password spraying attack on European satellite operator

Darktrace observed a password spraying attack on the network of a European satellite operator, originating from infrastructure associated with Liminal Panda.

These attempts were aimed at the SaaS accounts of high-ranking engineering managers who are likely to have access to sensitive and privileged information. Previously, Liminal Panda actors have used password spraying techniques on eDNS servers. However, the recent focus on SaaS accounts, which serve as an initial point of entry but also likely have access to confidential information, could potentially signal a shift in objectives from espionage within GPRS to intellectual property theft.

These attempts coincided with the period when the targeted organization was reportedly involved in defense contracts with the European government and was adhering to pro-Ukrainian sanctions against Russia and Iran. The geopolitical efforts to reduce China's investment in European and Western telecommunications infrastructure, coupled with the targeted organization's participation in the Low Earth Orbit race, align with the apparent motivations of the threat actor to gain access to the organization's SaaS environment and sensitive information.

Case 2:

Likely targeting of edge infrastructure at an African energy distributor

While existing research has mainly associated Liminal Panda victimology with telecommunications organizations, the energy and telecommunications sectors are highly interconnected. In one case, Darktrace observed likely Liminal Panda infrastructure receiving data over HTTP from the firewall of an African energy distributor. The energy distributor's location was consistent with the geographical location of previous Liminal Panda targets.

CSPs often incorporate energy generation and storage capabilities at cell sites that generate energy which can be sold back to power grid operators.

Energy providers can leverage CSP networks as unofficial extensions of the power grid and use CSPs' communication technology to enable the real-time communication needed to support smart energy distribution [53].

Specifically, an African telecommunications provider had cited the expansion of this energy distributor's grid network as a contributor to the telecommunications provider's ability to double their number of grid-connected sites on the network. The potential overlap between threat actors targeting telecommunications and energy providers emphasizes the dependencies between critical infrastructure sectors in both operational and cybersecurity risk.

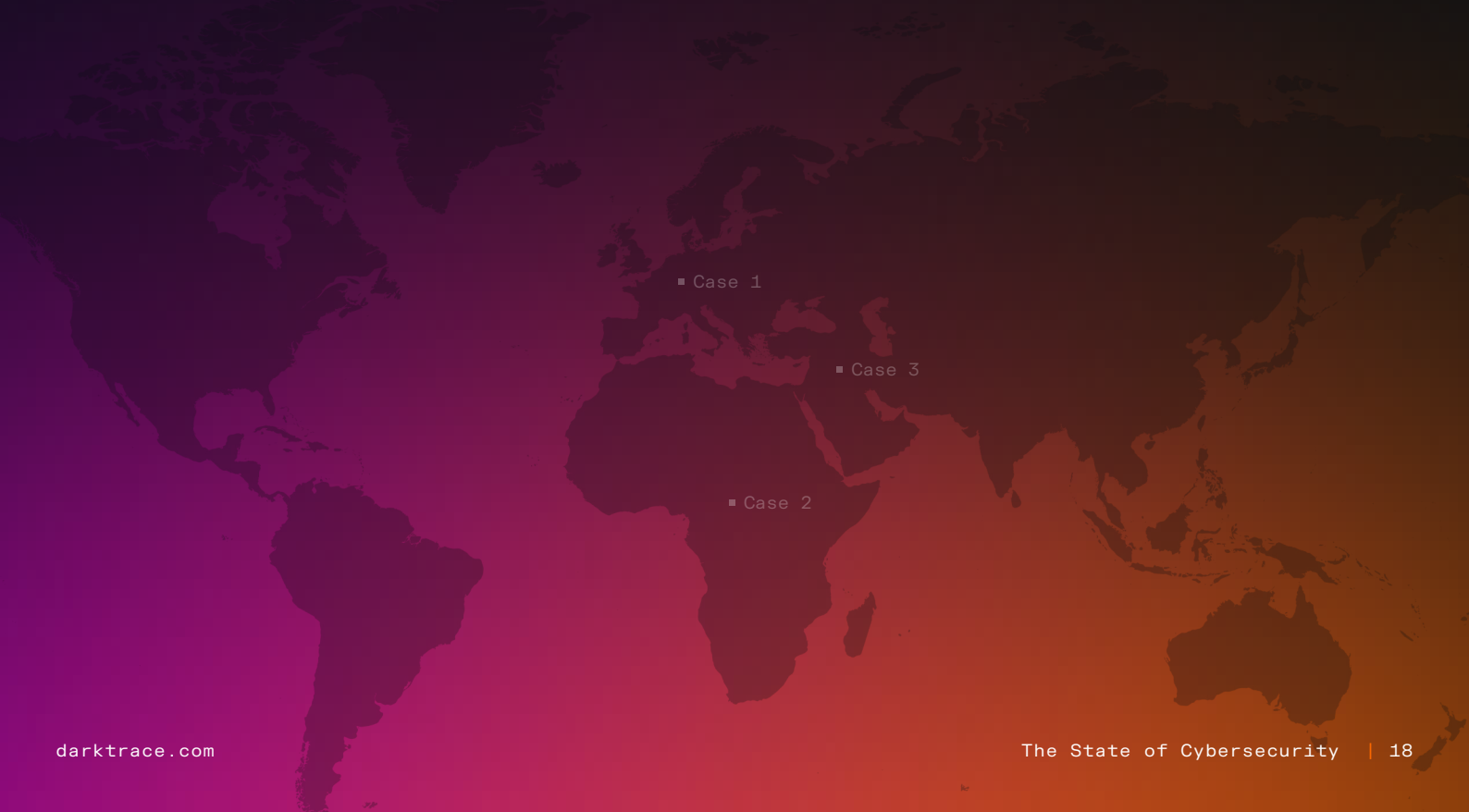
Case 3:

Probing of Middle Eastern Internet Service Provider (ISP)

Darktrace observed several devices belonging to a Middle Eastern ISP receiving inbound DNS requests from suspicious external IP ranges that have low to moderate confidence association with Liminal Panda. Other incoming connections from infrastructure associated with Russian wiper malware were observed alongside external connections to likely Liminal Panda infrastructure [54].

These devices appeared to be a mix of Open DNS resolvers and internet-facing devices, which are contextually expected within an ISP environment. Darktrace did not detect any anomalous internal activity linked to these connections that would suggest escalation beyond the devices being probed by internet scanners. However, these internet-facing devices were found to have vulnerabilities dating back to 2021, highlighting the risk of inadequate patch management.

The active probing of an organization that fits the target profile of Liminal Panda and other geopolitically motivated threat actors underscores the importance of securely configuring internet-facing infrastructure to avoid exposing low-hanging fruit to attackers.



Salt Typhoon Findings

Throughout their study, Darktrace researchers did not observe any anomalous use of the GRE protocol within telecommunications infrastructure indicative of malicious or C2 activities. However, the use of the GRE protocol was not restricted to the telecommunications sector alone. Interestingly, Darktrace observed its widespread usage across a plethora of sectors, such as Administrative and support services, Arts and Entertainment, Electricity and Utilities, Financial and Insurance, Manufacturing, and Transportation and Storage.

Apart from its utility in connections from DNS servers where GRE encapsulates DNS traffic to provider DNS servers, the protocol was also observed being used in data transfer to virtual private servers (VPS), VPN endpoints, satellite communication providers, and in communications to renewable energy plants. The prevalence of this protocol underscores the need for organizations to vigilantly monitor and secure their digital infrastructure against potential vulnerabilities.

Conclusion

The rapid evolution of telecommunications, particularly with the advent of 5G technology, has opened new avenues for cyber threats. The cybersecurity challenges that accompany this technological leap are multifaceted and need to be addressed holistically.

The perspectives of CISOs, as outlined in this report, underline the necessity for robust security frameworks and proactive measures against potential cyber threats. Their insights provide a clear understanding of the urgency and importance of implementing effective cybersecurity measures. The need for ongoing assessment, coupled with the utilization of advanced AI and machine learning tools to detect and mitigate cyber threats, is a common theme in their perspectives.

Common threat issues across telecommunications were highlighted, while noting the importance of following the CIA Triad. Nation-state activity was highlighted to illustrate the sophistication of nation-state actors and the need for innovative technologies for cyber threat detection.

The telecommunications industry, being the backbone of the digital revolution, has a crucial role in safeguarding the digital space. As we usher in the AI era, it is incumbent upon all stakeholders in this industry to collaborate and create a safe and secure digital environment.

References

[1] https://www.researchgate.net/publication/379381999_The_Diamond_Model_of_Intrusion_Analysis

[2] https://cloud.google.com/learn/security/mandiant-academy-courses/threat-hunting

[3] https://www.ncsc.gov.uk/section/advice-guidance/all-topics?topics=Critical%20National%20Infrastructure%20(CNI)&sort=date%2Bdesc

[4] https://www.gov.uk/government/news/data-centres-to-be-given-massive-boost-and-protections-from-cyber-criminals-and-it-blackouts

[5] https://resources.companieshouse.gov.uk/sic/

[6] https://www.gsmaintelligence.com/research/2025-capex-outlook-2020-update-the-1-trillion-investment

[7] https://conference.hitb.org/files/hitbsecconf2018pek/materials/D1T2%20-%20Telecoms%20-%20Generational%20Evolution%20of%20Attack%20Surfaces%20-%20Emmanuel%20Gadaix.pdf

[8] https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf

[9] https://www.ericsson.com/en/blog/2018/6/detecting-false-base-stations-in-mobile-networks

[10] http://www.cse.hut.fi/fi/opinnot/T-110.5240/2010/luennot-files/Network%20Security%2006%20-%20cellular%20security.pdf

[11] https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2018/09/Diameter-2018-eng.pdf

[12] https://www.exfo.com/contentassets/7aa79ad06e3f48fc84ccefebb56f9802/anote_exfo-diameter-testing_en.pdf

[13] https://media.defense.gov/2022/Dec/13/2003132073/-1/-1/0/POTENTIAL%20THREATS%20TO%205G%20NETWORK%20SLICING_508C_FINAL.PDF [14] https://cyberdefensereview.army.mil/Portals/6/CDR%20V5N1%20-%2008_%20Fonyi_WEB.pdf

[15] https://www.ey.com/en_gl/insights/telecommunications/top-10-risks-for-telecommunications-in-2025

[16] https://www.darkreading.com/threat-intelligence/an-emerging-threat-attacking-5g-via-network-slices

[17] https://www.nokia.com/newsroom/csps-say-they-need-stronger-5g-network-security-capabilities-as-breaches-mount---nokiaglobaldata-research/

[18] https://www.networkworld.com/article/972286/5g-network-slices-could-be-vulnerable-to-attack-researchers-say.html

[19] https://blog.talosintelligence.com/salt-typhoon-analysis/

[20] https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

[21] https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

[22] https://therecord.media/china-based-hackers-evasive-isps-malware

[23] https://www.pandasecurity.com/en/mediacenter/salt-typhoon-cyber-espionage-affects-telecom-giants-usa/

[24] https://industrialcyber.co/threat-landscape/chinas-liminal-panda-hackers-target-global-telecom-networks-in-stealthy-cyber-espionage-campaign/

[25] https://www.ericsson.com/en/blog/2023/10/deciphering-the-evolving-threat-landscape-security-in-a-5g-world

[26] https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat

[27] https://www.atlanticcouncil.org/blogs/ukrainealert/ukrainian-telecoms-hack-highlights-cyber-dangers-of-russias-invasion/

[28] https://www.congress.gov/crs-product/IF12798

[29] https://www.fortinet.com/resources/cyberglossary/cia-triad

[30] https://socradar.io/cyber-attacks-telecommunication-industry-2023-2024/

[31] https://securityaffairs.com/159528/data-breach/telco-provider-tangerine-data-breach.html

[32] https://www.infosecurity-magazine.com/news/dark-web-floods-operator

[33] https://www.cbsnews.com/news/xfinity-hack-customers-usernames-passwords/

[34] https://www.cyfirma.com/research/cyfirma-industry-report-telecommunication-and-media/

[35] https://www.cyber.nj.gov/threat-landscape/phishing-online-scams/telephone-scams/sim-swapping-attacks

[36] https://www.darktrace.com/blog/untangling-the-web-darktraces-investigation-of-scattered-spiders-evolving-tactics

[37] https://social.cyware.com/news/understanding-sim-swapping-and-cloning-attack-techniques-230934eb

[38] https://tuvis.com/cybersecurity-in-the-telecommunication-sector/

[39] https://www.darktrace.com/resources/first-6-half-year-threat-report-2024?utm_source=executive-summary&utm_medium=social&utm_campaign=half-year-threat-report-2024&success=1

[40] https://www.zscaler.com/blogs/security-research/technical-analysis-crytox-ransomware

[41] https://thehackernews.com/2024/08/ddos-attacks-surge-46-in-first-half-of.html

[42] https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-botnet/

[43] https://heimdalsecurity.com/blog/ddos-as-a-service-attacks-what-are-they-and-how-do-they-work

[44] https://blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-leads-global-action-against-favored-cybercrime-tool/

[45] https://www.channelnewsasia.com/singapore/singtel-landline-down-phone-service-outage-disruption-kkh-dbs-uob-banks-businesses-4665266

[46] https://www.darkreading.com/cyberattacks-data-breaches/cellcom-restores-regional-mobile-services-cyberattack

[47] https://www.zdnet.com/article/the-dirty-cow-linux-security-bug-moos/

[48] https://github.com/firefart/dirtycow

[49] https://attack.mitre.org/groups/G1045/

[50] https://www.trendmicro.com/en_sg/research/24/k/earth-estries.html

[51] https://www.fortiguard.com/threat-actor/5557/salt-typhoon

[52] https://www.crowdstrike.com/en-us/blog/liminal-panda-telecom-sector-threats/

[53] https://inform.tmforum.org/features-and-opinion/as-energy-and-telco-industries-transform-is-there-room-for-partnership

[54] https://socradar.io/labs/campaigns/7/details

About Darktrace

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,700+ employees who protect nearly 10,000 customers globally. To learn more, visit www.darktrace.com.

North America: +1 (415) 229 9100 | Europe: +44 (0) 1223 394 100 | Asia-Pacific: +65 6804 5010 | Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com