

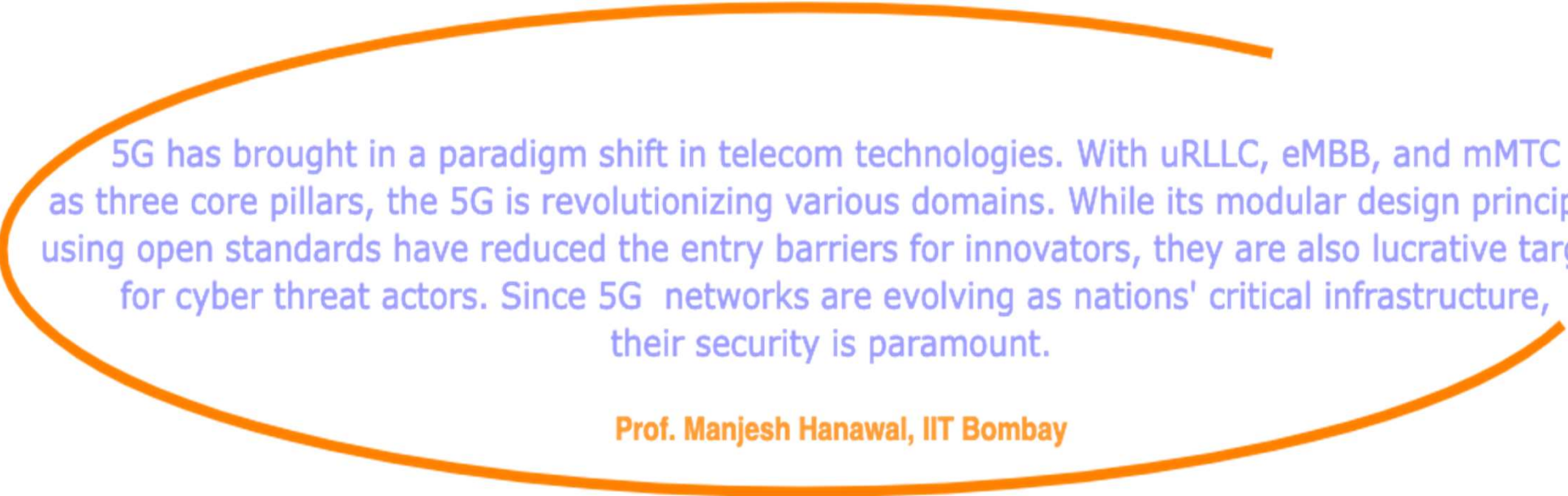


International Conference on 5G Network Security 9th & 10th Aug 2023

Vulnerability in 5G core and Mitigation Approaches

Manjesh Kumar Hanawal
IIT Bombay

Team Members: Shubhda Gadgil, Anjali Sharma, Sanjay Mehta



5G has brought in a paradigm shift in telecom technologies. With uRLLC, eMBB, and mMTC as three core pillars, the 5G is revolutionizing various domains. While its modular design principles using open standards have reduced the entry barriers for innovators, they are also lucrative targets for cyber threat actors. Since 5G networks are evolving as nations' critical infrastructure, their security is paramount.

Prof. Manjesh Hanawal, IIT Bombay

Vulnerability in 5G core

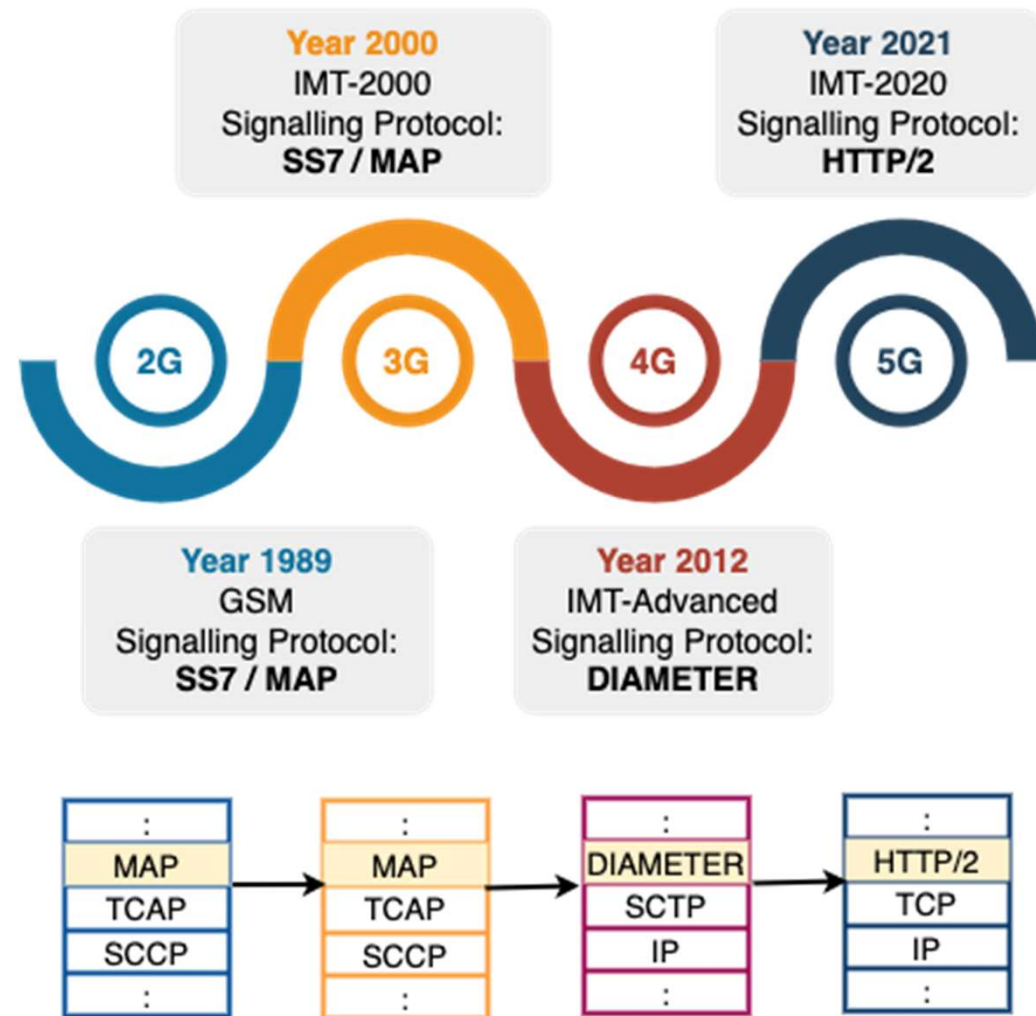
Evolution of Protocol Stack

Mobile network core signaling protocols evolved from **niche telecom-specific closed protocols to well known web-based protocols.**

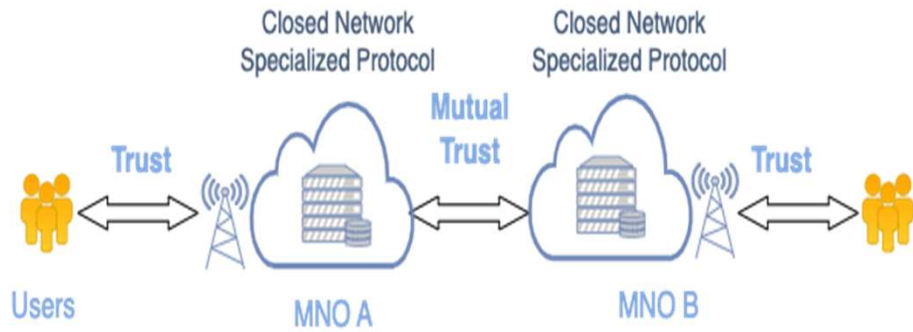
- HTTP/2 and JSON as application layer and serialization protocols, replacing Diameter.
- TCP with TLS providing encrypted communication between NFs and public land mobile network
- RESTful framework with OpenAPI as the Interface Definition Language (IDL).

As these protocols are used in the wider IT industry it will likely lead to

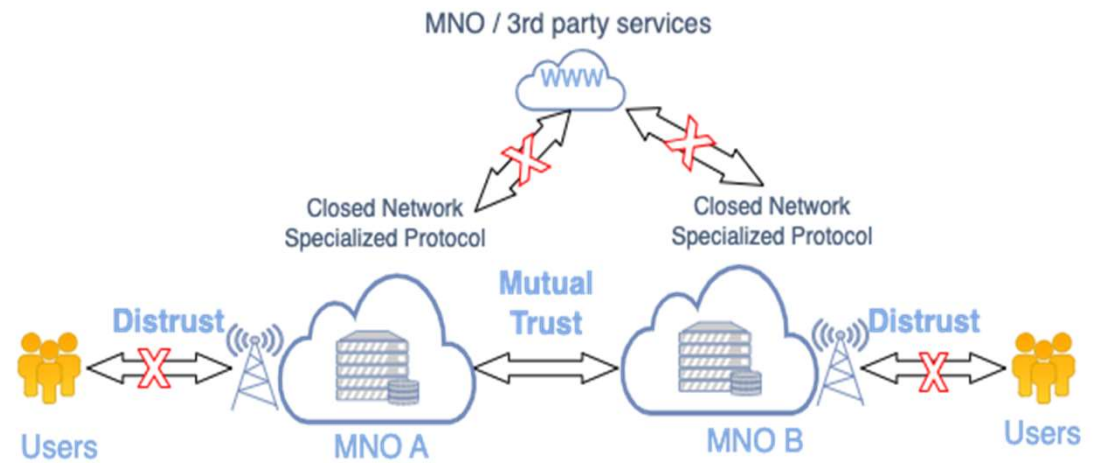
- **A shorter vulnerability to exploitation timeline**
- **Higher impact of vulnerabilities**



Evolution Of Trust Models



2G Trust Model

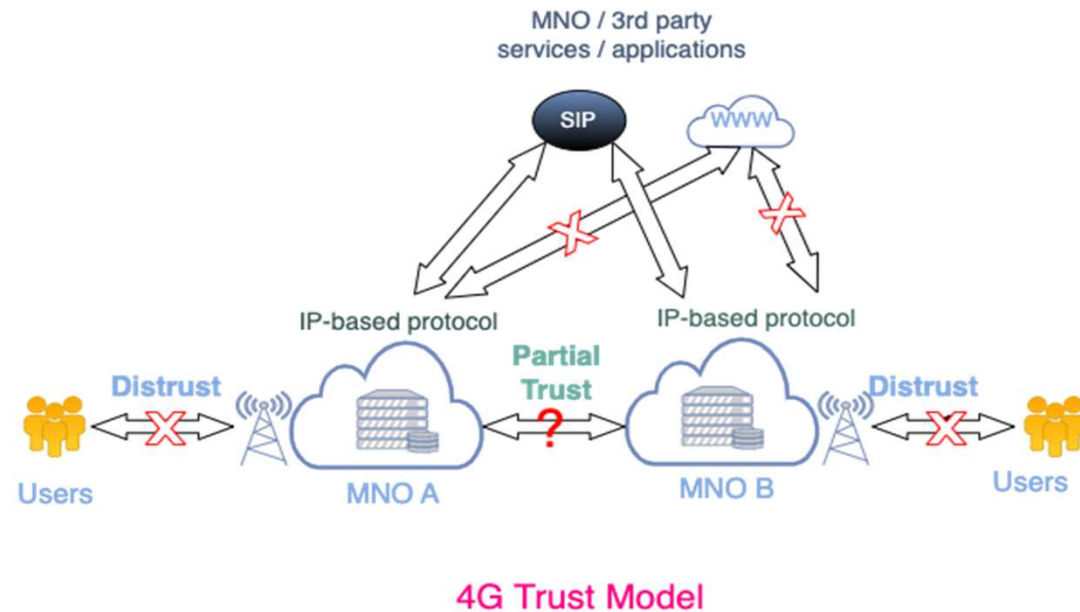
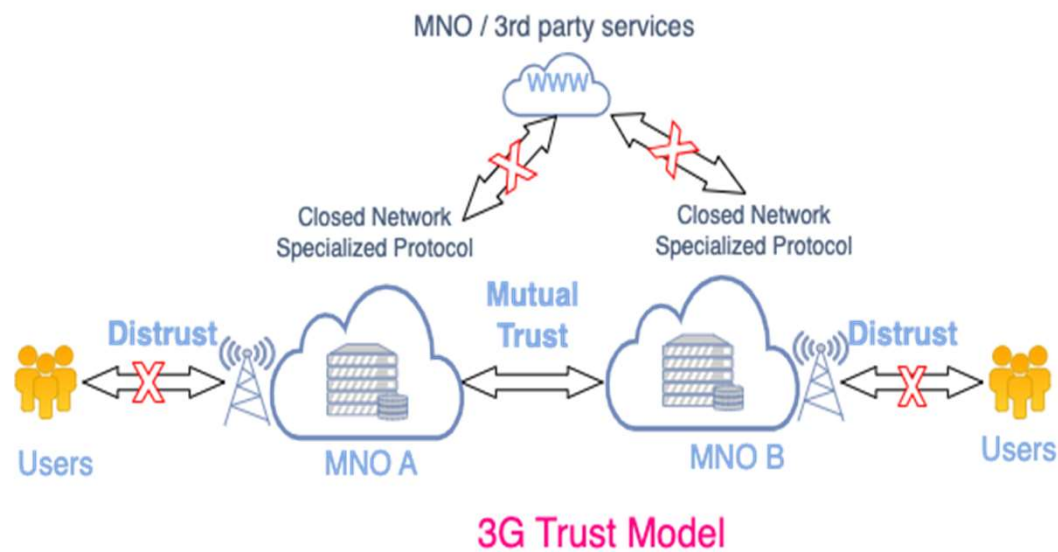


3G Trust Model

Full trust to trust only at the core

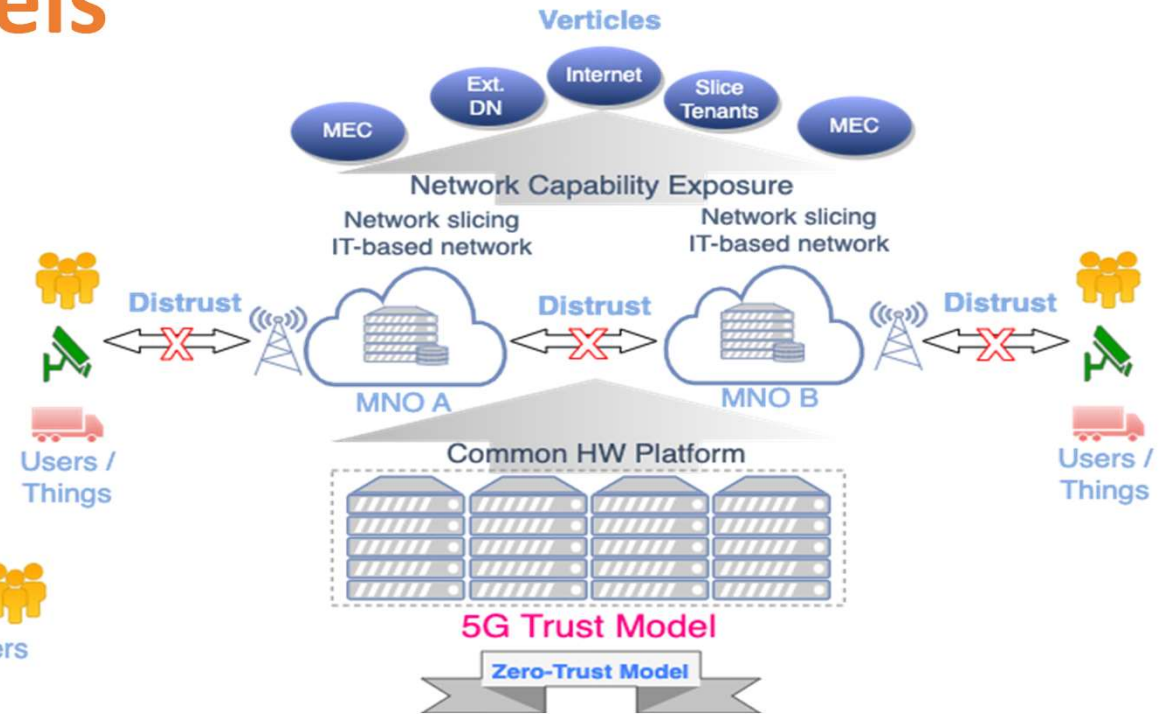
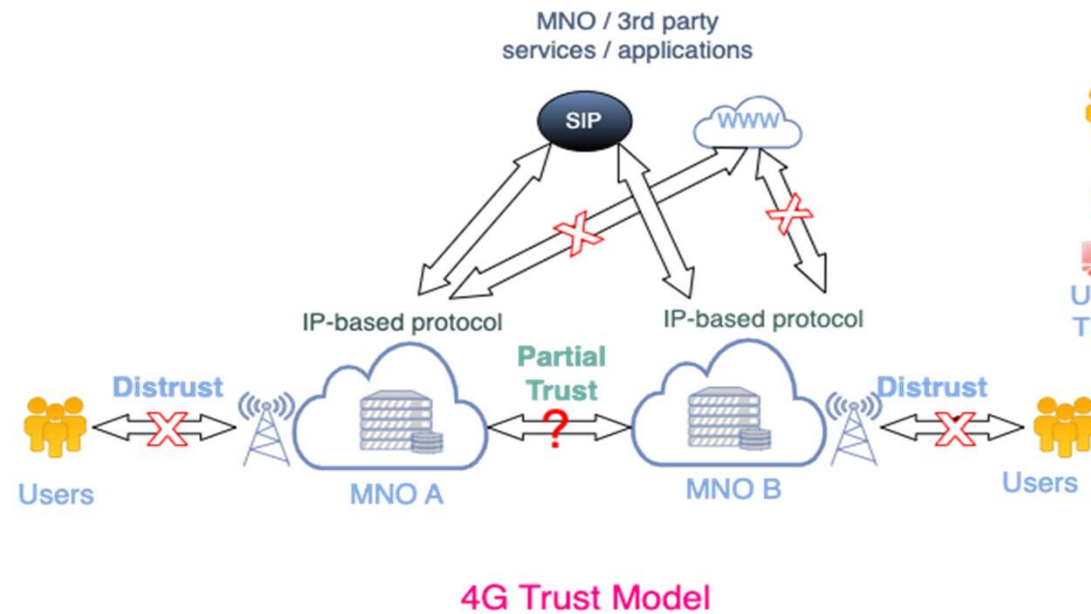
MNO: Mobile Network Operator

Evolution Of Trust Models



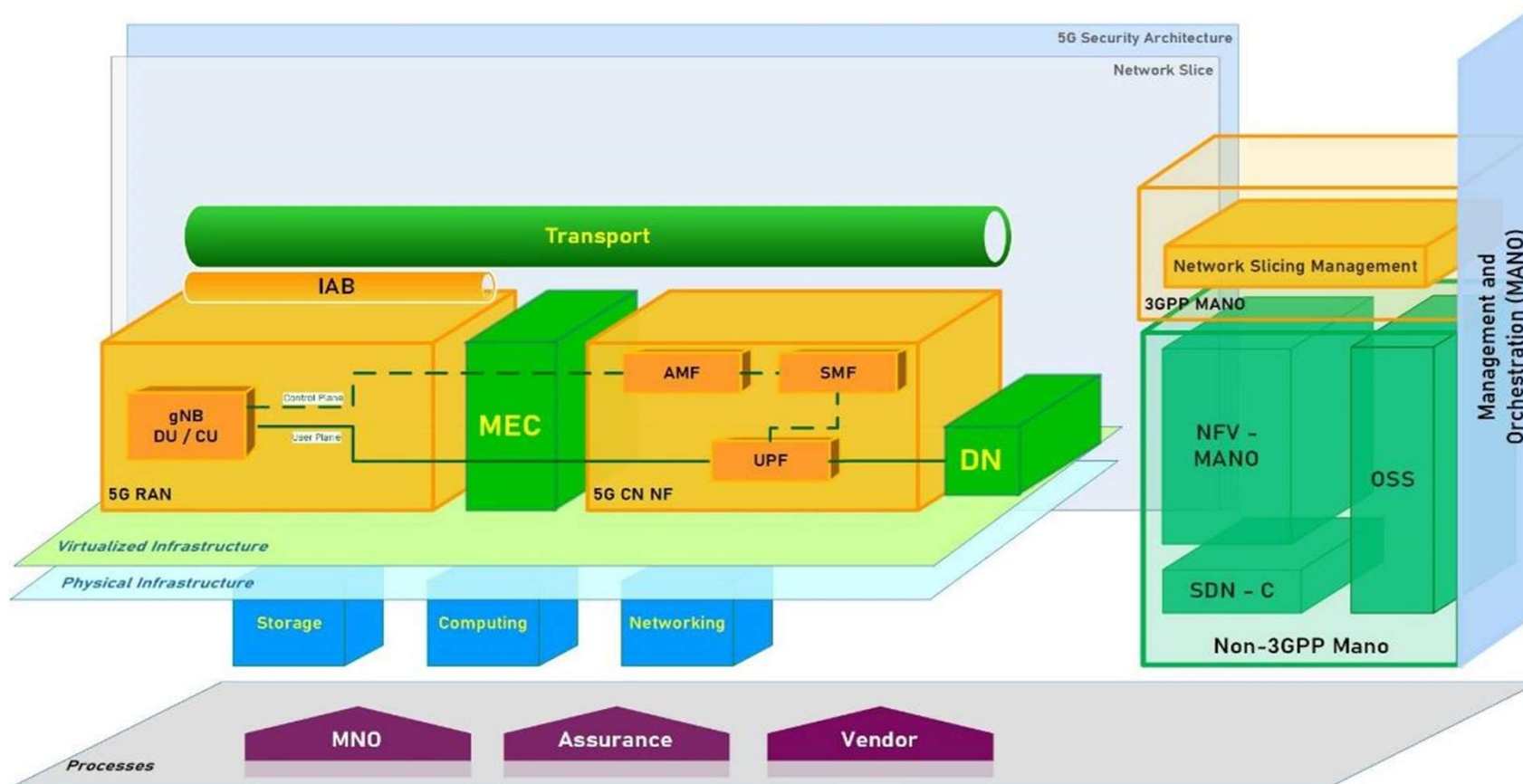
Trust at the core to partial trust at the core

Evolution Of Trust Models



Partial trust to zero trust

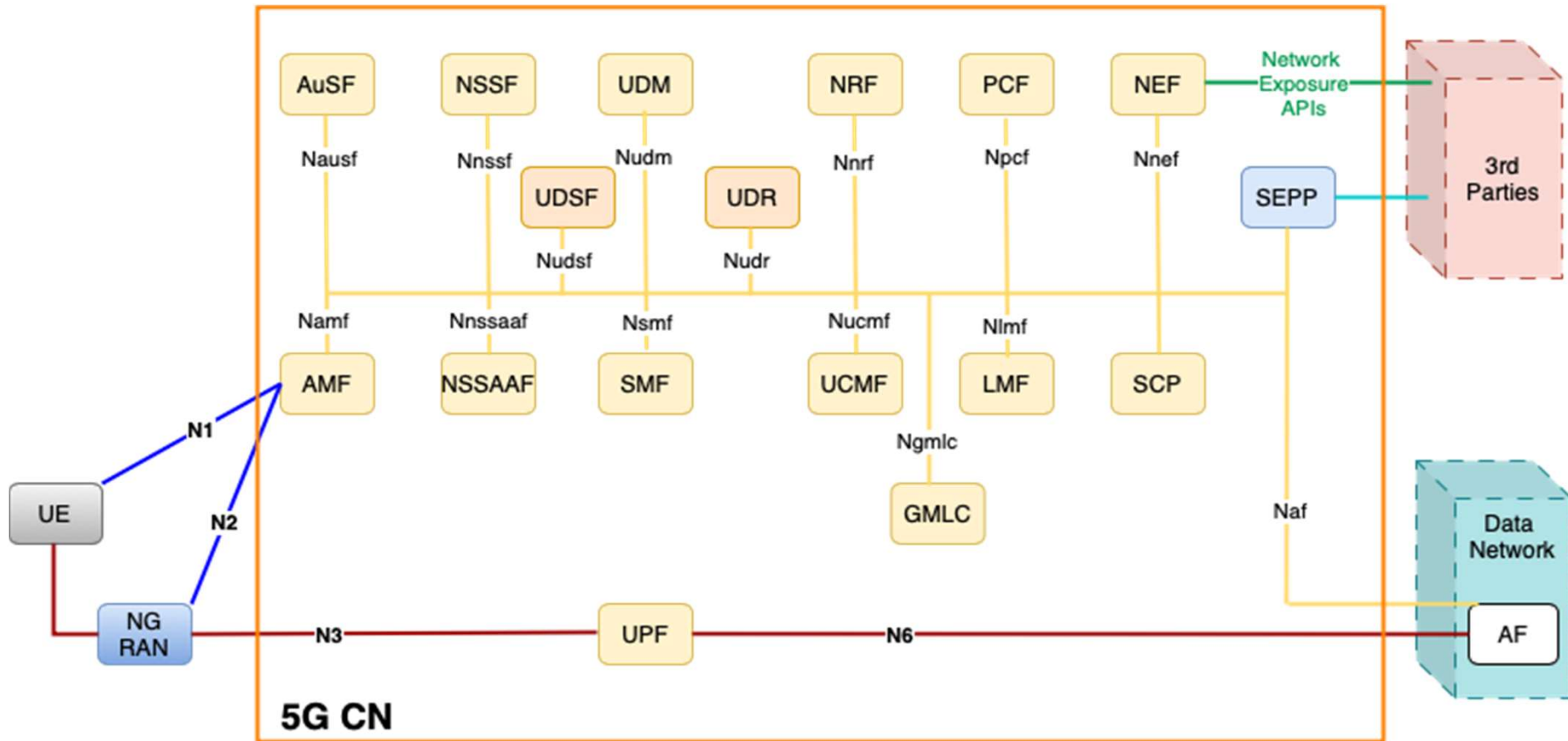
5G Generic Architecture



MNO: Mobile Network Operator
IAB: Integrated Access and Backhaul
DN: Data Network
MEC: Multi-Access Edge Cloud

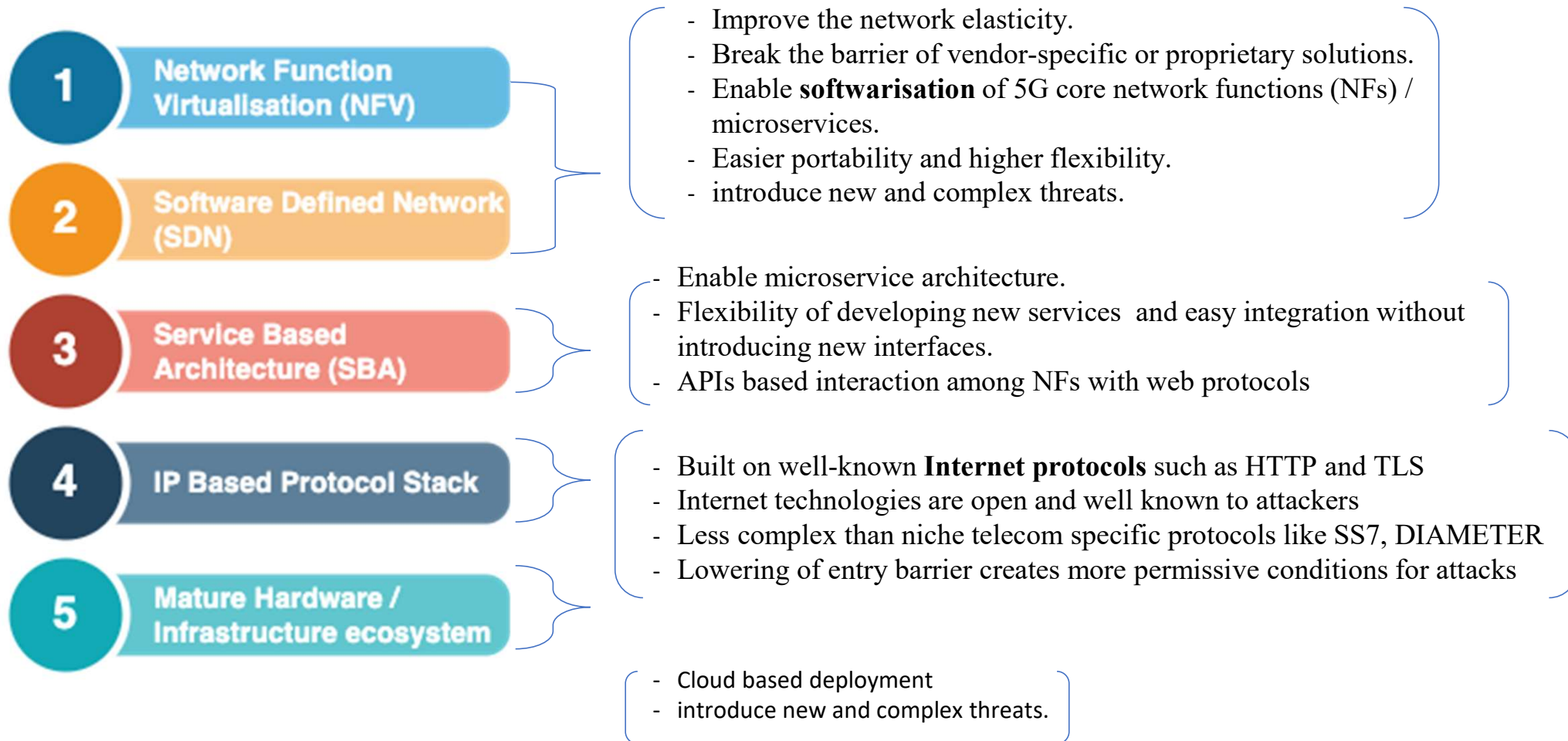


5G Core Network architecture

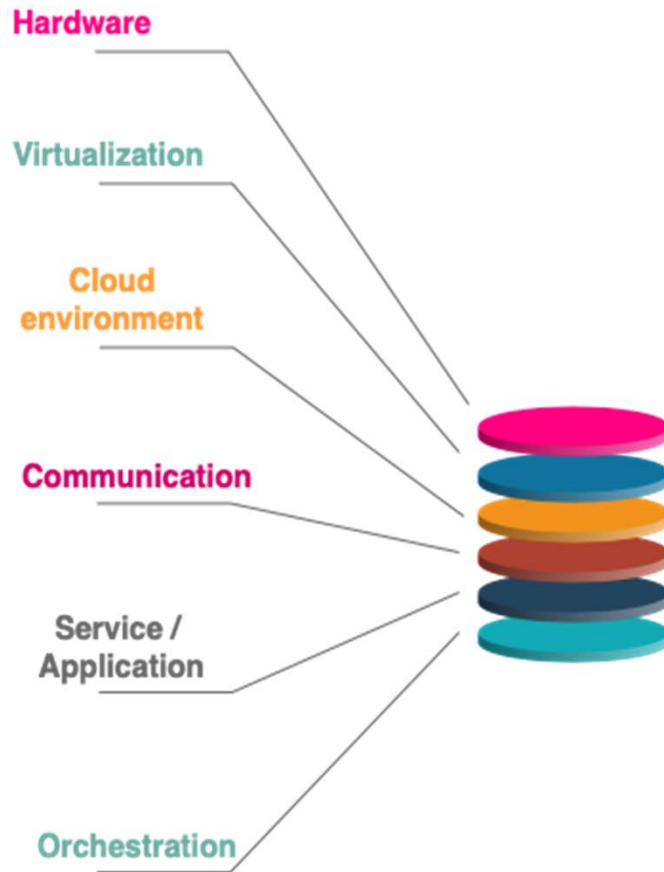


5G Core network structure as defined by 3GPP
(Service Based Architecture)

Key Components/Technologies enabling 5G Core



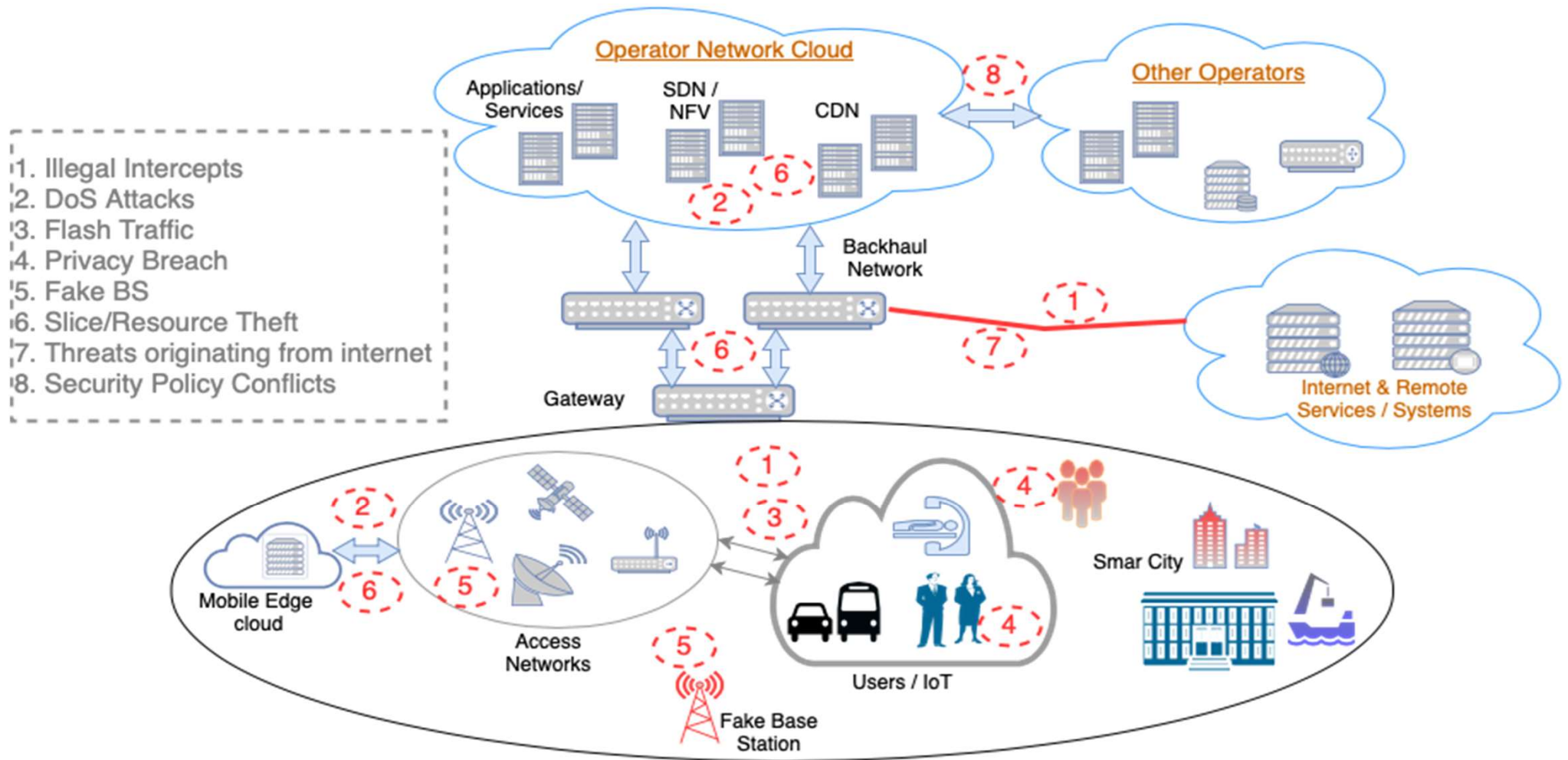
Threat Sources Landscape



Layers	Threat examples
hardware	Hardware backdoors, hardware bugs
Virtualizations	Sandbox escape, hypervisor compromise, shared memory attacks
Cloud	Unlimited control cloud providers over everything it runs
Communications	Classical attacks on the network stack, DDoS, MITM, Sniffing, Spoofing
Service/Application	Sql injection, broken authentication and access control
Orchestration	Registering malicious node and redirecting communication to them

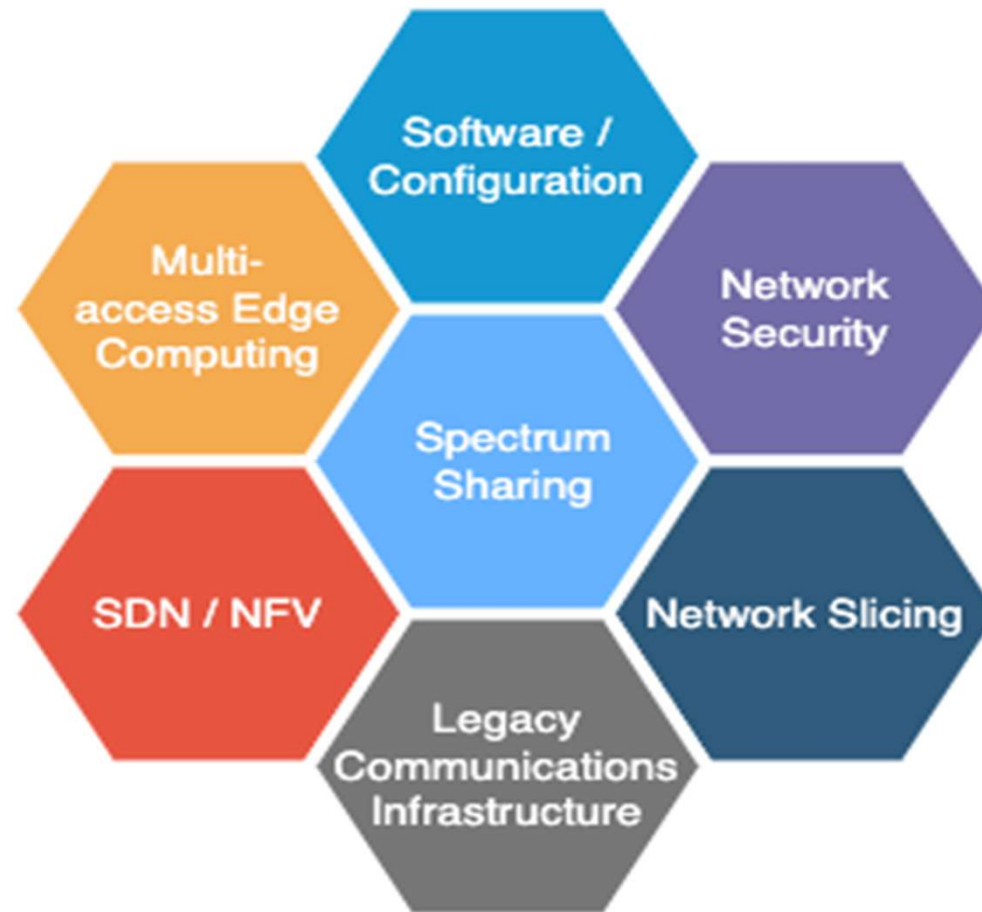
* This layered categorization is not claimed as complete, but it gives a good overview of threat sources

Security Threat Landscape



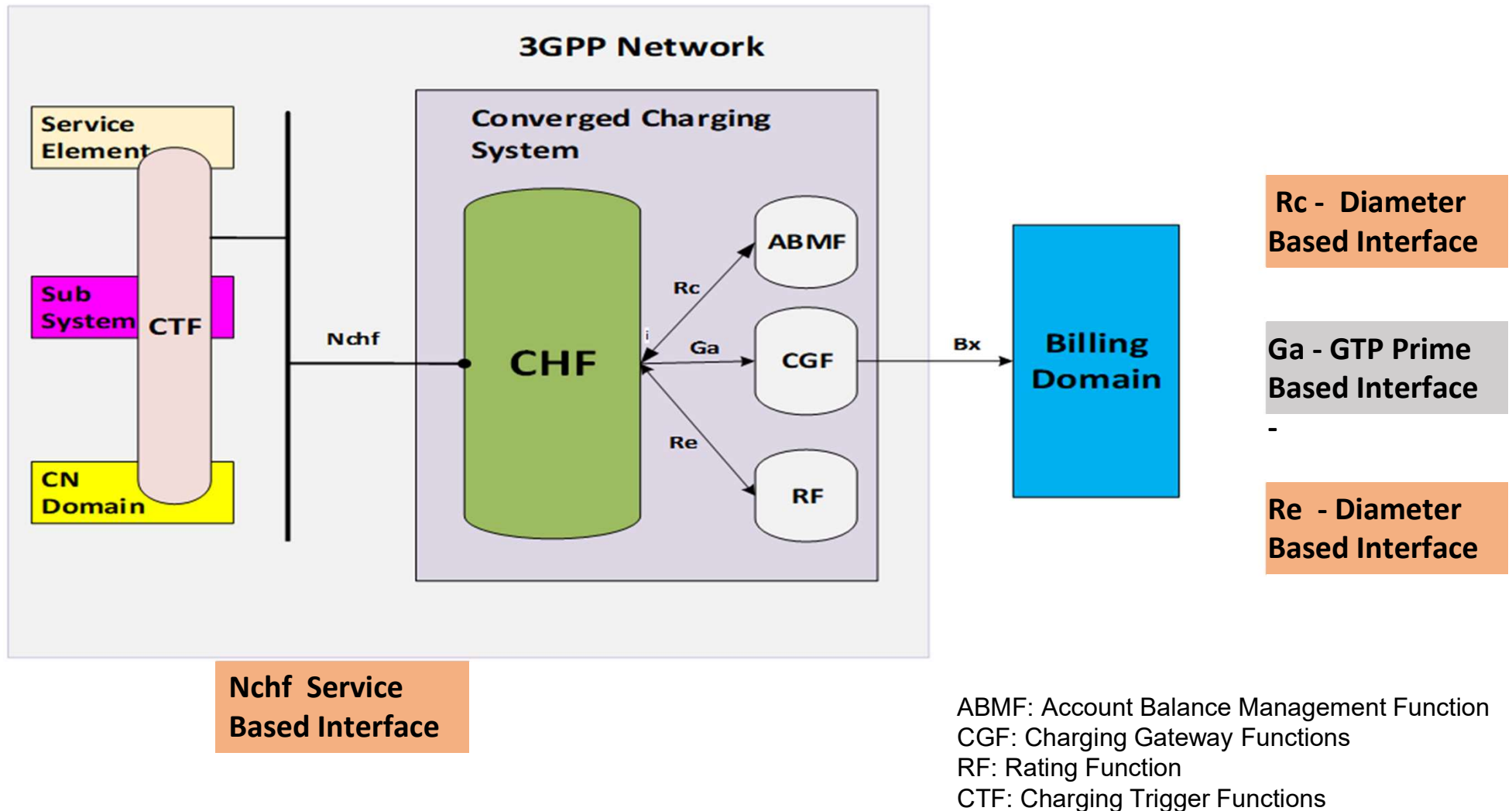
ITU: Security threat landscape in 5G networks

5G Systems Architecture Sub-Threat Vectors

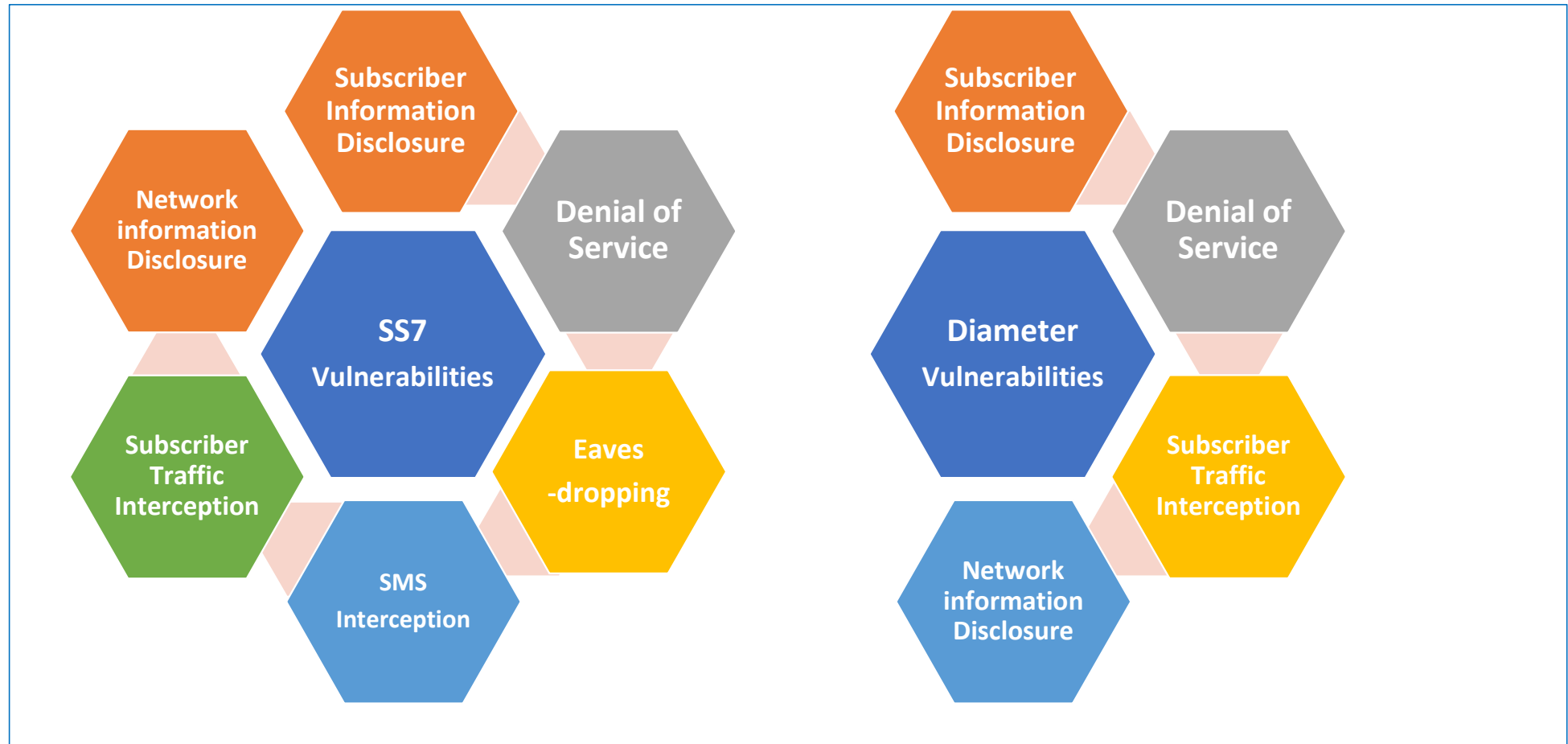


ESF *Potential Threat Vectors to 5G Infrastructure* white paper, released in May 2021,

Legacy Communication Infrastructure Example

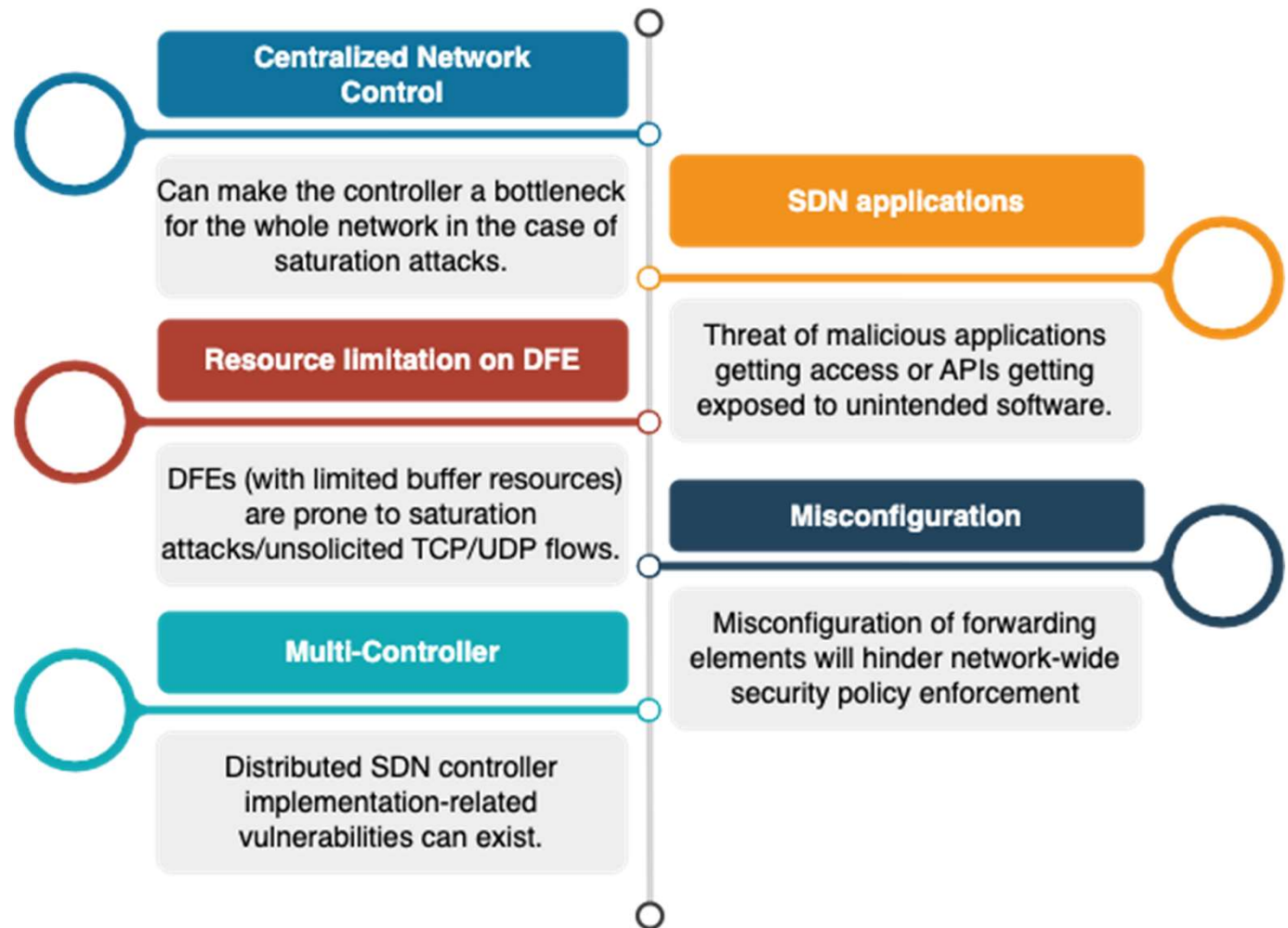


Threats from Legacy Protocols



Security Challenges in SDN

SDN simplifies network management with 'softwarisation' by enabling **programmability** and **centralized network control**.

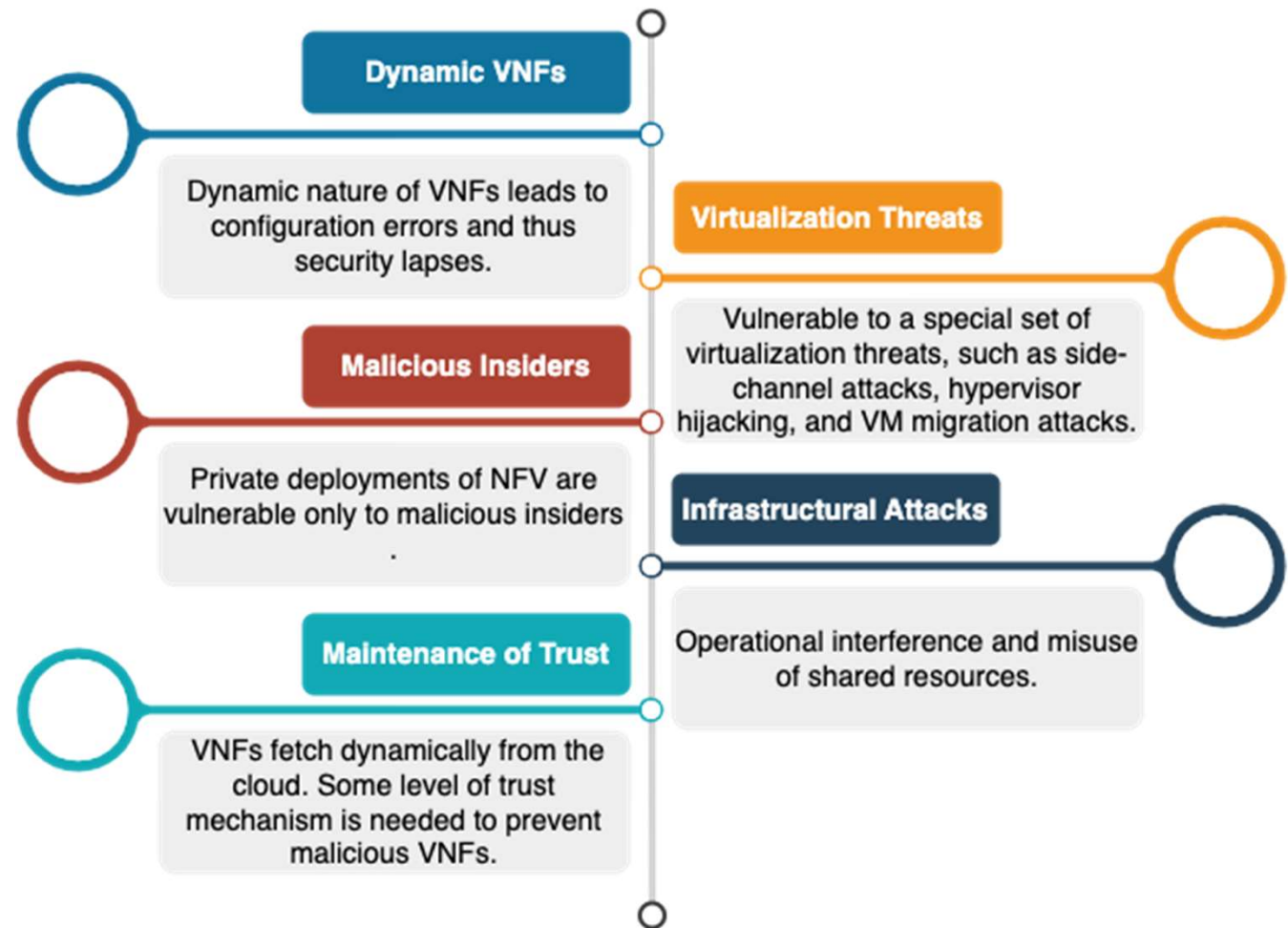


* DFE – Data Forwarding Element

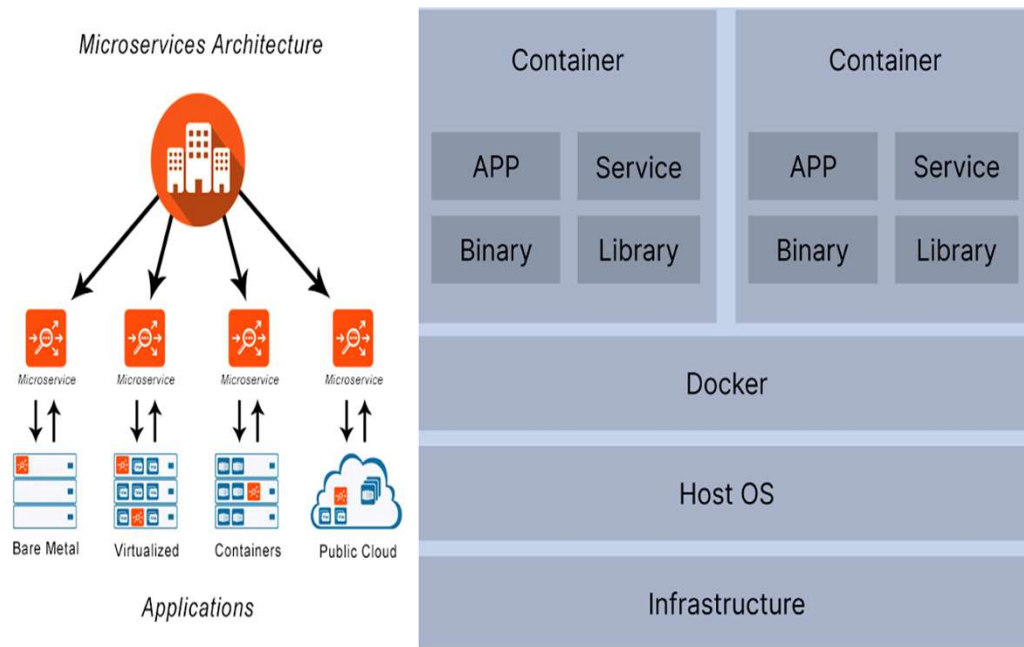
Security Challenges in NFV

ETSI Network Functions Virtualisation (NFV) is a technology innovation to support cloud, software and virtualization techniques.

It leverages virtualization characteristics to simplify deployments with increased support for automation.



Container Vulnerabilities and Attacks



Misconfigured Containers, privilege mode

Lateral movement and Privilege escalation

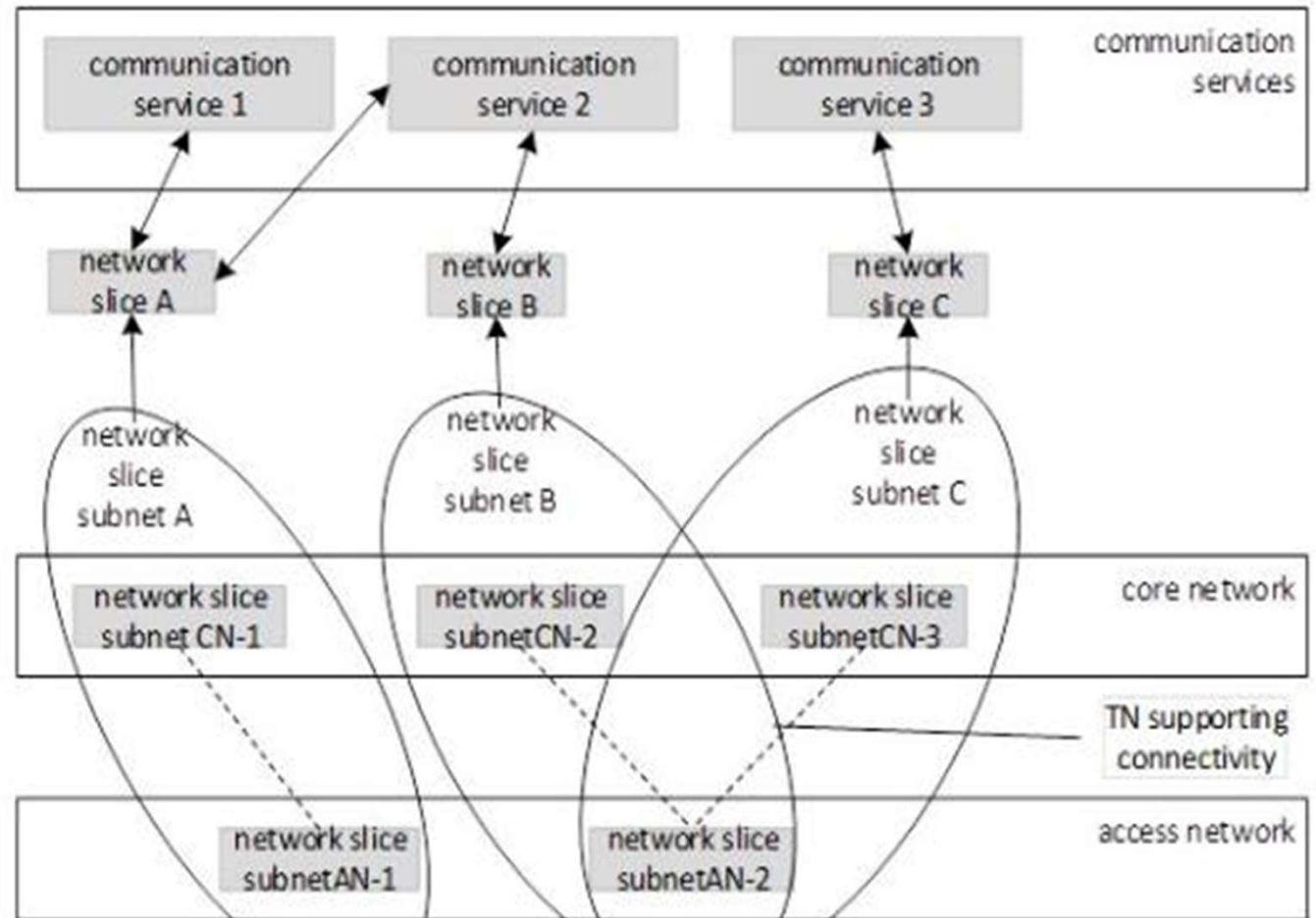
Container escape to control host machine

Compromised container images

Mismanaged container orchestration

Network Slicing

- Network slicing refers to partitioning of one physical network into multiple virtual networks, each architected and optimized for a specific application/service.
- Slices are logically isolated, but resources can be shared among them.



A variety of communication services provided by multiple network slices

Security Challenges in Network Slicing

Complexity of slice management

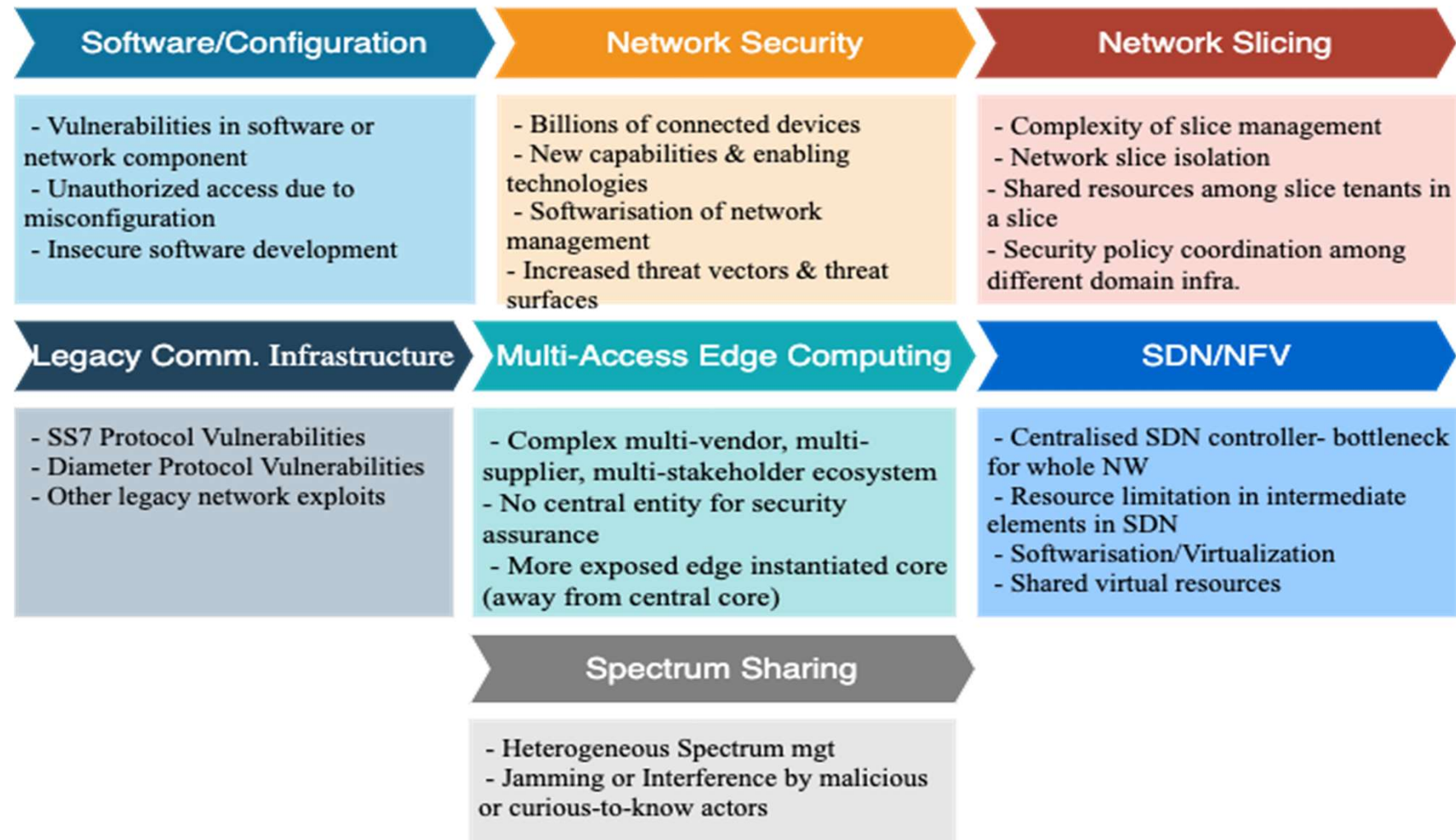
Network slice isolation (Inter-Slice)

Shared resources among slice tenants (Intra-Slice)

**Security policy coordination among different
domain infrastructure**

Decentralised resource allocation control

5G Systems Sub-Threat Vectors-Continued



Mitigation Techniques

CIA Framework



CIA triad



Extended CIA

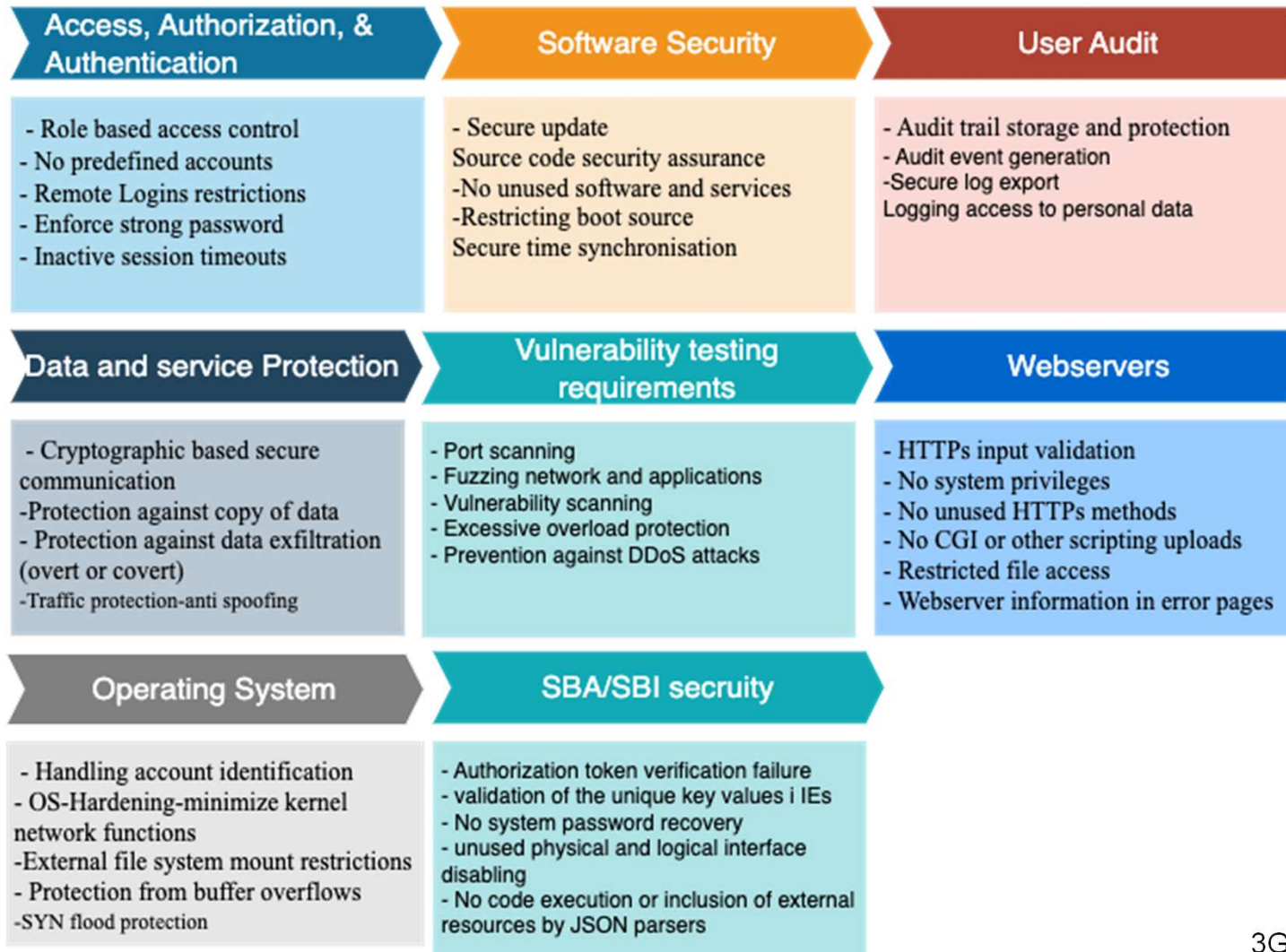
Common Security Requirement of Network Core

Applies to all network functions of 5GC



3GPP SCAS, ITSAR documents

Common Security Requirement of Network Core



Cloud security requirements

- Detect malicious cyber actor activity in 5G clouds and prevent actors from leveraging the compromise of a single cloud resource to compromise the network.
- A TEE is an area in memory protected by the processor in a computing device.
- Ensure that network and customer data is secured during all phases of the data lifecycle (at-rest, in transit, while being processed).
- Ensure that 5G cloud resources (e.g., container images, templates, configuration) are not modified without authorization.



Cybersecurity: Attack Life Cycle

1. Advanced Persistent Threat group (low-and-slow)
2. Ransomware attacks (smash and grab)



The attackers use certain Tactics, Techniques and Procedures (TTP) to launch attacks

MITRE ATT&CK framework

Linux Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the Linux platform.

[View on the ATT&CK® Navigator](#)

[Version Permalink](#)

layout: flat ▼

show sub-techniques

hide sub-techniques

help

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
8 techniques	8 techniques	16 techniques	11 techniques	22 techniques	15 techniques	21 techniques	7 techniques	14 techniques	16 techniques	8 techniques	13 techniques
Drive-by Compromise	II Command and Scripting Interpreter (4)	II Account Manipulation (1)	II Abuse Elevation Control Mechanism (2)	II Abuse Elevation Control Mechanism (2)	II Adversary-in-the-Middle (2)	II Account Discovery (2)	Exploitation of Remote Services	II Adversary-in-the-Middle (2)	II Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	Boot or Logon Autostart Execution (2)	II Boot or Logon Autostart Execution (2)	Debugger Evasion	II Brute Force (4)	Application Window Discovery	Internal Spearphishing	II Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication	II Boot or Logon Initialization Scripts (1)	II Boot or Logon Initialization Scripts (1)	II Deobfuscate/Decode Files or Information	II Credentials from Password Stores (3)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	II Data Encoding (2)	II Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Hardware Additions	Native API	Browser Extensions	II Create or Modify System Process (1)	II Execution Guardrails (1)	Exploitation for Credential Access	Debugger Evasion	II Remote Service Session Hijacking (1)	Automated Collection	II Data Obfuscation (3)	Exfiltration Over C2 Channel	II Data Manipulation (3)
II Phishing (3)	II Scheduled Task/Job (3)	Compromise Client Software Binary	II Event Triggered Execution (3)	II File and Directory Permissions Modification (1)	II Forge Web Credentials (1)	File and Directory Discovery	II Remote Services (2)	Clipboard Data	II Dynamic Resolution (3)	II Exfiltration Over Other Network Medium (1)	II Defacement (2)
II Supply Chain Compromise (3)	Software Deployment Tools	II Create Account (2)	II Escalate to Host	II Hide Artifacts (7)	II Input Capture (3)	Network Service Discovery	Software Deployment Tools	Data from Information Repositories	II Encrypted Channel (2)	II Exfiltration Over Physical Medium (1)	II Disk Wipe (2)
Trusted Relationship	System Services	II Create or Modify System Process (1)	II Exploitation for Privilege Escalation	II Hijack Execution Flow (1)	II Modify Authentication Process (2)	Network Share Discovery	Taint Shared Content	Data from Local System	Fallback Channels	II Exfiltration Over Web Service (2)	II Endpoint Denial of Service (4)
II Valid Accounts (3)	II User Execution (2)	II Event Triggered Execution (3)	II Hijack Execution Flow (1)	II Impair Defenses (5)	II Multi-Factor Authentication Interception	Network Sniffing		Data from Network Shared Drive	Ingress Tool Transfer	II Scheduled Transfer	Firmware Corruption
		External Remote Services	II Process Injection (3)	II Indicator Removal (7)	II Multi-Factor Authentication Request Generation	Password Policy Discovery		Data from Removable Media	Multi-Stage Channels		Inhibit System Recovery
		II Hijack Execution Flow (1)	II Process Injection (3)	II Masquerading (5)	II Network Sniffing	Peripheral Device Discovery		II Data Staged (2)	Non-Application Layer Protocol		II Network Denial of Service (2)
		II Modify Authentication Process (2)	II Scheduled Task/Job (3)	II Modify Authentication Process (2)	II OS Credential Dumping (2)	II Permission Groups Discovery (2)		II Email Collection (1)	Non-Standard Port		Resource Hijacking
		II Pre-OS Boot (2)	II Valid Accounts (3)	II Obfuscated Files or Information (8)	II Pre-OS Boot (2)	Process Discovery		II Input Capture (3)	Protocol Tunneling		Service Stop
		II Scheduled		II Process Injection (3)	II Process Injection (3)	Remote System Discovery		Screen Capture	II Proxy (4)		System Shutdown/Reboot
				Reflective Code Loading	II Steal or Forge Authentication Certificates	II Software Discovery (1)			Remote Access Software		
						System Information Discovery					
						II System Location Discovery (1)					

Mitigation Process

- Identity and Access Management
- Endpoint monitoring
 - Log collection and storing
 - Continuous log monitoring
 - Threat hunting
- Manage and respond
- Vulnerability Assessment
- Up to date knowledge of vulnerabilities
- Use of open source intelligence
- Incidence response
- Audit and compliance
- Enforce security best-practices
- Behavioral analytics (AI/ML techniques)



Invite all to visit our booth: Vajra



Thank you!