SecOre

APPROACHES AND SOLUTIONS TO SECURE 5G

JUL 2020

5G takes cybersecurity to a new level. With anti-tracking and spoofing features, criminals will find it difficult to manipulate connections associated with individual devices. With network slicing, the system gets sliced into various slices with each slice affording custom protections for specific devices and configurations. Beyond this, operators will have to deal with many other specific issues that stem from the use of legacy technologies,

Hackers and attackers are getting bolder and more persistent. Telecom companies are frequently at the receiving end as they own and operate critical infrastructure and are providing connectivity to agencies that manage critical infrastructure in entirety or parts of it. They also operate infrastructure used to communicate and store sensitive data belonging to customers, small and large businesses, and governments.

EVOLUTION

5G's stronger network encryption and user verification represent a significant leap from that offered by 4G. With download speeds hitting 10X faster than everything we are seeing today with 4G, the opportunities in fields like Industrial IoT and autonomous vehicles are immense. These speeds will enable the widespread adoption of industrial IoT, employee safety and, streamlining of workflows, and development of advanced features.

5G speeds will range from ~50 Mbit/s to over 2 Gbit/s at the start. The fastest 5G, known as mmWave, delivers speeds of up to and over 2 Gbit/s. 5G also claims to boost spectral efficiency and improved connection density. For use cases where the demand is for extremely low latency, the latency could be as low as 1 millisecond. This opens a whole new world of use cases.

MARKET POTENTIAL

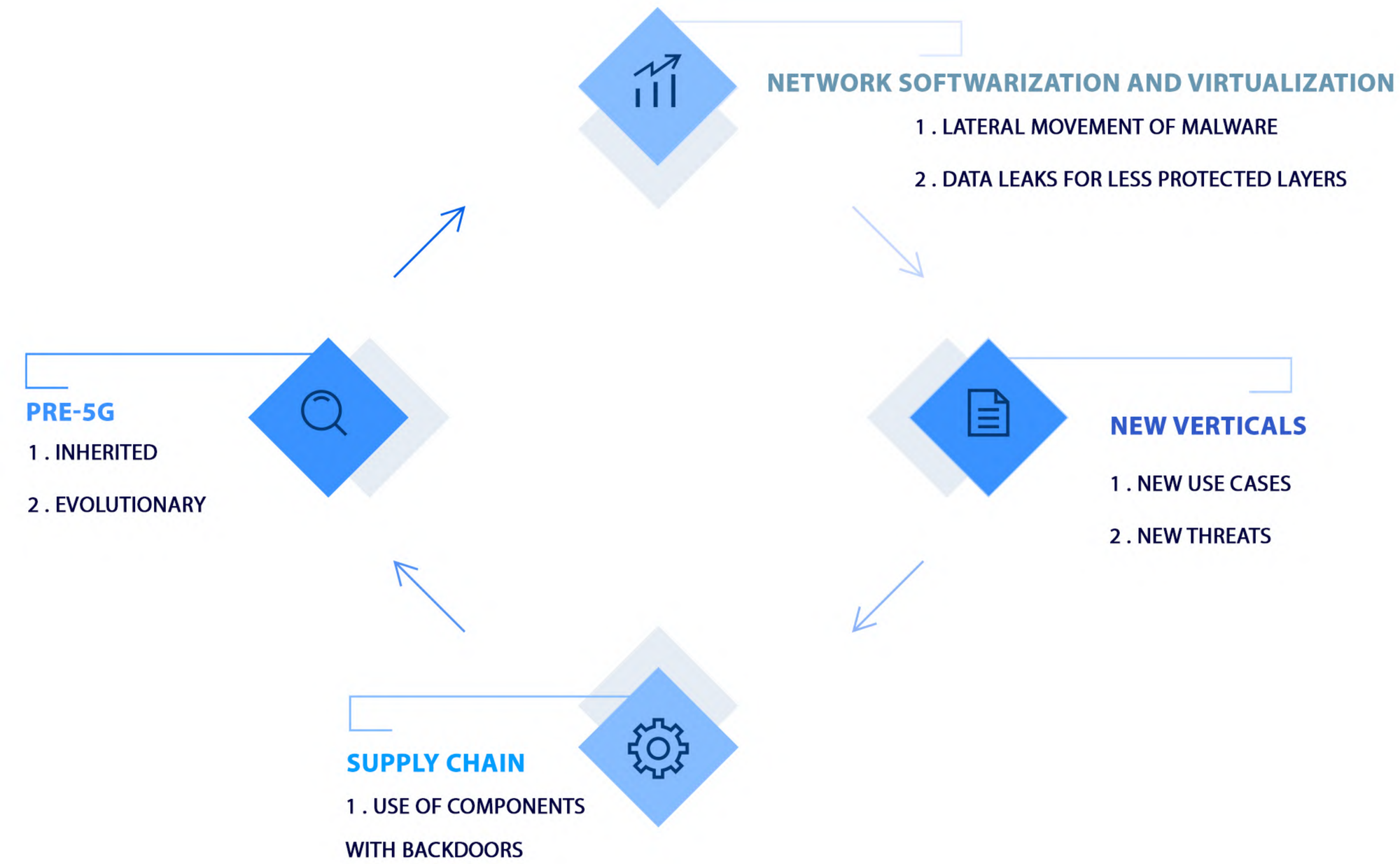
At the core of 5G lies network slicing which is the capability to amend a set of functions to improve network utilization for each use case. At the business end, slicing combines all network resources, assets, functions, and other aspects needed to cater to a specific bouquet of services or devices or business case. Network slicing helps operators customize their network resources and release them to enterprises who control them (B2B) or the operators release them to an intermediary like an MVNO who engages with an end-user (B2B2C).

5G SECURITY CHALLENGES

The switch to 5G presents users and vendors many opportunities to enhance security and deploy a better user experience. But it could also result in the emergence of new challenges surrounding supply chains, deployment, and, network security. Reliance on untrusted entities, integration with existing networks, design issues, vulnerabilities from previous generations are all sources of vulnerabilities that have been identified. Mass adoption will expose other vulnerabilities.

Most security researchers agree that 5G poses an elevated security threat mainly because there are more vectors available for adversarial entities to use for an attack. 5G will be deployed extensively to enable connected devices to function at large scales. Also, because of the complex use cases that come to the fore, such as connected cars, Industry 4.0 or IIoT, industry-specific requirements will arise.

On the other side of the spectrum, 5G will bring ICT constituents and data management to the edge. This is a significant development that will lead to enhanced security due to device management, authentication functions, edge computing power, network slicing, and localized detection and response to threats. This will add another layer of protection for the core networks while increasing network management capabilities and computing power.



UNDERSTANDING THE ISSUES WITHIN EACH CATEGORY

PRE 5G SECURITY ISSUES	SECURITY IMPACT OF NETWORK SOFTWARIZATION	SECURITY ISSUES RELATED TO NEW VERTICALS
Multi-mode attacks – DDoS, Botnet, hackers	The open architecture makes it more attractive to hackers	Each vertical comes with its own vulnerabilities
Attacks at the physical level such as jamming, cloning interference, snooping,	No implicit security due to the lack of understanding of issues	Most verticals have high-end uses that attract hackers of all hues
Roaming and IP hijacking	Software-based systems are easy to hack than their hardware-based counterparts	Since the focus will be on ensuring end uses, security can sometimes take a backseat
Man-in-the-middle with a fake base station	No perimeter security or physical security due to virtualization	Security issues are not fully understood
Data and location leaks through IMSI catcher leading to privacy issues	Fast deployment of a virtualized element withomit proper security testing	Espionage interest from APT hackers will be a major concern
Attacks via non-3GPP networks		

UNDERSTANDING THE ISSUES WITHIN EACH CATEGORY

The explosion in new use cases alone is enough to increase the risks associated with 5G. However, if increased emphasis is paid to understanding these and other risks and in addressing them, 5G adoption will be a much smoother and faster affair. The inherent complexity in securing 5G itself is a big factor that limits our ability to understand these risks and this factor presents a significant barrier to cross.

As with every other new technology, the 5G security risks can be divided into known knowns, known unknowns, and unknown unknowns.

RISK TYPE	EXAMPLE
KNOWN KNOWNS	Risks inherited from previous generations; risks arising from complexity
KNOWN UNKNOWNS	Risks posed by new use cases
UNKNOWN UNKNOWNS	

In addition to these, there are also security challenges that arise from network slicing. Since each slice caters to different types of services across verticals and use cases, each comes with a different level of security and privacy policies. Thus, the security and privacy protocols evolved to meet the needs of each slice will have an impact not just on that slice but also on other slices and the network system as a whole (while being focused on that slice).

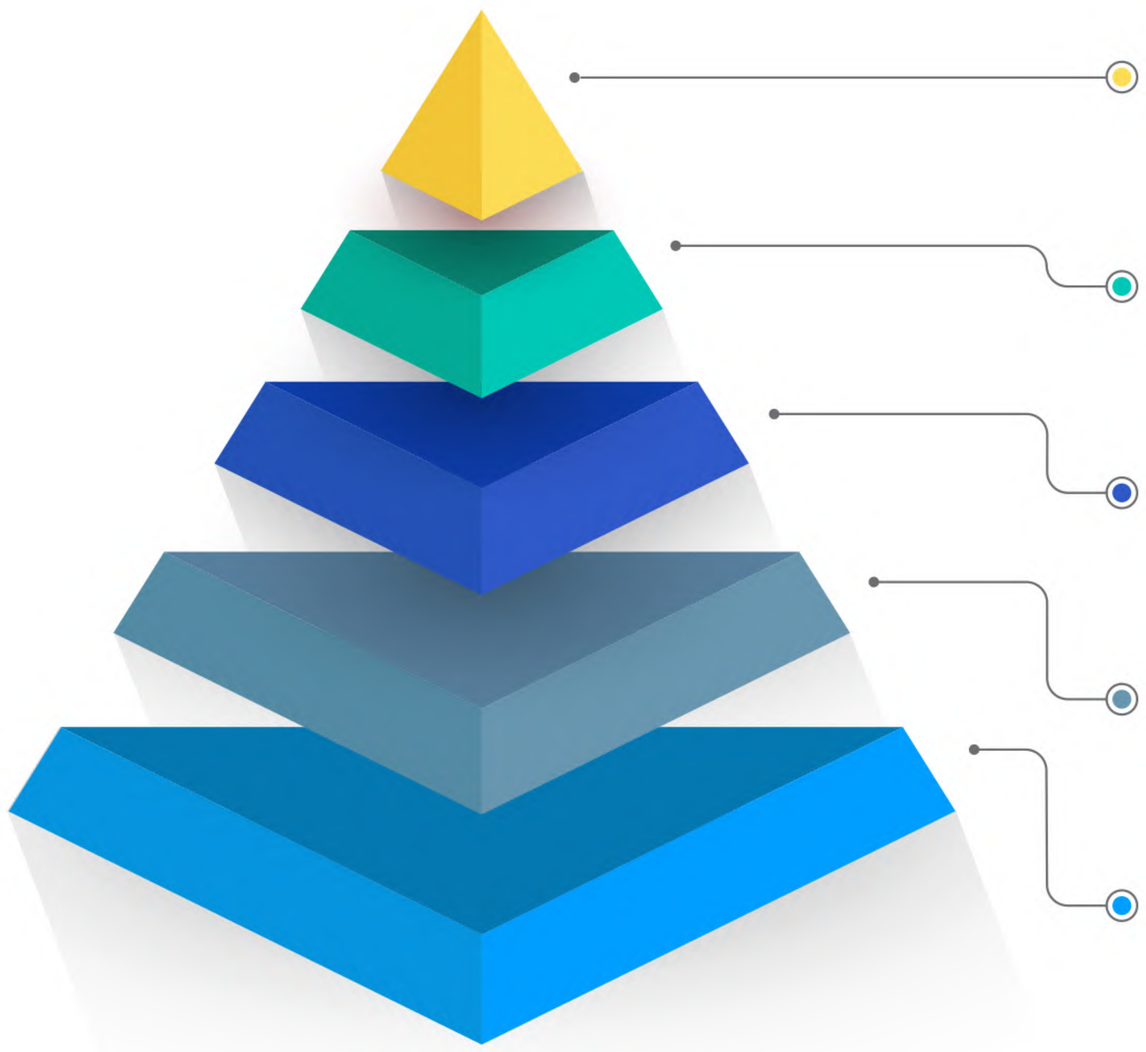
While keeping the above in mind, imagine a network slicing implemented in multi-domain infrastructures. The complexity that arises from this implementation will be inherently daunting. To address this challenge, security policies and efficient coordination mechanisms spanning various administrative domain infrastructures in 5G systems must be designed and developed. This requirement should not be left to the forces of evolution to materialize. Instead, a concerted effort must be made in every implementation.

RISK CATEGORIES AND SCENARIOS

RISK TYPE	EXAMPLE
RISK CATEGORIES AND SCENARIOS	R1-Misconfiguration of networks R2-Lack of access controls
RELATED TO 5G SUPPLY CHAIN	R3-Low product quality R4-Dependency on any single supplier within individual networks or lack of diversity on a nation-wide basis
RELATED TO MODUS OPERANDI OF MAIN THREAT ACTORS	R5- State interference through 5G supply chain R6- Exploitation of 5G networks by organized crime or organized crime group targeting end-users
RELATED TO INTERDEPENDENCIES BETWEEN 5G NETWORKS AND OTHER CRITICAL SYSTEMS	R7- Significant disruption of critical infrastructures or services R8-Massive failure of networks due to interruption of electricity supply or other support systems
RELATED TO END-USER DEVICES	R9-Exploitation of IoT (Internet of Things), handsets or smart devices

(SOURCE: THE EU COORDINATED RISK ASSESSMENT REPORT)

STRATEGIES TO SECURE 5G



SECURE DEVICES

in addition to regular patching, use test environments to understand threats and vulnerabilities, and analyze patches and updates; avoid outdated firmware, hardware, and operating systems. Run formal vulnerability and patch management programs.

SECURE SLICES

at every level, anomalous activity should be detected, contained, and mitigated. Lateral movement of malware should be prevented completely.

MONITOR TRAFFIC

traffic should be studied and analyzed to develop models and predictions to isolate instances of malicious communication attempts from within or outside the networks\slices.

DEVICE DISCOVERY

device profiles and architectures should be signatories in detail to prevent rogue devices from accessing networks or slices.

ATTACK DEFLECTION

create infrastructure decoys that attract attacks while the actual infrastructure is protected.

Address policy violations immediately without delay. Devices that violate policies should be isolated and denied access at the earliest.

Deploy security by design at all levels

TALK TO SUBEX

Subex is securing 5G across multiple sites globally. Our approach to 5G security covers solutions to counter inherent and evolving threat paradigms in addition to malware. Our 5G security use cases span protection from:

- Botnets
- Brute force attacks
- Unassigned Software updates
- Certificate Misuse
- Malware
- Policy Violations
- Ransomware
- Internal Compromises
- Denial of Service
- Backdoor attacks
- Certificate Repudiation
- DDoS
- Modbus/SCADA attacks

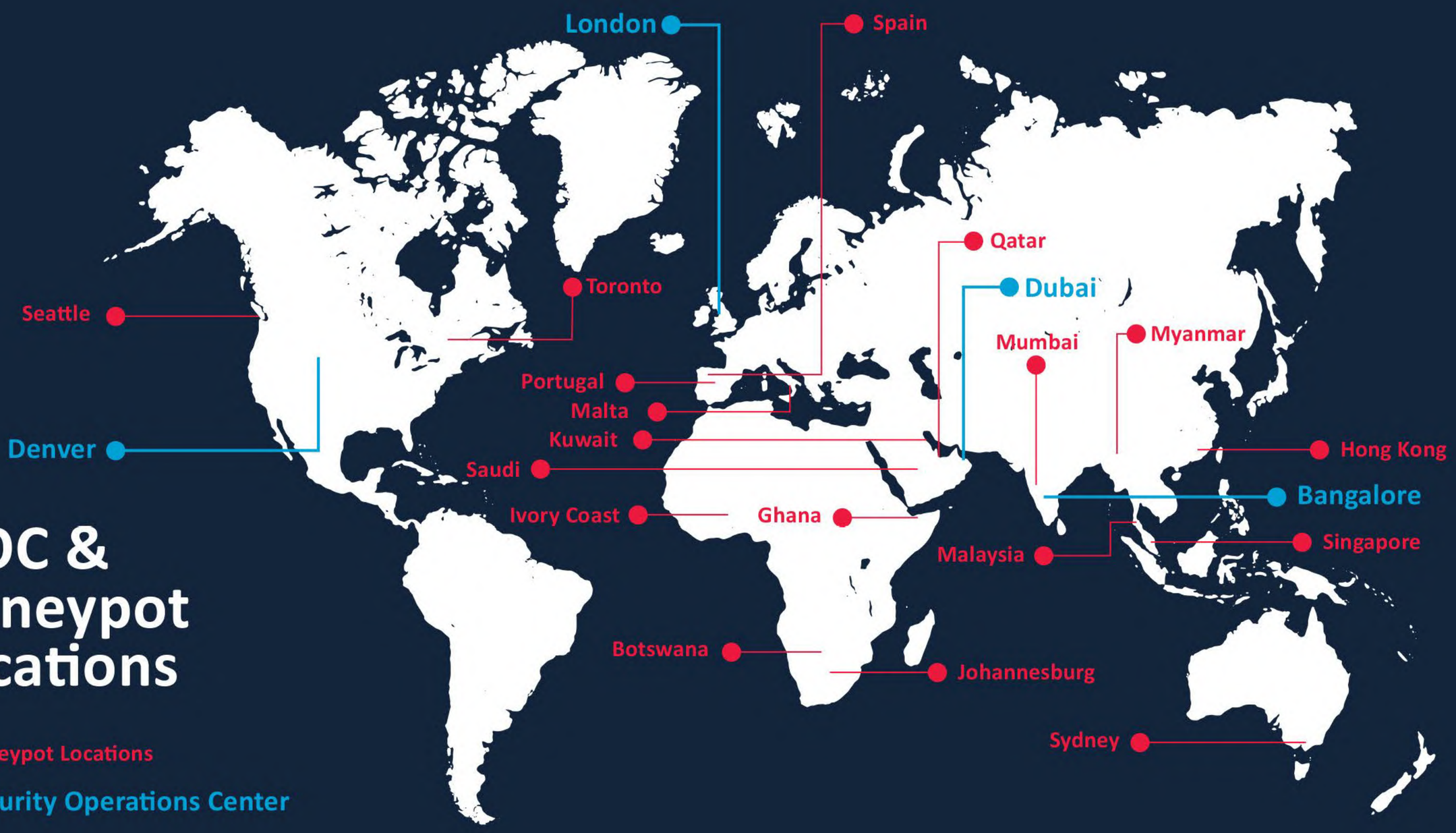
FRAUD PREVENTION

- Spoofing
- Arbitrage (PBX - CLI Refiling)
- Robo Calling
- IRFS
- Wangiri
- Misuse eSIM Subscriber Data

These are some of the use cases to learn more about our 5G security offerings, drop us a line at info@subex.com. Don't forget to mention #5gisec to qualify for a special conversation.

SUBEX

www.subex.com



ISOC & Honeypot Locations

- Honeypot Locations
- Security Operations Center

- Subex is the market leader in products Security and Fraud Management market, with over 180+ customers in total
- Awarded Pipeline Award at Nice 2016 for most innovative Security and Assurance Solution for IoT Security
- Subex is the Number 1 provider globally of Fraud Management and Security solutions in the Telecom Space, according to a Gartner report published in March 2016
- Subex runs the world's most comprehensive IoT and ICS focused honeypots of over 400 architectures in 32 locations around the world.
- +300 Installations around the world
- +700 Experts in Security/Fraud and other programs with assets, skills and innovative methods to ensure results for the operator
- Publicly listed in the National Stock Exchange (India) and Bombay Stock Exchange

Subex Limited

RMZ Ecoworld,
Devarabisanahalli,
Outer Ring Road,
Bangalore - 560103 India

Tel: +91 80 6659 8700
Fax: +91 80 6696 3333

Subex, Inc

12303 Airport Way,
Bldg. 1, Ste. 390,
Broomfield, CO 80021

Tel : +1 303 301 6200
Fax : +1 303 301 6201

Subex (UK) Ltd

1st Floor, Rama
17 St Ann's Road,
Harrow, Middlesex,
HA1 1JU

Tel: +44 0207 8265300
Fax: +44 0207 8265352

Subex (Asia Pacific) Pte. Limited

175A, Bencoolen Street,
#08-03 Burlington Square,
Singapore 189650

Tel: +65 6338 1218
Fax: +65 6338 1216

For more information write to info@subex.com

Regional offices: Dubai | Ipswich