White Paper

HardenStance

Defending Telecoms Against Nation State Cyber Threats

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

ENEA AdaptiveMobile Security

paloalto NETWORKS

June 2022

Executive Summary

- With rising geopolitical tensions, nation states are increasingly willing to take higher risk in offensive cyber operations to undermine an adversary's national security.
- Nation state proxies and organized cybercrime gangs can pose as much of a national security risk as direct threats from nation states. Worryingly, boundaries between these different threat groups are breaking down, risking greater escalation.
- Nation states have many more Advanced Persistent Threat (APTs) at their disposal besides trying to hide backdoors in a telecom vendor's software or in a chip. They rely on mundane threat vectors like SMS and email as well as APTs.
- Governments will get increasingly prescriptive about defending telecom networks against nation state cyber threats. Weaknesses in a telco's enterprise IT security present as much of a risk as weaknesses in the security of its telecom network.

An Escalation in Nation State Cyber Threats

Consistent with a rise in global geopolitical tensions, 2021 offered up plenty of evidence that some of the most important nation state threat actors in cyber space are taking more risk with their offensive cyber operations. The first few months of 2022 have offered up a lot more of the same.

Russia Achieved Unprecedented Success with the SolarWinds Hack

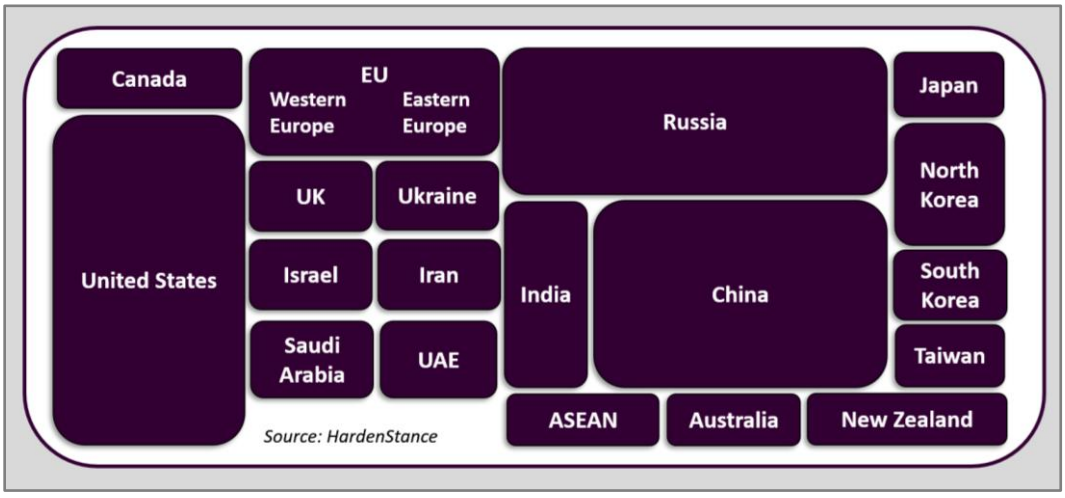
Russian state threat actors support the country's foreign policy goals which are to undermine NATO and its members and bring the countries of Eastern Europe and the former USSR back into its geopolitical orbit. Hence Russia's offensive cyber operations centre on large scale espionage to steal data from the commercial, government and military institutions of the U.S and its allies; disinformation campaigns to shape decision-making in those countries; and disruption of critical infrastructure in Eastern Europe.

Some of the most important nation state threat actors in cyber space are increasingly willing to take more risk and undertake more aggressive offensive cyber operations.

Aligned with its war aims, Russia has intensified cyberattacks on Ukraine, although with some exceptions Ukraine's defenders have mitigated most of them very effectively. Contrary to some expectations – perhaps because it doesn't want to risk a direct conflict with NATO – Russia is considered by some experts to be holding back from unleashing its most advanced cyber weapons against adversaries. This could easily change, though.

In any case, the SolarWinds hack – identified in December 2020 and attributed to Nobelium, a Russian state threat actor – has already broken new ground. With up to 18,000 organizations potentially compromised, the scale of Russia's one-time haul of sensitive data from many of the key organizations of its adversaries was unprecedented.

Figure 1: The Most Important Nation State Actors in the Cyber Domain



China Has Increased Its Targets and Adopted Higher Risk Techniques

FBI Director, Christopher Wray, told American TV's "60 Minutes" in April 2022 that "the biggest threat the U.S faces from a counterintelligence perspective is from the People's Republic of China, especially the Chinese Communist Party. They are targeting our innovation, our trade secrets, and our IP on a scale unprecedented in history."

The Hafnium attack on Microsoft Exchange, carried out by Chinese state threat actors, was notable for two things. The first was the SolarWinds-like scale of the access it served up to victim organizations – up to 60,000 world-wide. Second, and just as serious, were the techniques used. In the case of SolarWinds, Russia complied with established norms of cyber espionage in that the threat actor accessed the data and left it at that. With Hafnium, China deviated from these norms by also booby-trapping some of the victim's infrastructure. Leaving an adversary's infrastructure vulnerable to being subsequently damaged or depleted in this way significantly increases the risk of escalation in offensive cyber operations between nation state adversaries.

With the Hafnium attack on Microsoft Exchange, China deviated from cyber espionage norms by booby-trapping some of the victim's infrastructure.

China is now willing to direct offensive cyber operations across a wide variety of geographies including near neighbours to its Belt and Road supply chain initiative. As shown in **Figure 4**, China frequently directly targets the telecom sector. On June 7th, CISA, the FBI and the NSA in the U.S issued a Joint Cyber Advisory Alert warning of how Chinese state-sponsored cyber actors "exploit network providers and devices". The Advisory details how these threat actors are targeting vulnerabilities in networking products from a number of the world's leading network vendors.

Iran Shows "A Growing Willingness to Take Risks"

In its February 2022 Annual Threat Assessment, referring to offensive cyber operations, the U.S Office of the Director of National Intelligence (ODNI) cited Iran's "growing willingness to take risks when it believes retaliation is justified". Iran is focused on disrupting critical infrastructure and political espionage aimed at Israel and other adversaries in the Middle East and North Africa. The Lebanese Cedar example cited in **Figure 4** is a recent example of Iran's consistent focus on trying to breach telco organizations for espionage purposes.

North Korea's Income from Cybercrime to More than Double in 2022

North Korea's primary objective with offensive cyber operations is to generate foreign currency to drive its nuclear programme, hence a strong focus on ransomware. Operations date back to the WannaCry outbreak of 2018 and more recently to the heist of around $600 million in Ethereum cryptocurrency from video games company, Sky Mavis. Chainalysis estimated that North Korea stole $800 million in crypto currency in the year to May - twice the amount estimated for the whole of 2021.

Nation State Threats Against Telecom Networks

This White Paper looks at new developments in the ways hostile nation states are using cyber threats against targets in countries deemed to be adversaries. It focuses in particular on the ways nation state threat actors are exploiting foreign telecom networks in adversary countries to achieve their goals. This involves aiming attacks directly at the telecom infrastructure itself and on high value telco customer data at rest and in transit.

Among the examples shared in this paper are Russia's targeting of telecom networks as part of the hybrid war it is waging against Ukraine. On May 19th, Reuters cited Ukrainian cyber official, Victor Zhora, stating that "attackers continue to focus on the telecommunications and the energy sector." The example of the Viasat hack is cited in **Figure 4**. As part of their offensive cyber operations against telecom networks – in peace time as well as in war time - nation state adversaries are also exploiting foreign telcos as a conduit for delivering cyber attacks into target organizations and individuals. This paper also outlines guidelines for defending against these threats.

'Blended Threats' from Nation States Combining with Criminal Gangs

Bryan Vorndran, Assistant Director of the FBI, made the following statement in a May 11, 2022 RSA Conference webcast on 'Mitigating Russian State-Sponsored Cyber Threats':

"Let me address what we refer to as the blended threat. As time has continued, there is no bright line between where nation state activity starts and stops and where criminal activity starts and stops. We have seen an increase in criminal actors moonlighting for other purposes in certain countries. Or the allowing of criminals to act more autonomously without much oversight or constraints on their activities within certain countries. That poses us deep, deep, concerns because if we don't know the command structure of the nation state - who is or isn't being tasked or authorized to do work - it does expand the capability of threats against the United States and our [partners]. That is becoming a growing concern for us – not necessarily just in Russia but globally. That's something that within the intelligence community, and within the FBI especially, we're paying a lot of attention to on a regular basis."

There are Many More Nation State Threat Actors Than 'The Big 4'

The common identification of Russia, China, North Korea and Iran as the world's main nation state cyber threat actors is in some ways misleading. The U.S. and its western allies are cyber threat actors in their own right too. It's just that the bias in the western world's framing of the threat landscape doesn't reflect that. Also, other countries besides those shown in **Figure 1** have had offensive cyber capabilities for a while. For example, the recent 'Pegasus Project' research provided evidence that a great many governments throughout the world are using Pegasus, the Israeli NSO Group's smartphone spyware. But the reality is that some of these countries were exploiting vulnerabilities in SS7 and Diameter signaling for similar spying on dissidents, foreign politicians, journalists and activists abroad years before Pegasus made headlines last summer.

The U.S. and its western allies are certainly cyber threat actors in their own right too. It's just that the bias in the western world's framing of the threat landscape doesn't reflect that.

The Line between Nation States and Independent Actors is Blurring

Before addressing some of the specific threats to a telco organization, it's worth noting some very important aspects of the modus operandi of nation state threat actors nowadays. It's a mistake to think that nation state threat actors operate entirely independently of their private sector peers. The boundaries have always been blurred but as shown by the recent statement by the FBI featured at the top of this page, the rate at which these boundaries are blurring is accelerating. Some examples include:

- Nation state actors buying and selling services like network access on the dark net.
- Nation state employees moonlighting on profit-generating cybercrime.
- Nation state allegiances affecting cyber gang strategy. For example, while Conti is considered an independent criminal cyber gang, some of its leaders nevertheless declared support for Russia's war aims when the invasion of Ukraine began. In revenge, Ukraine-supporting gang members leaked some of Conti's own data.
- Independent threat actors operating as direct or indirect proxies for nation states such as the Hezbollah-linked Lebanese Cedar serving as a proxy for Iran; NSO Group serving as a proxy for its many nation state clients; or indeed the army of volunteer hackers openly recruited online by the Ukrainian government to attack Russian targets on its behalf.
- Independent gangs executing ransomware attacks whose consequences trigger a national security response (e.g. Colonial Pipeline and Cost Rica examples in **Fig 2**).

Combining these factors above with the willingness of key nation state threat actors to take more risk with their offensive operations, it's easy to see how the FBI arrives at "deep, deep concerns" about blended threats as expressed at the top of this page.

Figure 2: The Blurring of Nation State Threat Actors and Criminal Cyber Gangs

Date	Threat actor	Activity	Implications for understanding nation state threats
2020	Lebanese Cedar	Hacks on telecom operators in the Middle East & North Africa.	Lebanese Cedar has strong links to Hezbollah which is funded by Iran. NSO Group is an Israeli company with strong links to Israel. Rightly or wrongly, they can easily be viewed as a nation state proxy. Any one of their activities can potentially be viewed as being on behalf of Iran/Israel.
July 2021	NSO Group	NSO's Pegasus smartphone spyware is sold to nation states and has been used for espionage on foreign leaders and dissidents abroad.	
July 2021	Darkside	Colonial Pipeline ransomware attack prompts President Biden to trigger an "all of government" emergency response by U.S Federal government.	Even when acting entirely independently of any nation state, as in both these instances, a highly damaging cyber attack by criminal cyber gangs on a nation's critical infrastructure can nevertheless trigger a nation state-level response by the government of a victim country.
May 2022	Conti	A highly effective ransomware attack on behalf of internal opposition to the Costa Rican government triggers a declaration of a state of emergency.	

Source: HardenStance

Blurring Boundaries Can Lead to Greater Risk of Escalation

Blended threats pose a serious risk of an escalation in cyber hostilities between nation state adversaries for the following reasons:

- Existing nation state threat actors can expand offensive operations by outsourcing.
- Smaller, poorer, nation state players can gain easier access to the cyber threat ecosystem, risking more rapid proliferation of cyber-attacks tools.
- Criminal gangs could have easier access to advanced nation state cyber weapons.

As threats become more blended, states will find it harder to make accurate attribution calls – and will be more likely to respond disproportionately.

The other major risk with blended threats is that it makes attribution harder. Nation states owe it to their citizens to hold other nation states accountable for actions for which they are directly or indirectly responsible. In cyber security, attribution is already hard enough. A proliferation of threat actors that are affiliated to nation state groups in one of several different ways - and a blurring or blending of responsibilities and accountabilities between the state and private affiliates - makes attribution harder still.

Drawing on two of the examples in **Figure 2**, the U.S and Costa Rican governments were able to conclude that the recent attacks on their country's critical infrastructure by the Darkside and Conti ransomware gangs were carried out by these private sector Russian threat actors without any direction from the Russian state. Hence no retaliatory measures against Russia were called for. The risk is that as threats become more blended, states will find it harder to make accurate attribution calls – and will become more likely to respond disproportionately.

Nation States Use Many More Attack Vectors Besides APTs

The SolarWinds hack, the Hafnium attack on Microsoft Exchange, the attacks on Etisalat, Mobily, Vodafone Egypt, Roshan Telecom and other telcos cited in **Figure 4**, and the many attacks using NSO Group's Pegasus spyware, are all examples of nation state threat actors deploying Advanced Persistent Threats (APTs). Some of these leverage Zero Day vulnerabilities, of which Google identified 58 in 2021, up from 25 in 2020.

APTs are costly - both to design and execute on through multiple phases, over months or years. To date, it's mostly nation state threat actors that have used APTs. They tend to have long term strategic goals involving very specific targets which may be relatively well defended. Cybercrime groups tend to be more opportunistic. But nation state threat

actors do use off-the-shelf tools too. North Korea relies heavily on ransomware. Faced with global sanctions, Russian state threat actors may follow independent Russian ransomware gangs to use ransomware to generate foreign currency income for the state rather than private profit. The blending of nation state and private sector activity could also drive more cybercrime gangs to use APTs.

A Telco Perspective on Nation State Cyber Threats

Figure 3 shows how a telco appears through the lens of a nation state threat actor. Telcos have direct connectivity to millions of individuals and organizations' networks as well as access to those customers' 'eyeballs'; they transport customers' real-time communications; and they store their private data. At any moment telcos even have data on those individual users' last known location - or even their exact current location.

A Defensive Strategy for All Stakeholders

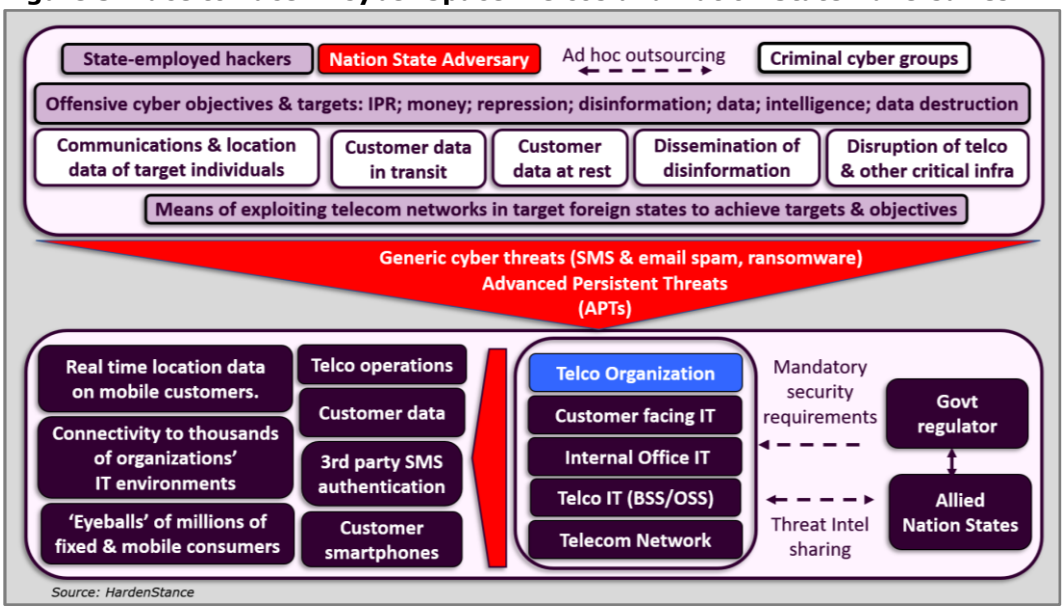
The rest of this paper looks at some key principles for defending telecom organizations and their networks in today's climate of increased cyber risk arising from adversarial nation state cyber operations. The first thing to consider is who the defender's stakeholders are and how their motivations are evolving. The security-related motivations of the telco itself (maintain revenues and reputation) and those of customers (a high quality, interruption-free, user experience) haven't changed much.

Faced with a heightened cyber threat emanating from adversary countries, governments are set to become increasingly prescriptive about telecom security.

By contrast, the outlooks of the governments that licence any telco or ISP are changing. Faced with a heightened cyber threat emanating from adversary countries, governments are set to become increasingly prescriptive about telecom security. They're also set to become increasingly willing to impose punitive sanctions on telcos that do not meet the higher cyber security standards expected of them.

A good example of this is the UK's new Telecommunications (Security) Act, which came into effect at the end of last year. The accompanying draft Telecommunications Security Code of Practice runs to 129 pages. As an example, the lengths that the draft code goes to to prescribe, mandate and prohibit detailed aspects of securing a telco's management plane goes much further than any previous UK legislation, possibly further than any telecom security code of practice anywhere. As for punitive sanctions, the Act gives Ofcom the power to impose fines for non-compliance of up to 10% of a telco's "relevant turnover". In most cases this is likely to cover the large majority of their annual revenues as a UK telecom operator. Once again, this is unprecedented for the UK telecom sector.

Figure 3: Face to Face in Cyber Space: Telcos and Nation State Adversaries



Untrusted Telecom Software Vendors are only the TIP of the Iceberg

Over the last five years, politicians and the media have focused intensely on the risk of nation state cyber threats arising from "untrusted" telecom vendors. In particular, western countries have banned Chinese vendors from their 5G networks. The risk of an adversarial nation state planting backdoors in a domestic telecom vendor's software is certainly real. However, there are other ways to plant backdoors in a telecom vendor's code. Bribing insiders to corrupt a western vendor's code is only one of many.

More importantly, the narrow focus on this one, politically charged, dimension of securing telecom networks against nation state threats has been extremely unhelpful to an accurate understanding of the nature of the threat outside the cyber security community itself. The range of stakeholders in business and politics - and within the telecom sector itself – that needs to be able to advocate the right kind of improvements in telecom security has been badly served by this myopia around backdoors in untrusted vendor software. This issue only scratches the surface of how telecom operators need to upgrade their security to the level required to defend against nation state threats.

A telco's entire CI/CD lifecycle needs to be secured by managing vulnerabilities, protecting workloads at runtime and securing APIs.

As part of a strategy to harden their security posture, telecom operators should be security testing all telecom vendor software themselves before they deploy it – no matter what vendor it comes from. As the saying goes, there's as much risk from bug doors as there is from backdoors. Hence telcos should also be rigorously managing the security risk associated with all the opensource software they use too.

The principle of Zero Trust, which needs to be embraced by telcos as much as by any organization, mandates not just that one or two foreign vendors are "untrusted" but that all vendors – and ultimately all interactions within the telco's environment – are inherently untrusted. The inherent trust that's embedded in the security architecture of a telco organization today must be evolved to support Zero Trust principles of least privileged access and continuous verification.

Telcos shouldn't just be asking for information about the security of a vendor's software development lifecycle either - they should be getting that development lifecycle independently audited. And as they migrate to cloud native deployments in their own telco cloud or in third party public clouds, a telco's entire Continuous Improvement/Continuous Deployment (CI/CD) lifecycle also needs to be secured by managing vulnerabilities, protecting workloads at runtime and securing APIs.

Hackers Had Access to Syniverse's Systems for Five Years

In the mobile services context, the highly sensitive role of IPX carriers and roaming hub providers in the ecosystem means that their security processes should also be independently audited. In September 2021, Syniverse stated in an SEC filing that hackers had access to some of its systems for five years before they were eventually detected. Although there has been no public attribution of this hack to any specific threat actor, the type of data that a company like Syniverse holds makes a nation state actor a prime suspect. Even if it wasn't a nation state, whatever it took to get in is something any nation state threat group would almost certainly have been able to pull off.

Figure 4: Nation State Threats Targeting Telecom Operators or Exploiting them to Target Others

Date	Threat	Cyber Attack or Threat Activity	Implication for Telco security
2019	Message Tap	Attributed to China-affiliated APT41 group, this monitored and stole SMSs on specific phone and IMSI numbers and keywords from compromised SMSC servers.	There are many more ways to intercept highly sensitive communications than listening in to voice calls via a switch.
2020	Lebanese Cedar	Breached un-patched Atlassian and Oracle servers in IT environments of several telcos including Vodafone Egypt, Mobily, and Etisalat for customer data.	Vulnerabilities in enterprise IT infrastructure can represent as great a cyber security risk to telecom operators as weaknesses in their telecom network infrastructure.
July 2019	Soft Cell	CDR exfiltration of CDRs from 10 telcos via a foothold in public facing web server by a threat actor assessed as China-affiliated.	
September 2021	Calypso, Red Foxtrot	Data exfiltration from the email servers of Roshan Telecom in Afghanistan by Chinese state threat actors over months. Activity spiked at the time of the U.S withdrawal.	
July 2021	NSO Group	Nation state adversaries are using NSO's Pegasus smartphone spyware for espionage on foreign leaders and dissidents abroad.	SS7 and Diameter firewalls must be a mandatory part of mobile network security to enable mobile operators to monitor and block attempted nation state espionage. While generally pretty good, smartphone operating systems still require further security hardening.
February 2022	Hidden Art	AdaptiveMobile Security publishes research on this Russia-based threat actor exploiting mobile network signaling for location tracking and intercepting communications.	
February 24th 2022	Russian state threat actor	Routers of thousands of Viasat's customers in Ukraine, including in the military, rendered inoperable. Government called it "a really major loss of communication."	End user CPE needs protecting from nation state threats – at both the network and endpoint level.

Source: HardenStance

China Has Shown How to Steal Telco CDRs via Public Facing Servers

All four nation state affiliated threat groups cited have shown there are easier ways to steal sensitive data from telcos than by embedding malware in a vendor's code.

Any politician or business leader with an opinion on banning Chinese vendors from 5G networks will know the names 'Huawei' and 'ZTE'. Very few would also recognise the names 'APT41' 'Lebanese Cedar', 'Soft Cell' or 'Red Foxtrot' cited in **Figure 4**. This is ironic, because all four of these nation state affiliated threat groups have shown there are easier ways to steal sensitive data from telcos than by cleverly embedding malware in a telecom vendor's code.

All four of these serious breaches managed to achieve the respective nation state's espionage goals by exploiting routine vulnerabilities in the target telecom operator's enterprise IT environment. As shown, in one case an initial foothold was established via un-patched Atlassian and Oracle servers. In the other three it was Short Message Service Centres (SMSCs) running on Linux, public facing web servers and email servers.

Protecting sensitive telco data against these types of attacks doesn't require political speeches. It shouldn't even require political action (although governments will seek to fill the gap if telcos don't raise their game themselves). What it needs as a matter of urgency now is investment in best practice enterprise IT security. That means comprehensive visibility, automation of monitoring and patching; and machine learning-assisted threat detection and response across networks and endpoints.

Telco Interfaces Need Protecting – Including the Old Ones

The telecom industry takes pride in its response to cyber threats in terms of the security features that are baked into the latest standards, most notably in the case of 5G. But the 5G Standalone (5G SA) networks that enable most of these security enhancements are only just starting to roll out in volume this year. It will be at least five to ten years before a sizable majority of mobile network traffic is protected by these new features, albeit the introduction of distributed User Plane Functions (UPF) and Multi Access Edge Compute (MEC) nodes will also serve to increase the attack surface.

Meantime, older protocols and interfaces must be protected. Even now in 2022, far too many telcos still do not use readily available encryption, integrity protection or firewalling of traffic on key mobile network interfaces. This includes Gi or SGi firewalls between the mobile core and the Internet; GTP firewalls within the mobile network and S1 and X2 protection across 4G backhaul networks.

Also still considered 'nice to have' rather than critical in too many cases are SS7 and Diameter firewalls on the operator-to operator-interconnect in 2G, 3G and 4G. This is a proven favourite threat vector for nation state espionage, whether by exploiting SS7 and Diameter signaling vulnerabilities or by combining endpoint malware and information harvesting messages as with Pegasus spyware. The S8 interface, which provides user plane tunnelling and tunnel management in roaming scenarios, is among other interfaces that are vulnerable unless properly protected. Consistent with Zero Trust principles, the kind of visibility that allows lateral movement of threats to be detected and mitigated in enterprise IT needs to be imported into a telco's network environment too.

Monitoring is helpful to telco security teams and the national security agencies that they are accountable to. But enhanced techniques need to be found for better defence in depth against Pegasus and other spyware variants.

Pegasus is Both Advanced and Persistent

There is no agreed definition of what an APT is but it's not controversial to consider Pegasus to be both advanced and persistent. Imagine, then, if a nation state got Pegasus onto the smartphone of an adversary country's President or Prime Minister. Imagine if the hostile actor were then able to use data from Pegasus to assassinate them. This would amount to the use of an APT to pull off a catastrophic breach of a country's national security.

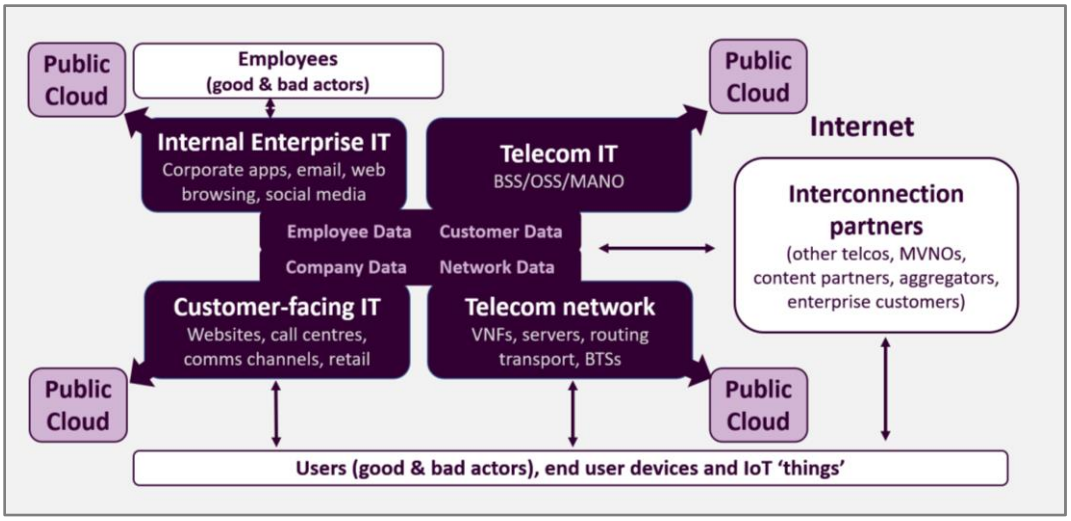
Pegasus is difficult to defend against because it leverages evasion techniques such as using encrypted messaging applications like WhatsApp. That said, many countries don't even have measures in place to monitor command and control messages like HLR lookups or user plane signatures like malicious DNS traffic, which could be used to support Pegasus in executing attacks. Monitoring of these can help telco security teams and the national security agencies they are accountable to. But enhanced techniques are also needed for better defence in depth against Pegasus and other spyware variants.

SMS and Email Spam Form Part of any Nation State's Cyber Arsenal

The examples cited in **Figure 4** show how a telco's SMS and email systems can be a target for nation state APTs. At a more basic level, consider also the key role that SMS email and social media campaigns play in a nation state's defensive and offensive cyber operations, most obviously right now in Ukraine.

Here, quite convincing fake CNN and BBC news pages are being created to fabricate news to suit either the Russian or Ukrainian governments. SMS and email campaigns are targeting soldiers and civilians with propaganda including guidance on giving themselves up on favourable terms. These nation state threat vectors are neither advanced nor persistent. Yet these rudimentary tools are nevertheless a critical part of the cyber arsenal that nation states are using to undermine stability and democracy in adversary countries – and they're doing this every day in peacetime, not just in exceptional wartime circumstances.

Figure 5: A Telco Security's Security Posture Covers the Entire Organization



Source: HardenStance

The C-Suite of telco management must lead in regularly reviewing and rehearsing the organization's cyber-attack response plans.

Anticipation and Preparation are Everything

As alluded to throughout this White Paper, and as depicted in **Figure 5**, a telecom operator's cyber security posture must embrace all of the organization's domains as well as the seams between them. That's why, for example, the UK's new draft Telecommunications Security Code of Practice prohibits so-called "Browse Up" architectures, whereby admins use the same corporate device for accessing the telco network management plane as well as for email and other office IT applications.

Anticipation and preparation are also critical. The C-Suite of telco management must lead in regularly reviewing and rehearsing the organization's cyber attack response plan. Ukraine's telecom sector has won great admiration over the last three months for the way it has maintained network and service availability in the face of intense cyber attacks from Russia. It's inconceivable this could have been achieved without rigorous anticipation of these threats and rigorous preparation for how to defend against them.

Lastly, the effective creation, enrichment and sharing of threat intelligence across the telecom sector – within and between countries and regions – is a key aspect of being able to anticipate advanced threats and defend against them. The telecom sector has a long way to go in this regard. Thanks to widespread adoption of the MITRE ATT&CK Framework, cyber security professionals in other industries share a basic common language and format for describing, classifying and sharing information on the threats they see - and sharing best practice approaches to prevention, detection and mitigation.

Such a common framework, one that takes into account the unique protocols and unique protocol behaviours of telecom networks, doesn't exist. It goes without saying that it's urgently needed. The last twelve months have at least seen an acceleration in telecom industry efforts aimed at developing this in a way that aligns as much as possible with the enterprise security model of threat intel sharing. Work is underway but the pace of progress does need to pick up. ■

About the Sponsors

The sponsors of this White Paper are Enea AdaptiveMobile Security and Palo Alto Networks.

About Enea

Enea is a world-leading specialist in software for telecom and cybersecurity. The company's cloud-native solutions connect, optimize, and secure services for mobile subscribers, enterprises, and the Internet of Things. More than 100 communication service providers and 4.5 billion people rely on Enea technologies every day.

Enea has strengthened its product portfolio and global market position by integrating a number of acquisitions, including Qosmos, Openwave Mobility, Aptilo Networks, and AdaptiveMobile Security. Enea is headquartered in Stockholm, Sweden, and is listed on Nasdaq Stockholm. For more information on Enea AdaptiveMobile Security visit www.adaptivemobile.com

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyber threats, so organizations can embrace technology with confidence. We provide next-gen cyber security to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art AI and automation.

Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice. For more information on mobile network security, visit www.paloaltonetworks.com/5G

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, OASIS, MEF, The GSMA and ETSI. HardenStance is also a recognized Cyber Threat Alliance 'Champion'. To learn more visit www.hardenstance.com

HardenStance Disclaimer