Security Conference 2022

Nation State Threats and Supply Chain Risk to the Telecom Sector

Patrick Donegan, Principal Analyst,
HardenStance

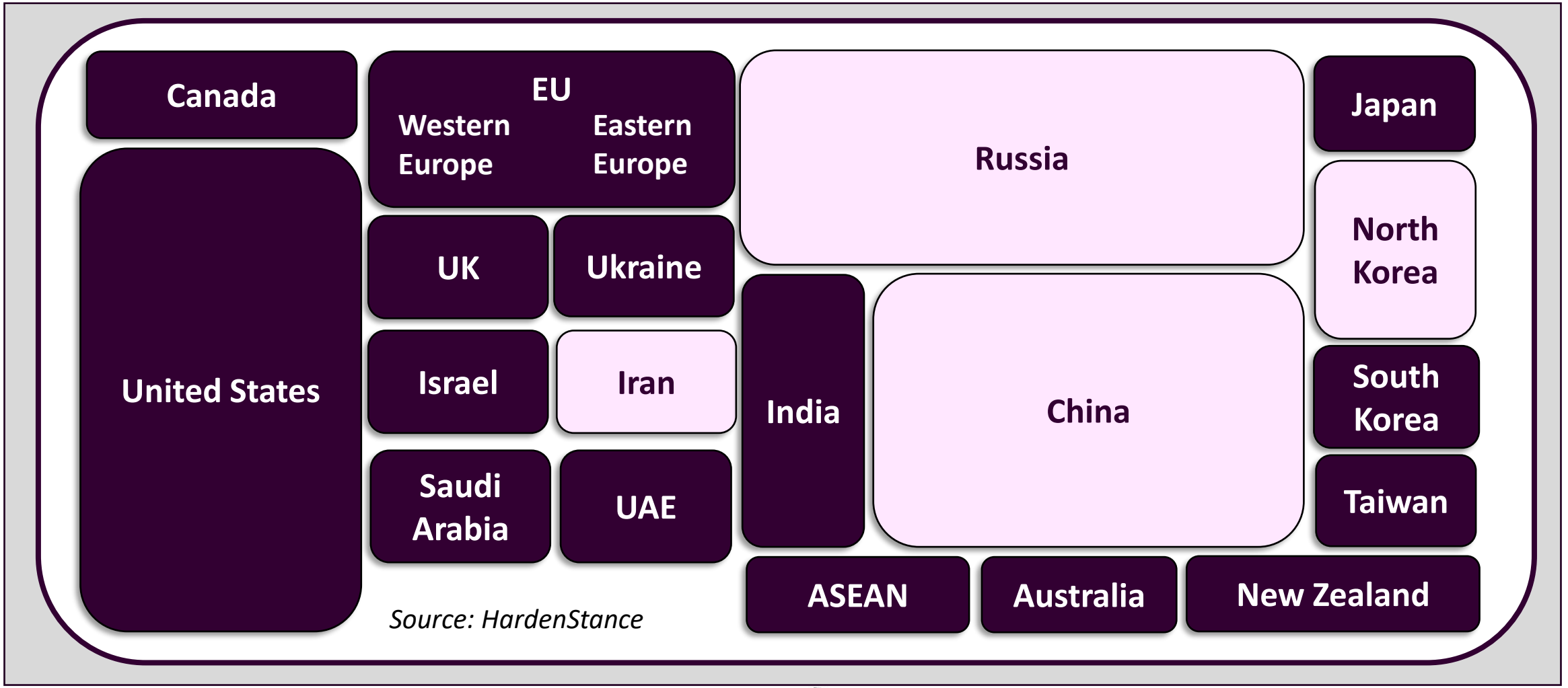
3/10/22

Agenda

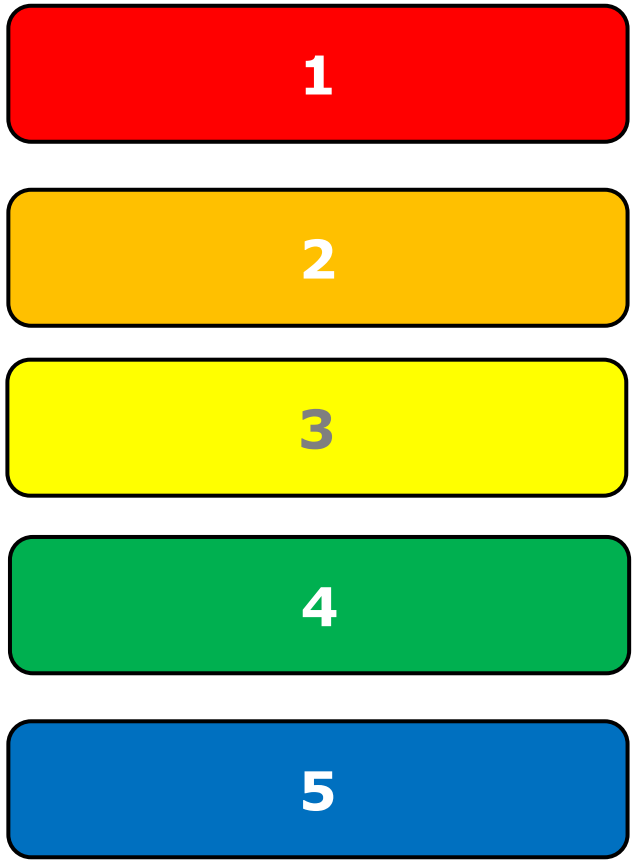
- Cyber and kinetic conflict between nation states.
- The telecom sector in defensive and offensive cyber operations.
- Defending the telecom sector against nation state cyber threats.
- Supply chain risk and risk mitigation in telecom.
- Recommendations

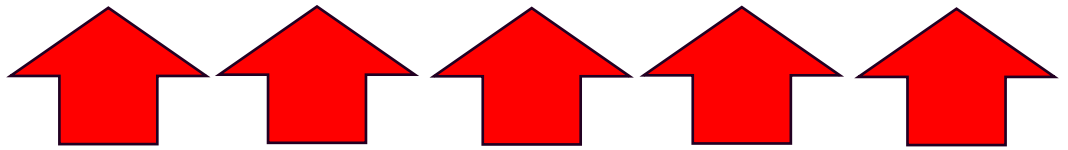
Nation State Cyber Threats

The World's Leading Cyber Powers:
A Western Perspective



Nation states are taking more risk with offensive cyber operations





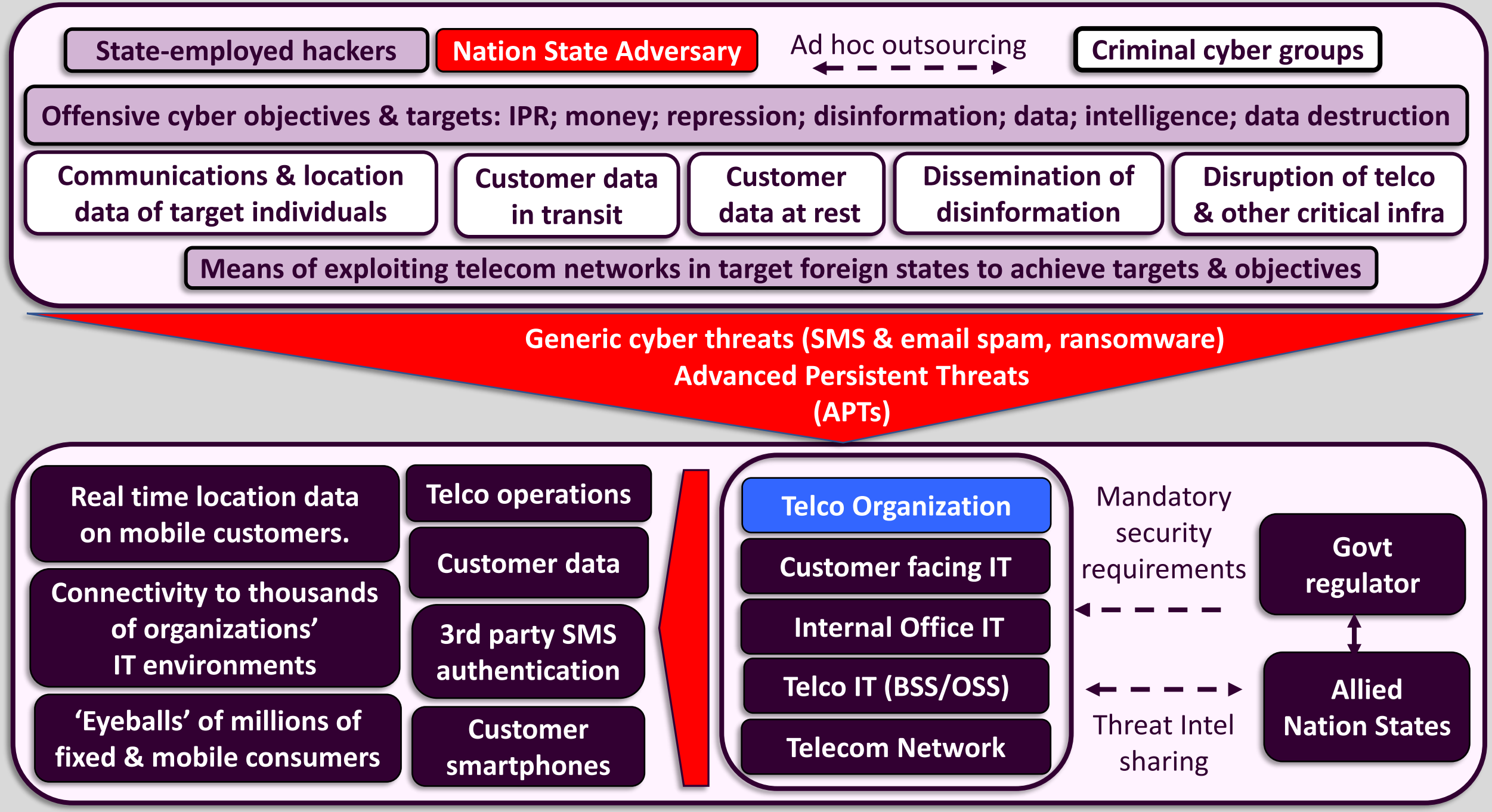
Russia (Viasat)

Hafnium (China) Albania/Iran

The Blurring of Cyber Threat Actors Makes Attribution Harder

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



Source: HardenStance

Nation State Cyber Threats Targeting Telcos

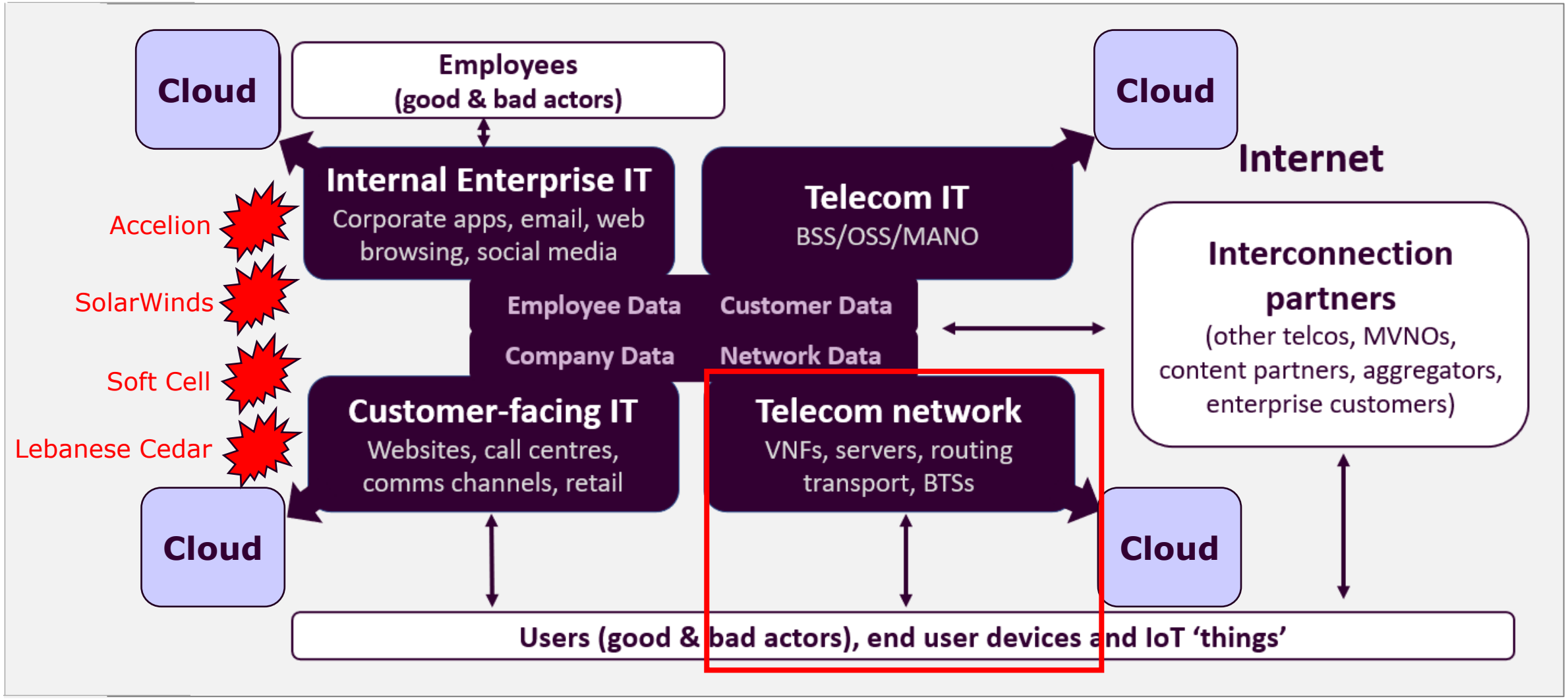
Date	Threat	Cyber Attack or Threat Activity	Implication for Telco security
July 2019	Soft Cell	CDR exfiltration of CDRs from 10 telcos via a foothold in public facing web server by a threat actor assessed as China-affiliated.	Vulnerabilities in enterprise IT infrastructure can represent as great a cyber security risk to telecom operators as weaknesses in their telecom network infrastructure.
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.	
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

Mainstream IT vulnerabilities ←

Legacy telecom vulnerabilities ←

Security Must Span Multiple Domains



Mobile networks at war: Ukraine's experience

Source: Enea AdaptiveMobile Security

Supply Chain Risk

A permanent restructuring of regional and global supply chains

~~**Cost & Efficiency**~~

Stability & Sustainability

Evolution in Supply Chain Risk

Source: HardenStance

Supply Chain Risk in Telecoms: Network Equipment

- **Drivers**
  - Governments, national security agencies, hyper-scalers.
- **Core**
  - Good progress - increasing diversity of supply.
  - Investor scrutiny still needed.
- **RAN**
  - Some progress - End to End system vendors making the biggest impact.
  - **OpenRAN**
    - On its third iteration.
    - Negligible market momentum.
    - Quality of security is always dependent on scale.
    - Minor impact on supply diversity (or costs or revenues)
    - Politicians have yet to catch up.

Supply Chain Risk: Chip Supply

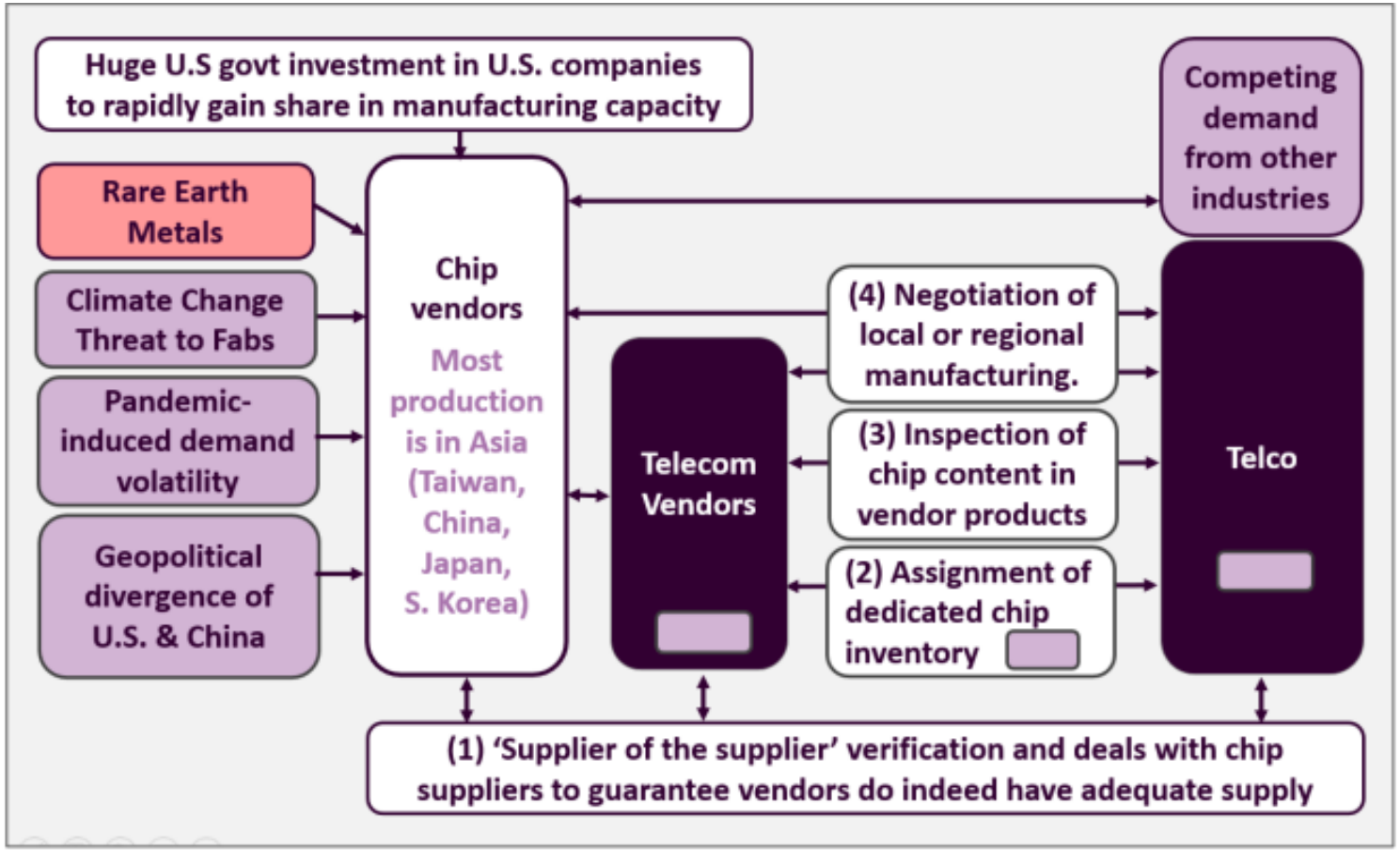
Chuck Robbins, CEO, Cisco

August 18th 2022: "After a challenging April due to the Covid-related shutdowns in Shanghai, and the impact on semiconductor and power supplies, overall supply constraints began to ease slightly at the back half of the fourth quarter [which ended 30 July]"

Gary Smith, CEO, Ciena

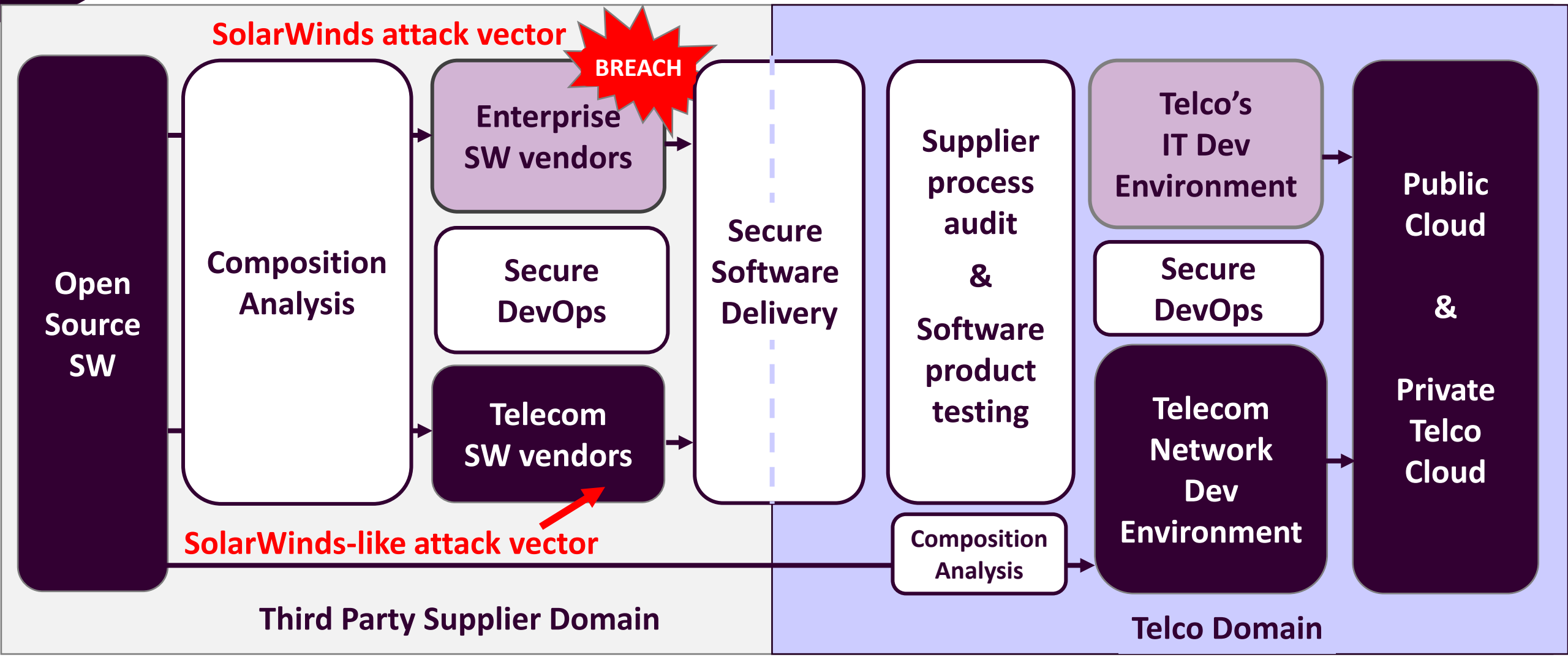
September 1 2022: "late delivery and substantially lower-than-committed volume from a small number of suppliers for specific components"

Supply Chain Risk: Chip Supply



Source: HardenStance

Securing the Development Life Cycle



Recommendations for operators

- **Nation State Cyber Threats**
  - Risk is escalating and potentially set to escalate further.
  - Invest more in cyber security defences - people, processes, office IT.
  - Improve cyber threat intelligence sharing.
- **Supply Chain Risk**
  - Invest in challenger core network vendors and E2E system vendors.
  - Chip supply issues are ongoing – reach further back, revise, scrutinize.
  - Secure your supply chain - comprehensively
- **Step up now – ahead of more stringent govt regulation**

Questions?