No.69
August 2023

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/UNSPONSORED**

This report was first released to the live event registrants and attendees as well as HardenStance report subscribers on June 12th, immediately following TTIS 2023.

Threat Intel in Telecoms (TTIS2023)

On June 6th - 7th, HardenStance hosted the 2023 Telecom Threat Intelligence Summit (TTIS2023). This executive summary of the event includes a link to the event recording.

- Changes in telco network architecture and operations introduced with 5G as well as changes in threat actor TTPs all make for a dynamic cyber threat landscape.
- Several TTIS2023 speakers encouraged telcos to embrace the global trend toward stronger government regulation of telecom security as an opportunity.
- As threats converge across nation state and criminal gangs, and across IT and OT, telcos are converging siloed SOCs and converging CISO roles across IT and OT.
- Guidance was provided for threat sharing between SOC teams; automated step by step visualizations of current attack playbooks for telcos; sharing telecom threats and mitigation expertise with other industries; detecting incidents when they don't breach quantitative thresholds; and extending threat sharing to MEC and ORAN.

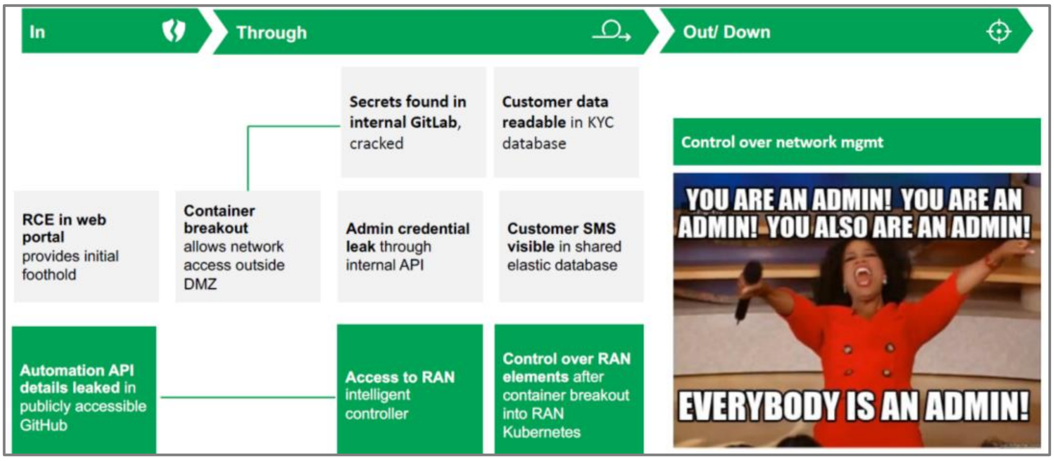
Karsten Nohl focused his talk on what he called "the new hacking frontiers that weren't there before."

5G Transforms Mobile Network Security Risk

Both feared and revered as a high profile white hacker of telco networks, Karsten Nohl's talk began by sharing what the world looks like when you flit between roles as an externally hired 'red team' attacker and an in-house telco security consultant – "the security part is often more difficult than the hacking part." As telcos migrate to cloud native 5G Stand Alone (5G SA) networks, Karsten focused his talk on what he called "the new hacking frontiers that weren't there before." He cited the following specifics:

- **The scope for hackers to break out of a Kubernetes container to compromise other containers or the underlying infrastructure:** Karsten pointed to several weaknesses, noting that the HostPid feature that allows pods to access all the processes running on a host "is done wrong by almost everyone."
- **The risk from automation.** Karsten stated that red team exercises "regularly show that telcos are hackable" from flaws such as incautious developers leaking sensitive data on the Internet and weak privilege access management that allows hackers to

Figure 1: Hacking into A Telco Network


In
Through
Out/ Down
Secrets found in internal GitLab, cracked
Customer data readable in KYC database
Control over network mgmt
RCE in web portal provides initial foothold
Container breakout allows network access outside DMZ
Admin credential leak through internal API
Customer SMS visible in shared elastic database
YOU ARE AN ADMIN! YOU ARE AN ADMIN! YOU ALSO ARE AN ADMIN!
EVERYBODY IS AN ADMIN!
Automation API details leaked in publicly accessible GitHub
Access to RAN intelligent controller
Control over RAN elements after container breakout into RAN Kubernetes

Source: Autobahn Security

take control of telco nodes and other critical systems". He described automation as "what will ultimately allow us to win the hacking race but as an intermediate step, automation actually makes it harder to defend networks."

Karsten argued that "it's futile to answer the question 'should we go into the cloud or not?' or 'should we move to OpenRAN or not?' The economics are pushing in that direction. It's cheaper and more flexible. As security people we just have to live with it – face the consequences, deal with the reality. Am I happy from a security perspective that everything becomes super-complex and highly automated overnight? No but I also can't stop it." His guidance to TTIS attendees was "hack yourself faster than someone else will. Learn from it: iterate, iterate, iterate. Because with 5G the network is changing every month whereas 3G and 4G infrastructure was mostly configured by humans, never to be touched again. The 5G network has a life of its own - giving you a continuous challenge to understand what your current security posture is."

Aspects of the threat landscape telcos face are changing constantly

Some aspects of the cyber threat landscape telcos face is constant while others are constantly changing. Several people spoke to changing threats in the telecom network or Operational Technology (OT) domain. For example, the latest threat intel findings shared by NETSCOUT and Nokia are captured on the next page.

Rick from VMware said that bringing security monitoring in telco networks up to the same level as enterprise IT "may wind up exposing a number of issues that that we don't yet know much about."

One theme that got a lot of attention this year was the vulnerability of a telco's enterprise IT domain to cyber attacks. For context, T-Mobile in the U.S. has suffered some six or seven substantial data breaches in recent years - every one of them arose from a flaw in T-Mobile's enterprise IT security rather than its public fixed or mobile telecom network assets. Discussion at TTIS2023 centred around the vulnerability of a telco's enterprise IT in its own right. Just as – or more – importantly, it also focused on the growing threat posed by cyber attacks that can impact both a telco's IT and OT domains.

Professor Ciaran Martin from Oxford University, former head of the UK's National Cyber Security Centre (NCSC), got the ball rolling on this by noting the importance of understanding the critical dependencies between the two domains rather than merely ensuring that they are properly air-gapped. "I think strategically, for critical infrastructure security", Ciaran said, "Colonial Pipeline is the cyber breach of this century that we should study the most. In my former role as Head of the UK's National Cyber Security Centre (NCSC), most of the assurances I would have received about de-linking of OT from enterprise technology were essentially worthless."

"The Colonial breach wasn't about jumping air gaps", he went on. "It was about enterprise systems being so messed up by a routine, medium-sophistication, cyber attack that the company wasn't able to operate the pipeline itself. They [attackers] didn't jump onto the OT controls. Colonial just couldn't run the business which meant they had to switch off the pipeline. That to me is a development of the most profound importance."

It's easier and cheaper to hack into IT than OT

All four participants in the Day 1 panel on enterprise IT security recognized the greater vulnerability of a telco's enterprise IT compared with its' OT. They pointed to various types of convergence across the two domains as providing an important framework for hardening a telco organization's overall security posture. In the majority of cases where attackers are motivated by financial gain, Michael Daniel from Cyber Threat Alliance and Rick McElroy from VMware both noted how much easier and cheaper it is to hack into enterprise IT than telecom OT - because of how widely deployed and familiar the technologies are. Rick said this tends to be "the path of least resistance." That said, he also noted that because we tend to have more granular visibility into enterprise IT, bringing security monitoring in telco networks up to the same level "may wind up exposing a number of issues that we don't yet know much about." Derek from Fortinet agreed that "we don't have as much visibility as we need on the OT side of the house."

The Latest Threat Landscape Insights from NETSCOUT & Nokia

Nelson Silva shared highlights from Nokia's new 2023 Threat Intelligence report. This leverages the company's global footprint of Nokia NetGuard endpoint security and Nokia Deepfield IP network intelligence, analytics and DDoS protection deployments. Among the key datapoints:

- 35% of all detected malware attacks are adware, crypto mining or banking trojans. The share of banking trojans has almost doubled from 5% in the 2021 threat report to 9% in 2023.
- Android-based systems account for 49% of mobile malware infections as well as 30% of malware activity in fixed residential networks.
- There are now between half a million and a million globally distributed, remote controlled IoT hosts or cloud server instances active every day – up from 200,000 un 2022. 90% of complex multi-vector DDoS attacks are leveraging botnets now.

Roland Dobbins shared highlights from NETSCOUT's 2H 2022 threat report derived from the company's global footprint of the NETSCOUT Arbor DDoS protection portfolio:

- 40% of DDoS attacks seen were multi-vector attacks. 29% comprised 2-5 vectors. 8% comprised 6-10 vectors. 3% comprised 11 or more vectors.
- NETSCOUT saw an aggregate of 389.57 Tbps of DDoS traffic on just one day – November 30th – last year. That arose from 44,497 DDoS attacks the company saw that one day.
- Citing an 18% increase in Direct Path DDoS attacks (sourced directly from the attack infrastructure) and an 18% decrease in Reflection/Amplification attacks, Roland pointed to this "great re-balancing" as "the biggest change in the DDoS threat landscape in the last decade." Telco DDoS protection teams have been largely responsible for this rebalancing due to accelerated deployment of anti-spoofing or source address validation (SAV) solutions at customer edge sites over the last couple of years. Two Direct Path attacks - ACK and SYN flooding which abuse TCP acknowledgement and synchronization messages – were the two most common DDoS attack vectors in 2H 2022.
- From what he has seen in the first five months of 2023, Roland shared that the company's next threat report will feature a deep dive into what NETSCOUT calls 'carpet bombing' attacks. These target a range of addresses or subnets which can contain hundreds or even thousands of destination IP addresses and can have create substantial collateral impacts on organizations besides the target.

The panellists pointed to how attackers are bridging the two domains – hence how defenders should too. Michael pointed to "Pipedream", a new malware identified by Industrial Control Systems (ICS) security specialist, Dragos, in a recent cyber threat report. 'Pipedream' is the first malware that can be applied across multiple different OT environments, thereby lowering the cost of launching cyber attacks on these targets.

Aligning with Ciaran Martin's "development of profound importance" assessment of the Colonial Pipeline hack, Fortinet's Derek Manky cited momentum behind various types of convergence – IT and OT; nation state APT groups and cyber criminal gangs; network and security. Derek noted momentum behind threat actors directly targeting OT environments like a telco's public networks. This, he said, is "the new cross hairs" for organizations like telcos that have substantial investments in OT. "This isn't broad blanketing, 'spray and pray', he added, it's different with these targeted attacks."

Derek said there is clear merit in defining specialized threat intel sharing frameworks such as MITRE's ATT&CK Enterprise, ATT&CK ICS and 5G Hierarchy of Threats or 'FiGHT' frameworks. At the same time, he and Michael from CTA emphasized the importance of recognizing how much these frameworks have in common as well as what differentiates them. "The differences lie in the techniques", Derek said. "But the tactics – the reconnaissance, the evasion, the code execution – these are largely the same.” Michael added that “the beauty of a common framework is that it puts different aspects into a common language. Building common lexicons for different terrains helps defenders communicate better and transfer learnings much more quickly. You do have to recognize that some aspects are different in a mobile network, for example. But at a conceptual level that’s not all that difficult to manage.”

Hyperoptic’s Paul MacKenzie gave a different perspective on the threats a Tier 2 wireline ISP like his company tends to prioritize. “There are big cyber attacks that make headlines and a lot of discussion about nation state threats”, he said, “but basic phishing and business email compromise (BEC) are what I spend most of my time on.” Referring to the stringent new regulations being imposed across the sector by the UK’s new Telecommunications (Security) Act, Paul stated that “we have to keep doing these basics well as we respond to the more interesting aspects the new regulations require of us.”

There is significant momentum behind covering siloed Security Operations Centres (SOCs) across the telco organization.

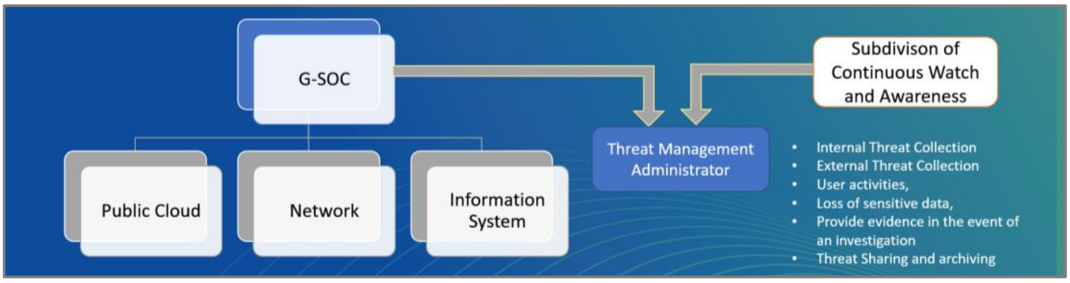
Telcos Are Converging Security Operations at An Organizational Level

Faced with nation state threat actors and criminal cyber gangs converging and IT and OT – as well as IT and OT threats – also converging, TTIS yielded encouraging evidence that telcos are responding by converging their own security operations across IT and OT domains. For example, the David Rogers, Chair of the GSMA’s Fraud and Security Group (FASG), confirmed what is a clear industry trend, especially among leading telcos, namely that “Chief Information Security Officers (CISOs) are now becoming responsible for cybersecurity covering all of the IT and telco network security.” Sami Said added that he holds both CISO and Chief Security Officer (CSO) roles in Tunisie Telecom.

Consistent with job roles converging, there is also significant momentum behind converging siloed Security Operations Centres (SOCS) across the telco organization. Sami Said explained that Tunisie Telecom is in the process of converging its three SOCs – telecom network, enterprise IT and cloud – under a single General SOC or ‘G-SOC’ by the end of this year. As part of that convergence, 80% of the company’s tools have already been federated at the direction of the ‘G-SOC’ Director. A dedicated Threat Management Administrator function is also being established to collect, curate and share threat intelligence across all three teams that have historically done this themselves within their own dedicated silo (see **Figure 2**). In her talk, Maria Martinez from Telefonica Tech affirmed that this convergence of SOCs has already been completed within the Telefonica Group.

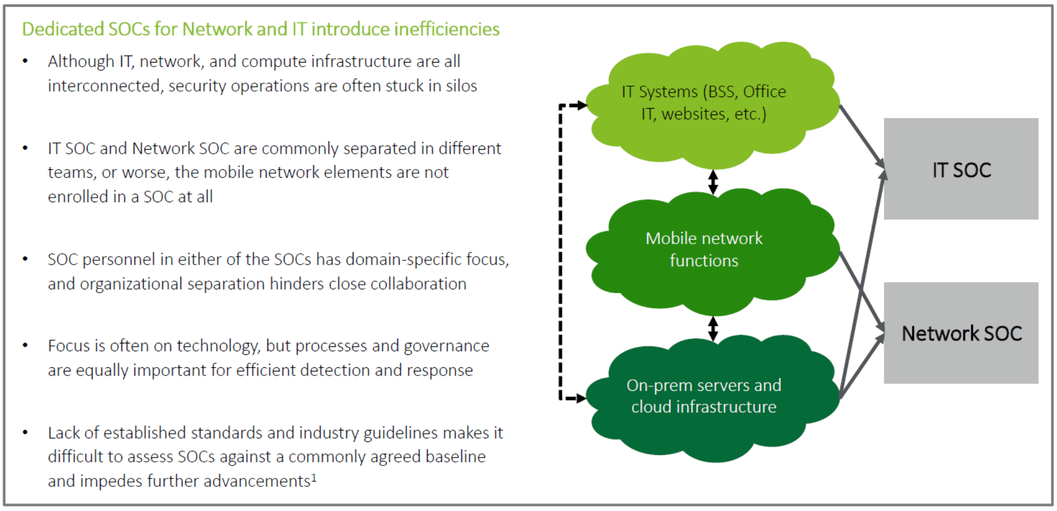
Anand Prasad, former Chair of 3GPP security group SA3, now a partner with Deloitte Tohmatsu Cyber, made the key point that SOC convergence is enabled by common technology across the different domains (Linux based systems); similar protocols (HTTPS and OAuth2); and similar threats (e.g. API exploits, DDoS). Naturally, he acknowledged telecom-specific threats in the telecom network or OT domain. However he also labelled these as being “largely limited to domain-specific protocols (e.g. on the interconnect) and the air interface (e.g. false base stations).

Figure 2: A Single Threat Management Function Within the G-SOC


G-SOC
Subdivison of Continuous Watch and Awareness
Threat Management Administrator
Public Cloud
Network
Information System
Internal Threat Collection
External Threat Collection
User activities,
Loss of sensitive data,
Provide evidence in the event of an investigation
Threat Sharing and archiving

Source: Tunisie Telecom

Figure 3: SOCs are Often Managed Separately and Lack Established Standards



Dedicated SOCs for Network and IT introduce inefficiencies

- Although IT, network, and compute infrastructure are all interconnected, security operations are often stuck in silos
- IT SOC and Network SOC are commonly separated in different teams, or worse, the mobile network elements are not enrolled in a SOC at all
- SOC personnel in either of the SOCs has domain-specific focus, and organizational separation hinders close collaboration
- Focus is often on technology, but processes and governance are equally important for efficient detection and response
- Lack of established standards and industry guidelines makes it difficult to assess SOCs against a commonly agreed baseline and impedes further advancements[1]

IT Systems (BSS, Office IT, websites, etc.)

Mobile network functions

On-prem servers and cloud infrastructure

IT SOC

Network SOC

Source: Deloitte Tohmatsu Cyber

In his talk, Anand noted that before converging, personnel in siloed SOCs tend to have a domain-specific focus and organizational separation which hinders collaboration. The focus is often too technology-centric when in fact, he said: "processes and governance are equally important for effective detection and response." He stated simply that "having separate SOCs within the telco organization can lead to lack of visibility and impede incident response."

Having separate SOCs within the telco organization can lead to lack of visibility and impede incident response.

As well as arguing for SOC integration, Anand pointed to the case that can also be made for integration of SOCs and Network Operations Centres (NOCs). He nevertheless added an important rider that this requires a high level of organizational maturity. In particular it requires that the CISO or CSO shares the same status within the telco organization as the CTO. Towards the end of the enterprise security panel, CTA's Michael Daniel added that "while I'm leery of absolutes, the economics and drivers will indicate for a lot of organisations that convergence of their different SOCs makes most sense. The easiest way to get to the agility you need across them is to merge them."

Stricter government regulation isn't patchy – it's a clear global trend

There is a clear global trend of greater government regulation of cybersecurity of critical infrastructure generally, and of the telecom sector in particular. For context, some background is provided below, together with some comments made during TTIS:

- **UK**: The Telecommunications Security Act of which Hyperoptic's Paul MacKenzie said: "there are few areas of our operations that are untouched by this legislation."
- **EU:** The far-reaching Network and Information Services (NIS2) Directive is required to be implemented by member states by October 2024.
- **United States**: The January 2023 Federal Communications Commission (FCC) Notice of Proposed Rule Making (NPRM) seeks to impose stricter terms upon which America's telcos report cybersecurity incidents.
- **Tunisia:** At TTIS2023, Tunisie Telecom's Sami Said pointed to Tunisia's March 2023 Decree-Law No, 2023-17. This triggers far-reaching cybersecurity requirements on critical infrastructure providers.
- There are major regulatory overhauls underway in other markets as diverse as Australia, India, Canada and Singapore to mandate better standards of cyber security for the telecom sector.

Government regulation represents an opportunity

Several speakers encouraged attendees to embrace greater government intervention in telco security as an opportunity. No-one made the contrary case objecting to tighter regulation, although that isn't necessarily reflective of overall industry sentiment.

In his talk, Cyber Threat Alliance's Michael Daniel framed his thoughts around a theme of: "Incident Reporting – What's In It For Me?" Michael began by pointing out that information security professionals lack enough data to be able to accurately scope the problem posed by the cyber threats they face. "We still see so many conflicting reports on things like ransomware – the size of the problem, whether it's going up or down, who's being targeted," he said. Michael argued that mandatory incident reporting can fill gaps in our understanding of the threat landscape. It can enable government to make guidance and support more granular and more tailored, as well as drive better response actions and better policy-making.

Several speakers at TTIS encouraged telcos to embrace greater government intervention as an opportunity.

Michael sought to assuage concerns that organizations might suffer negative consequences from more stringent incident reporting requirements. He noted that reporting regimes often explicitly prohibit any regulatory action being taken based solely on an incident report. In terms of the risk to an organization's brand and reputation from having to report an incident, he said that most regimes typically require that agencies protect information from disclosure.

He also said that where organizations have adequate incident response planning and incident response procedures, the impact of a breach on brand and reputation usually ends up being "pretty transitory, it does not usually seem to have long term consequences." Michael didn't mention this himself, but T-Mobile in the U.S has enjoyed strong subscriber growth despite enduring all the high profile data breaches cited earlier. Michael also said mandatory incident reporting will typically not affect any determinations with respect to an impacted organization's legal liability. That's because "most of the reporting regimes set that question aside because these reports go to entities whose job it is to respond and not necessarily be the regulator or enforcer."

Also supportive of greater government engagement, Rowland Corr from Enea AdaptiveMobile Security pointed to the good work of the European Parliament's PEGA Committee into the use of spyware, with recommendations arising for the role of both regulators and telcos themselves. Ciaran Martin's closing remarks in his talk consisted of a passionate appeal to embrace cybersecurity regulation in telecoms. "In the UK we have a bunch of people who understand how telecoms works, they know what kind of regulation would make the industry unwieldy and unviable", he began. "Like all regulation, it's about balancing operability and profitability with security but we know how to do that. So my plea is for everybody to approach this in good faith, in a spirit of openness and technical expertise, and let's make these new regulations work."

The UK can be a model for the world in telecom cyber resilience

Ciaran held out a big prize that he said is within our grasp: "this could be a real model for the rest of the world about how to make telecoms infrastructure safer. If we can do that, and I really think we can, then we will have taken a huge step forward. Even though many of the details will be utterly tedious, we will have hardened the infrastructure of the UK. And we will have shown an example to the world that in this tumultuous decade of pandemic, war and great power competition, we will have strengthened our resilience against whatever this mad, crazy world has to throw at us."

On behalf of Tier 2 ISPs, Paul MacKenzie argued that Tier 1 operators alone must not be allowed to lead the detailed direction that telecom security takes. "A particular anxiety I have", Paul said, "is that Tier 1s tend to be more mature and have deeper pockets. As the tide of security regulation rises, Tier 2s risk being taken in a direction that they can't respond to if we're not at the table influencing that conversation."

New threat intel capabilities tempered by ongoing weaknesses

As in previous years, the detailed mechanics of building better capabilities for collecting, curating, using and sharing threat intelligence within the broader telecom market framework made up by far the most contributions at TTIS. This year's talks yielded a mix of 'need to do a lot better' shortcomings and encouraging evidence of progress.

On the negative side of the ledger, Enea AdaptiveMobile Security's Rowland Corr gave a sobering assessment of where the mobile communications industry is still at in terms of generating and sharing threat intelligence for signaling protocols like SS7 and Diameter. "While calls for threat intelligence sharing are imperative, they're also premature," Rowland said, because of what he called "a systemic deficit" in the installed base of telco and government capabilities to detect mobile signaling threats. The legacy of signaling security being excluded from cybersecurity as an IT-oriented discipline lies at the heart of the problem, he said: signaling threats are typically excluded from national threat assessments, giving operators little incentive to invest in signaling threat detection.

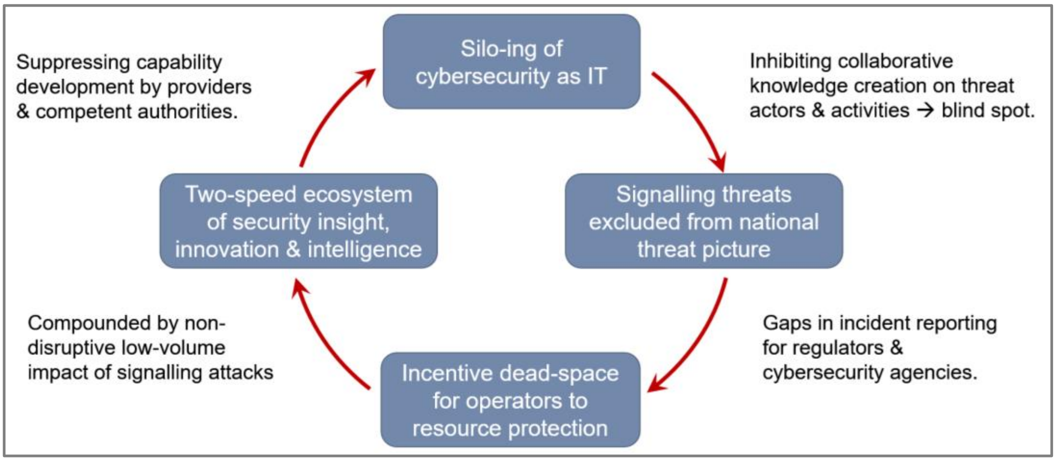
Signaling threats are typically excluded from national threat assessments, giving operators little incentive to invest in signaling threat detection.

David Rogers from the GSMA recognized Rowland's description of IT and telecom security silos. More positively, he cited the UK and the U.S. as countries that have done a good job of breaking these silos down in the way their new national cyber security strategies now define cyberspace a lot more broadly to include telecoms. "It's not just the internet, it includes telecom, it's virtual, logical, physical. All types of different devices have to connect to this broad set of networks that we call cyberspace", David said. "They're all at risk from all the different threats we have to deal with."

Breaking down threat intelligence silos within a telco organization – both within and between domains – was identified by Fortinet's Derek Manky as a human and culture challenge - "you need top down support first." Ciaran Martin overlapped in part with Rowland in seeing under-achievement in industry's use of threat intelligence. "One of the slightly disappointing aspects is perhaps underachieving relative to what we can do in terms of scaling the use of threat intelligence to block threat actors", he said. "In which case let's look really closely at what Ukraine has managed to achieve with our help and let's take that mainstream."

The fact that signaling attacks, in particular, tend to be low volume, and therefore largely non disruptive to the operator's own infrastructure, has further reduced the incentive to invest here, Rowland went on. As shown in **Figure 4**, the absence of detection capability then means that the kind of hard evidence of threats needed to build a business case for investment is lacking, perpetuating the vicious circle of under-investment.

Figure 4: The Vicious Circle of a Two-Speed Telecoms Security Ecosystem


Silo-ing of cybersecurity as IT
Inhibiting collaborative knowledge creation on threat actors & activities → blind spot.
Signalling threats excluded from national threat picture
Gaps in incident reporting for regulators & cybersecurity agencies.
Incentive dead-space for operators to resource protection
Compounded by non-disruptive low-volume impact of signalling attacks
Two-speed ecosystem of security insight, innovation & intelligence
Suppressing capability development by providers & competent authorities.

Source: Enea AdaptiveMobile Security

Rowland pointed out that a key step in breaking out of the vicious circle is understanding the increased propensity of threat actors to blend signaling threats with other threats. He specifically cited interconnect attacks, spyware and human threats (for example arising from malicious activity or benign errors by telco employees). As he pointed out, malicious hackers don't artificially limit themselves to specific technology silos when assembling attack vectors – they choose freely from whatever is available. Hence telcos and other organizations should likewise break down their own silos.

Threat detection shouldn't just focus on quantitative thresholds

Citing the European Union Agency for Cyber Security (ENISA)'s 2022 Threat Landscape report, Rowland argued that signaling protection is key to capturing incidents that do not exceed quantitative thresholds for the number of users impacted but are nevertheless significant. He cited public examples of threat actors claiming to interfere in national elections via hacks that intercept SMS security codes from the Telegram accounts of leading campaign officials or strategists from target political parties, such as recently in Kenya. Rowland confirmed these aren't just claims, stating "Enea AdaptiveMobile Security's threat intelligence unit continues to detect threats entirely consistent with the kind of targeting activity described in that reporting." He concluded by identifying qualitative reporting requirements as "the critical catalyst for incident reporting" and the development of threat intelligence capabilities.

Rowland cited examples of threat actors claiming to interfere in national elections via hacks that intercept SMS security codes from the Telegram accounts of leading campaign officials or strategists.

Driving threat sharing beyond telecoms to other sectors of industry

As he has at TTIS in previous years, FASG Chair, David Rogers, provided an update on what the GSMA is doing to drive better, more automated, cyber threat sharing – both within the telecom industry and into other sectors of industry that are increasing reliant on telecom networks.

David cast the latter as especially challenging. "We now have to deal not just with consumer handsets but with every industry, all their different devices with embedded or physical SIMs and all the different things they're attached to as well. There are lot of different frauds evolving, each involving specialist hacking hardware and software." he said. "As well as getting our own act together, we have to help these other industries too. They may not understand telecom technology but they do have to use things like SMS 2 Factor Authentication (2FA)." David also pointed to help needed in areas like how signaling works. "With private mobile networks, for example, people will need help interconnecting out into the wider world", he said.

Within the telecom environment, David pointed to different radio interface attacks, mobile malware (some targeting consumers, others nation state Advanced Persistent Threats or APTs). In the realm of regular IT threats that telcos also have to deal with, he said that the biggest right now is ransomware and the way it is evolving to data extortion threats.

Introducing FIRST's new Network Security Special Interest Group

The group's Co-Chair, John Kristoff, introduced the new NETwork SECurity Interest Group (NetSEC SIG) within the Forum of Incident Response Teams (FIRST) to the TTIS2023 audience. Founded in 2022, this group seeks to bridge together groups focused on Inter-AS (Autonomous Systems) security – those with responsibility for DNS, routing, and other issues that have an impact on network security issues.

John cited some of the key areas of focus as route hijacks and leaks; DDoS; traceback and attack source attribution; DNS and DNSSEC operational issues; RPKI, ROV and other burgeoning routing technologies; BCPs and tools such as MANRS and PeeringDB.com; and operator and research collaboration.

Within its Telecommunications ISAC (T-ISAC), GSMA is sharing Indicators of Compromise (IoCs) and has a community of interest with other ISACs. It produces its annual threat report now. These days, more than 50% of the agenda at the FASG group meetings is dedicated to threat intelligence and threat intelligence sharing issues. GSMA is also supporting regional threat intel meetings that are focused on specific local fraud campaigns. The work of the GSMA's MObile Threat Intelligence Framework (MOTIF) is drawing to a close now, with decisions to made on which technical schemas to use for information sharing. David said he supported being able to support "multiple types of schema as soon as possible" and that he was really looking forward to seeing this rolled out as it will see "rapid adoption" and drive "positive change."

These days, more than 50% of the agenda at the FASG group meetings is dedicated to threat intelligence and threat intelligence sharing issues.

On behalf of Tier 2 wireline ISPs that don't enjoy the scale of some of the GSMA's big mobile operator members (although that arguably applies to some of GSMA's smaller operator members too) Hyperoptic's Paul MacKenzie said that the challenge of being heard in such kinds of industry fora as a small player is as much one of organizational scale as anything else. "It's not that the door is closed", Paul said. "It's more to do with all the steps that are required. Participating is immensely valuable but it's almost an extra-curricular activity. Investing that time is difficult when you've got limited resources but there are ways of benefitting from sharing security learnings as a group of altnets without compromising competitive information and we will do it."

David concluded by citing other barriers the GSMA and industry partners are still working on breaking down: limited understanding of threat intel related issues; challenges sharing using APIs; monetization of threat intel getting in the way of information sharing; and what he called "parochial issues" such as people being unwilling to share beyond a particular scope of partners or beyond a specific region.

New visual threat intelligence modelling for telecoms

A number of speakers articulated either best current practice or articulated the value of new tools coming to market that are tailored to the telecom sector. Maria Martinez from Telefonica Tech discussed some of the details of how tactical, operational and strategic threat intelligence are collected, applied and shared within the Telefonica Group.

Derek from Fortinet shared details of new visual threat intelligence modelling tools that Fortinet is building for industry verticals like telecoms. In collaboration with MITRE Engenuity and the Centre for Threat Informed Defence, Fortinet has now published a number of these projects on GitHub. The graphic visualizations automatically generate what the very latest cyber attack playbooks look like mapped against the MITRE ATT&CK framework. The approach borrows from the way forensics is done in incident response.

The value lies in defenders being able to watch an emulated sequence of moves in the latest attack playbooks unfolding like a chess game. It highlights which specific subset of TTPs the adversary is using – what for and when – in that specific campaign. Machine learning can also be applied for predictive analysis to arrive at a better understanding of an attacker's full range of behaviours. Derek described these tools as making the MITRE ATT&CK framework more easily accessible. Defenders can use it to view the threat landscape "from a 20,000 foot view rather than just a 40,000 foot view" and more effectively integrate MITRE's threat intelligence into their security stack. "Once you understand the flow", he said "you can then ask 'do you have the relevant security tools early on in that flow to block it?'" Importantly for mobile operators, Derek said these visualization tools can also be used in conjunction with MITRE's 5G FiGHT framework.

New releases of MITRE's FiGHT framework

Driving off the core principle that "cybersecurity should be threat-informed", Eric Arnoth and Muddasar Ahmed from MITRE gave an update on FiGHT. They explained that FiGHT leverages concepts from existing security frameworks and builds upon them, incorporating predictive and lab-proven threats to critical 5G assets in an effort to "anticipate the adversary rather than waiting for them to do something and then react."

As with the MITRE ATT&CK Framework, FiGHT will enable defenders to see the threat, emulate adversaries, develop analytics and assess their defences. The Phase 1 release of FiGHT was released in September 2022 addressing what TTPs might look like, 5G critical assets, and the type of detections and mitigations that are going to be most effective. As 5G core networks are rolled out, Phase 2 will start reflecting real world experience of specific threat adversaries and their behaviours. Version 1.1 and 2.0 are planned for later this calendar year. FiGHT will also be extended to other mobile network domains such as MEC and OpenRAN. Muddasar concluded with good advice for telcos: "don't drive without headlights, you're not going to have good consequences." ■

View the TTIS2023 Event Recording

TTIS2023 was sponsored by Enea AdaptiveMobile Security, Nokia, NETSCOUT, and Fortinet as well as co-sponsored by The Cyber Threat Alliance. You can register to view the full recordings of the two day event here:

https://www.hardenstance.com/online-events/

Each speaker and the start-time of their talk in the video recording is listed here:

Day 1

- 0.00.00 Patrick Donegan, (Founder & Principal Analyst, HardenStance)
- 0.06.53 Ciaran Martin (Professor of Management, Oxford University)
- 0.29.48 Paul MacKenzie (Head of Security, Hyperoptic)
- 0.54.52 Rowland Corr (VP, Government Relations Enea AdaptiveMobile Security)
- 1.20.44 David Rogers (Chairman, GSMA's Fraud and Security Group – FASG)
- 1.41.19 Nelson Silva (Head of NetGuard Security Portfolio, Nokia)
- 2.05.38 Sami Said (CISO, Tunisie Telecom)
- 2.32.42 Michael Daniel (President and CEO, Cyber Threat Alliance – CTA)
- 2.51.42 Derek Manky (VP Global Threat Intelligence, Fortinet)
- 3.23.26 Panel "Defending a Telco's Enterprise IT" (Michael Daniel, Derek Manky and Rick McElroy, Principal Cybersecurity Strategist, VMware).

Day 2

- 0.00.00 Patrick Donegan (Founder & Principal Analyst, HardenStance)
- 0.05.47 Maria Martinez, (Head of Threat Intel Operations, Telefonica Tech)
- 0.34.39 Roland Dobbins (Principal Engineer, NETSCOUT)
- 1.02.45 Anand Prasad (Partner, Deloitte Tohmatsu Cyber)
- 1.20.48 Karsten Nohl (Managing Director, Autobahn Security)
- 1.48.12 Muddasar Ahmed and Eric Arnoth (MITRE)
- 2.14.17 John Kristof (Co-Chair, FIRST NetSec SIG)
- 2.32.19 Patrick Donegan (Founder & Principal Analyst, HardenStance)

More Information

- NETSCOUT Threat Intelligence Report (2H 2022)
- Fortinet Labs Global Threat Landscape Report (February 2023)
- Nokia's Threat Intelligence Report 2023
- About Cyber Threat Alliance

- GSMA's T-ISAC home page
- GSMA Mobile Telecommunications Security Landscape 2023
- FIRST's NETSEC SIG
- MITRE FiGHT
- Enea AdaptiveMobile: "Spectrum of Violence: Mobile Network-enabled Attacks in Hybrid Warfare"

HardenStance Reports

- "RSA Survey on 'Barriers to Effective Use of Threat Intelligence" (March 2023)
- "Intelligence-Driven DDoS Defence" (February 2023)
- "Streamlining Telco SOC Operations" (November 2022)
- "Preparing for New Incident Reporting Requirements" (November 2022)
- "Tidal Cyber's Community Edition is GA" (August 2022)
- "Defending Telecoms against Nation State Cyber Threats" (June 2022)
- "Using Threat Intel in Telecoms (TTIS2022)"
- "Using Threat Intelligence in Telecoms (TTIS2021)"

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a leader in custom cyber security research and leading publisher of cyber security reports. HardenStance is also a strong advocate of industry collaboration in cyber security and is the organizer and host of the Telecom Threat Intelligence Summit. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The GSM Association, MEF, OASIS, ETSI. The Cyber Threat Alliance. HardenStance is also a recognized Cyber Threat Alliance 'Champion'.

Register to receive public domain HardenStance reports when they're released

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.