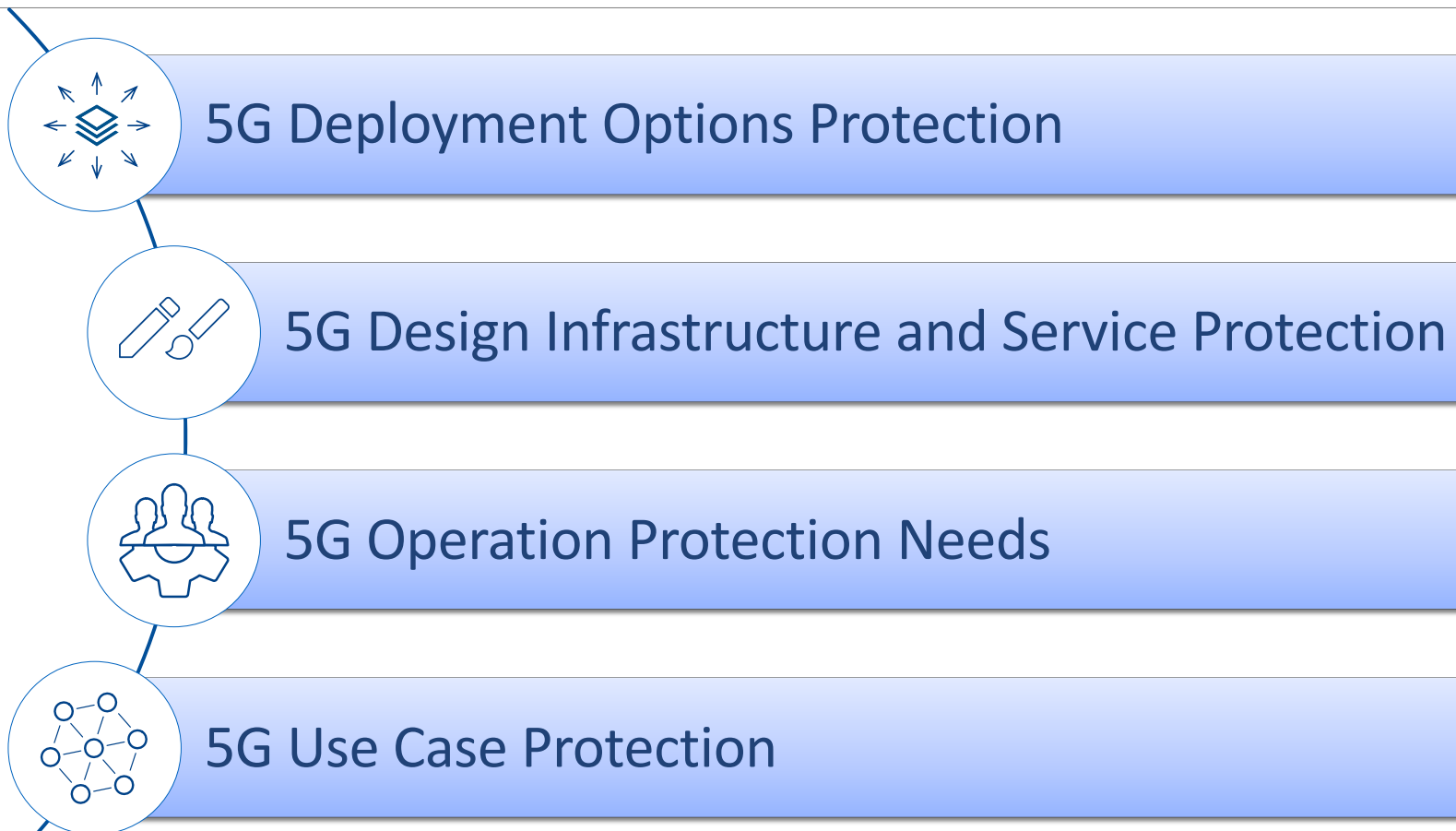# 5G Security Deployment and Operations

Dr. Stan Wong
Assistant Vice President
Email: stan.ws.wong@pccw.com

HKPC Information Security Summit
9 – 10th Mar 2021

Agenda

5G Deployment Options Protection

5G Design Infrastructure and Service Protection

5G Operation Protection Needs

5G Use Case Protection

Operation Knowledge Gap

Telecommunication Knowledge Requirement More and More
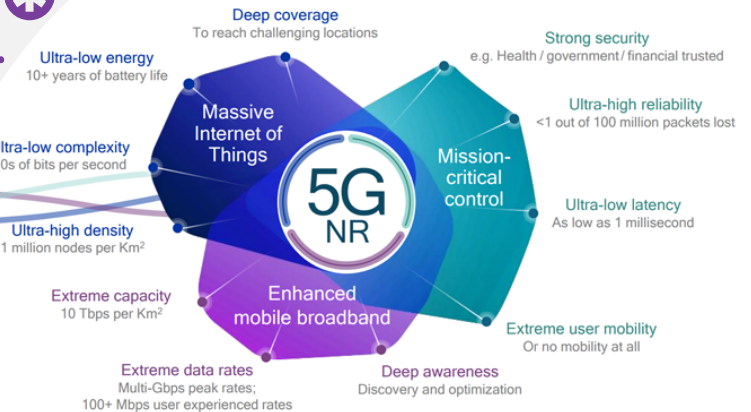
5G

Virtualisation
containerisation
softwarisation

4G
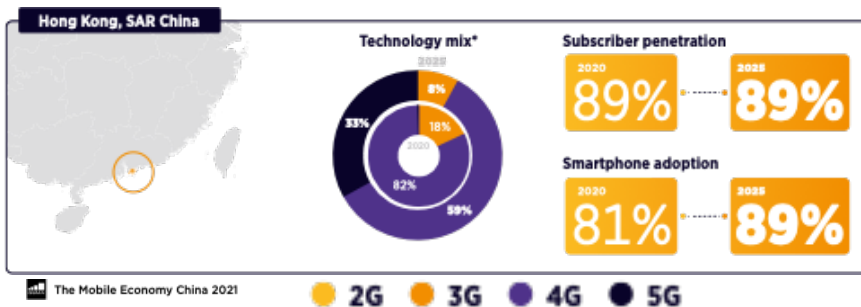
Attack surface is wider

3G

Attack vector is more

2G

Telecommunication Engineer also require to have Information technology knowledge

Deep coverage
To reach challenging locations

Strong security
e.g. Health / government / financial trusted

Ultra-low energy
10+ years of battery life

Ultra-high reliability
<1 out of 100 million packets lost

Ultra-low complexity
10s of bits per second

Massive Internet of Things

Mission-critical control

Ultra-low latency
As low as 1 millisecond

Ultra-high density
1 million nodes per Km^2

5G NR

Extreme capacity
10 Tbps per Km^2

Enhanced mobile broadband

Extreme user mobility
Or no mobility at all

Extreme data rates
Multi-Gbps peak rates;
100+ Mbps user experienced rates

Deep awareness
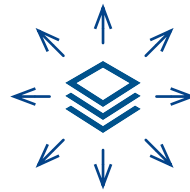Discovery and optimization

SS7

Signalling System No. 7 (SS7) designed in 1975

The legacy technologies and protocols would be targeted as the initial attacks

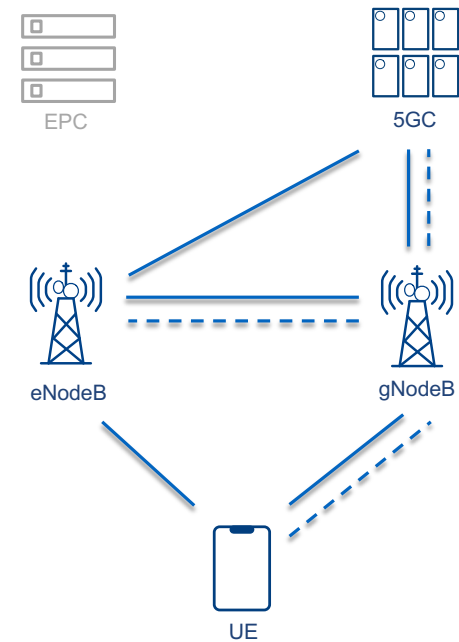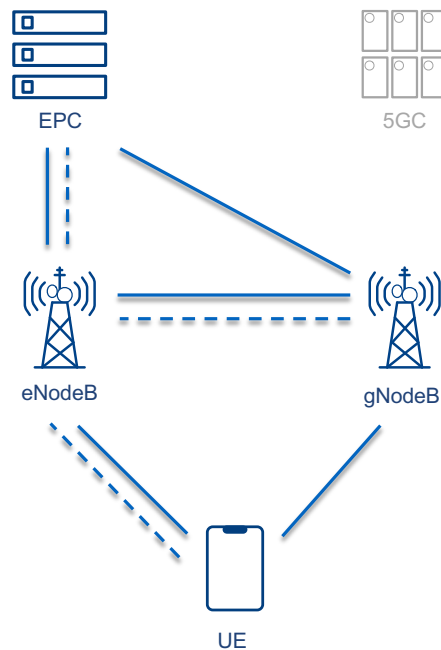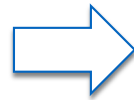There are at least 4bn subscribers worldwide & 70% of firms rely on the SS7 network

Hong Kong, SAR China

Technology mix*

Subscriber penetration
2020 **89%** ···· 2025 **89%**

Smartphone adoption
2020 **81%** ···· 2025 **89%**

The Mobile Economy China 2021

● 2G ● 3G ● 4G ● 5G

HKT Here To Serve

Deploy 5G

5G Deployment Options

Option 1, 4G LTE

Option 3 5G Non-standalone

Option 4, 5G Standalone

EPC

EPC

5GC

EPC

5GC

eNodeB

eNodeB

gNodeB

eNodeB

gNodeB

UE

UE

UE

5GC: 5G Core
EPC: Evolved Packet Core
LTE: Long Term Evolution
UE: User Equipment

User Plane
Control Plane

HKT Here To Serve

a PCCW Group member

5G Deployment Option 3

☑️ **Option 3 5G Non-standalone**

EPC

5GC

eNodeB

gNodeB

UE
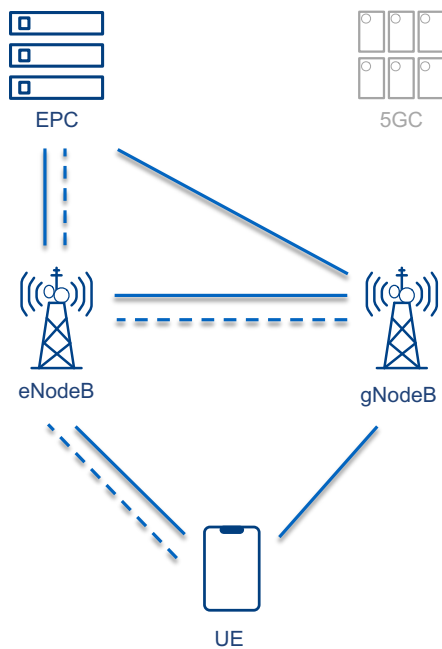
💬 **4G Authentication and Key Agreement**

No Integrity Protection on User Plane 🧩

USIM / AuC

K

UE / HSS

CK / IK

K_{ASME}

UE / MME

K_{NASenc} K_{NASint}

$K_{eNB, NH}$

UE / eNB

K_{UPint} K_{UPenc} K_{RRCint} K_{RRCenc}
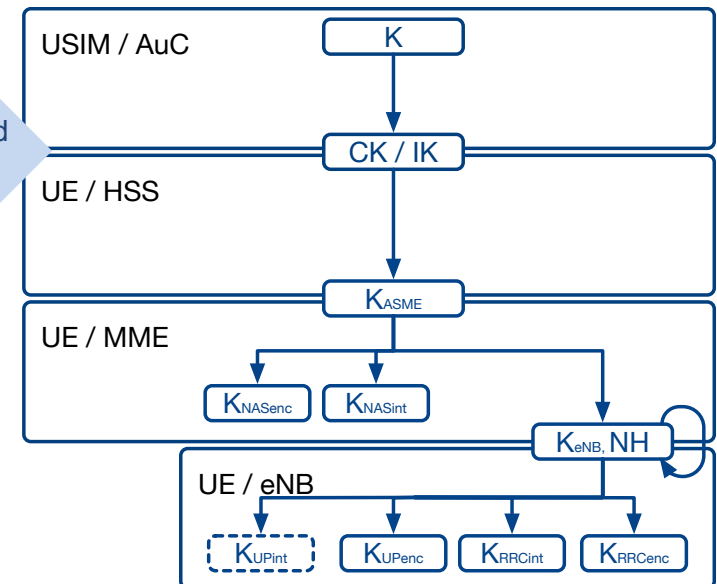
5G Deployment Option 4

☑ ☐☐ **Option 4, 5G Standalone**
◉ ☐

EPC

5GC

eNodeB

gNodeB

UE
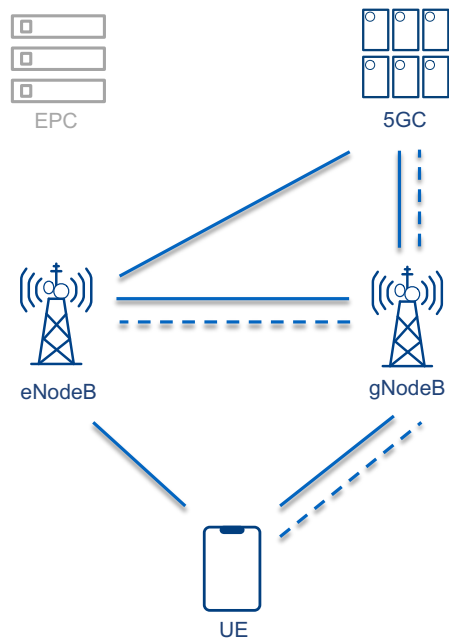
5G Authentication and Key Agreement

User Plane Integrity Protected

HPLMN

Serving Network

HKT Here To Serve

5GC: 5G Core
EPC: Evolved Packet Core
LTE: Long Term Evolution
UE: User Equipment

—— User Plane
- - - Control Plane

a **PCCW** Group member
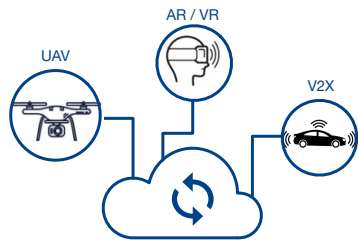
HKT Here To Serve
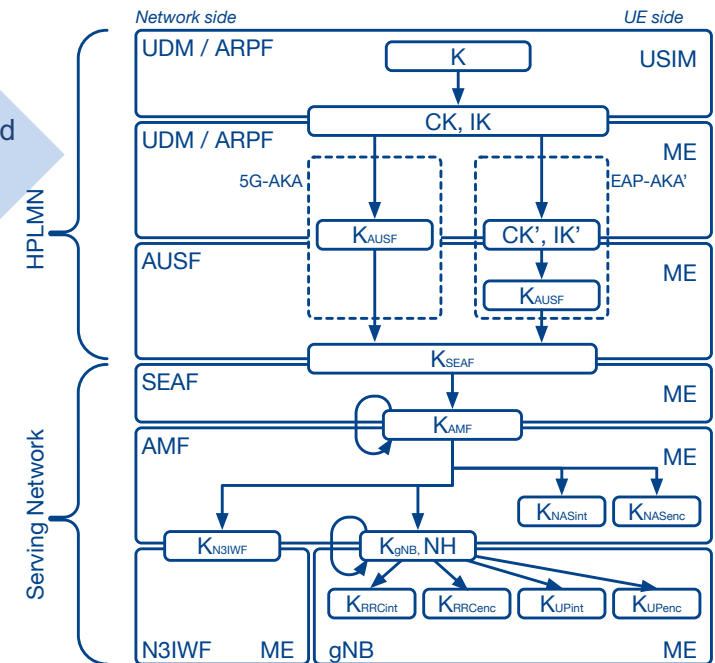
Design 5G

5G Standalone Services

The 5G innovation also include the following technologies and services ownership
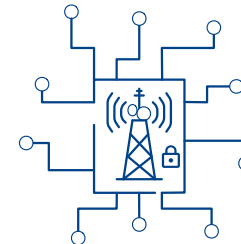

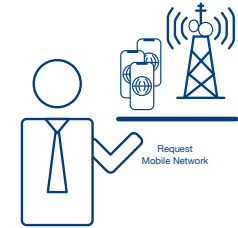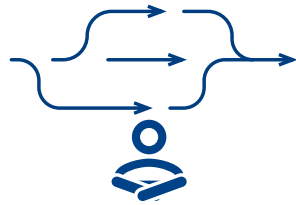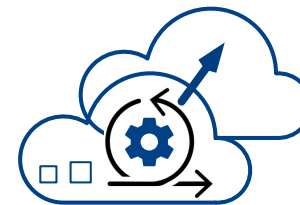Tactile Internet   Multi-Access Edge Computing   Network Slicing   Non-public Network   Mobile Network On-demand

Network Infrastructure Flexibility   Enterprise Network Service Agility
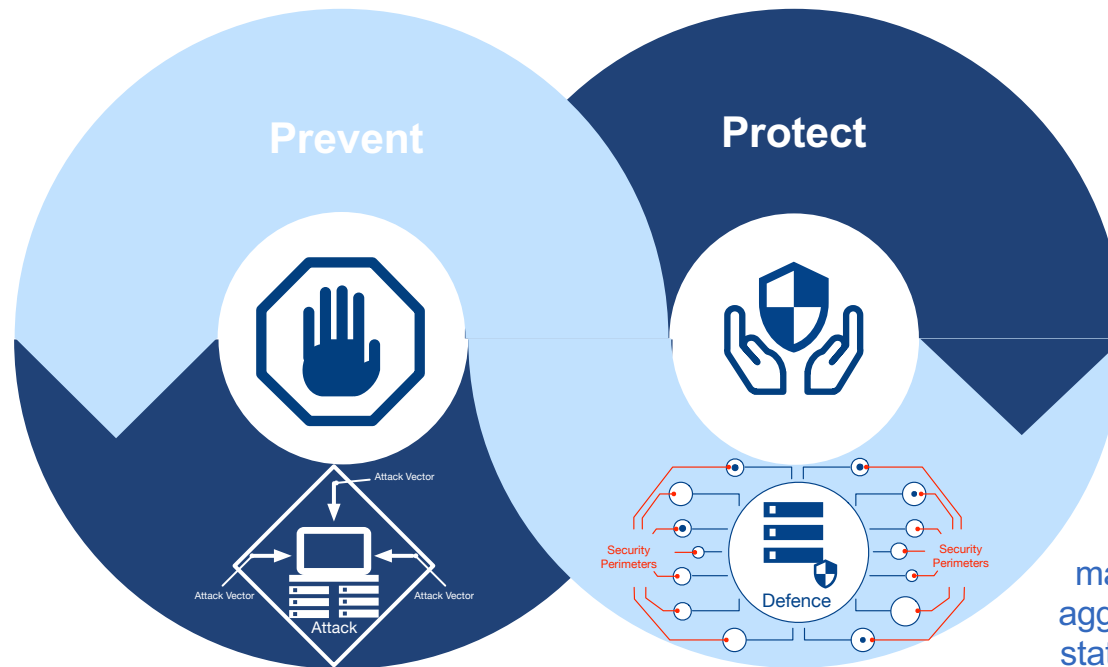
With 5G Network Infrastructure Flexibility and Enterprise Network Service Agility,
would gain the market competence, and velocity of services delivery.

4G LTE

LTE infrastructure is a closed network, traditional firewall and perimeter defence could resolve most of attacks.

Prevent

Protect

4G LTE is to **protect** subscribers and network elements

4G LTE is to **prevent** impersonation and eavesdropping

5G

macro to micro management, aggregation to disaggregation, static physical infrastructure to flexible and elastic infrastructure.

5G is to **protect** subscribers, tenants, resources (virtual and physical) and tenant's subscribers

5G is to **prevent** other to affect the service availability

Attack Vector

Attack Vector

Attack Vector

Attack

Security Perimeters

Security Perimeters

Defence

5G Infrastructure Security by Design

Standard Development Organisation (SDO) methodologies:
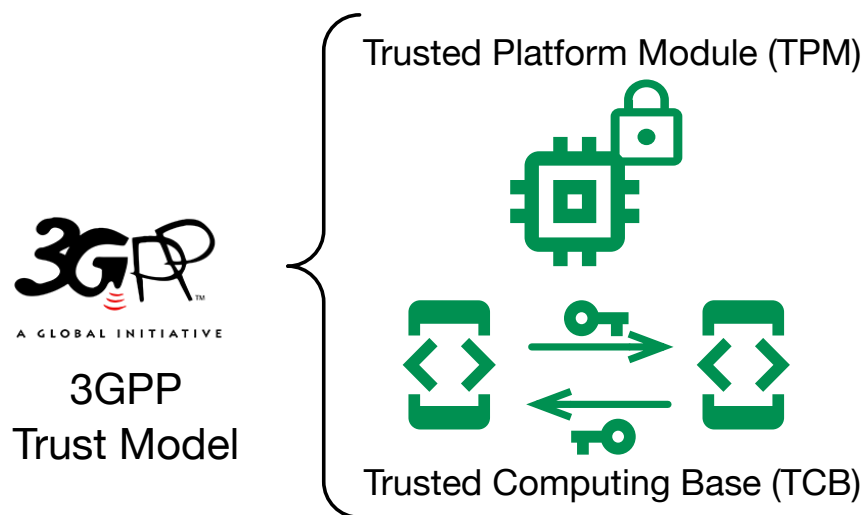
Protocol Interaction System Design:

Trusted Platform Module (TPM)

3GPP
Trust Model

Trusted Computing Base (TCB)

Protocol reinforces the interaction behaviour
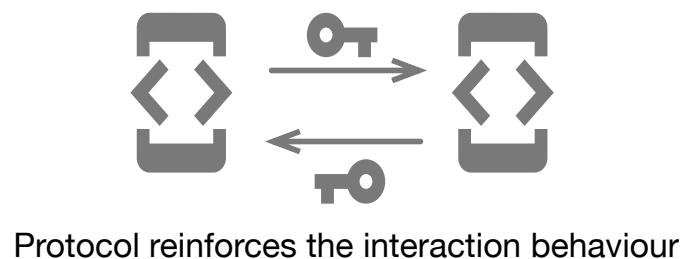
Virtualisation, Containerisation and Softwarisation

5G infrastructure and services protection must be started from application to every network segment.

Application Protection

Same application might belong to different tenants that could exist in the same physical machine, virtual machine or under a kernel.

VM & Container Protection

Side-Channel Attack could attack from one VM to other via CPU or Hypervisor.

Virtual Resource

Physical Network Function Protection

The hardware and software supply chain would affect multi-dimensional issues

Software-defined Network Protection
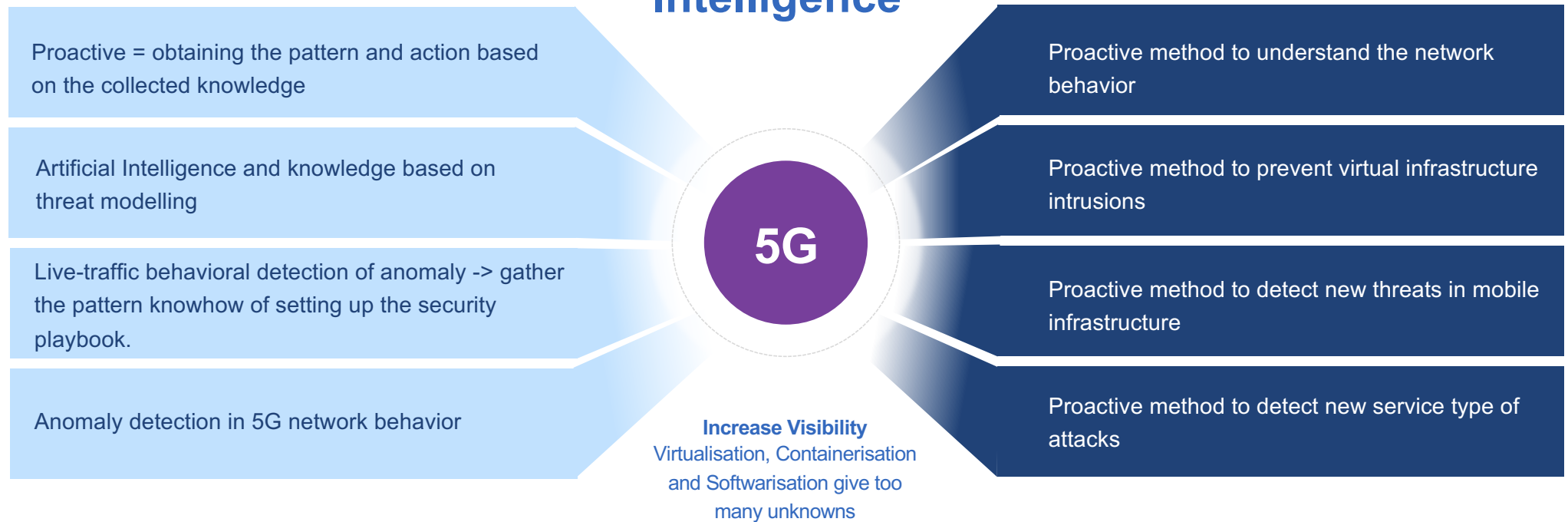
A single point of failure and virtual switch attacked by side-channel attack from one virtual port to another, or from one controller to another.

Threat Intelligence

Proactive = obtaining the pattern and action based on the collected knowledge

Artificial Intelligence and knowledge based on threat modelling

Live-traffic behavioral detection of anomaly -> gather the pattern knowhow of setting up the security playbook.

Anomaly detection in 5G network behavior

5G

Increase Visibility
Virtualisation, Containerisation and Softwarisation give too many unknowns

Proactive method to understand the network behavior

Proactive method to prevent virtual infrastructure intrusions

Proactive method to detect new threats in mobile infrastructure

Proactive method to detect new service type of attacks

5G Use Cases

Hospital IoMT Scenario

IoMT

5G NR

Wi-Fi

Machine Learning Edge Computing

5G Core Network

5G SA and Wi-Fi Convergence Core

Elasticity on increasing the compute resource

Configuration

Automation

Policies

Application

Management

Theatre or Concert Scenario

360 Video Streaming

5G NR

Wi-Fi

5G Core Network

5G SA and Wi-Fi Convergence Core

Elasticity on increasing the network bandwidth resource

Home Network VR Scenario

Wireless Virtual Reality

5G NR

Wi-Fi

5G Core Network

5G SA and Wi-Fi Convergence Core

Elasticity on increasing the rendering resource

HKT Here To Serve

Thank you!

Dr. Stan Wong

Assistant Vice President

Strategic Planning and Design

HKT Limited

Mobile: +85297746660

Email: stan.ws.wong@pccw.com

jedistan@gmail.com

jedistan@mac.com

HKT Here To Serve