



## *Expert Meeting on Strengthening Security and Interoperability along Euro-Asian Inland Transport Corridors*

*Johnathan Partouche, Tbilisi 12.12.2019*



# BEYOND THE KNOWN THREATS



# UNECE

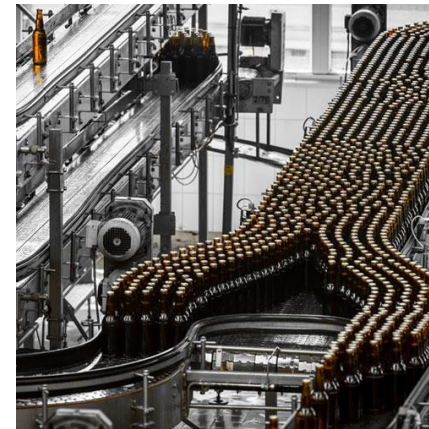


Organization for Security and  
Co-operation in Europe

# OUR MISSION



- Secure and optimize the industrial control & IT networks that run the world.





UNFORTUNATELY, WE ARE NOT THERE YET!!!



# SOME VICTIMS OF CYBER ATTACKS



## Cyber-attack on ports in Asia Pacific Economic effects

Economic loss

**\$110bn**

Covered by insurance

**8%**

[lloyds.com/shenattack](http://lloyds.com/shenattack)

#ShenAttack

#CyRim

## Malicious Email Per User by Industry (per year)

Industry	Users Targeted (%)
Mining	38.4%
Wholesale Trade	36.6%
Construction	26.6%
Non-classifiable Establishments	21.2%
Retail Trade	21.2%
Agriculture, Forestry & Fishing	21.1%
Manufacturing	20.6%
Public Administration	20.2%
Transportation & Public Utilities	20.0%
Services	11.7%
Finance, Insurance & Real Estate	11.6%



95% of enterprise-network attacks are a result of a spear-phishing campaign

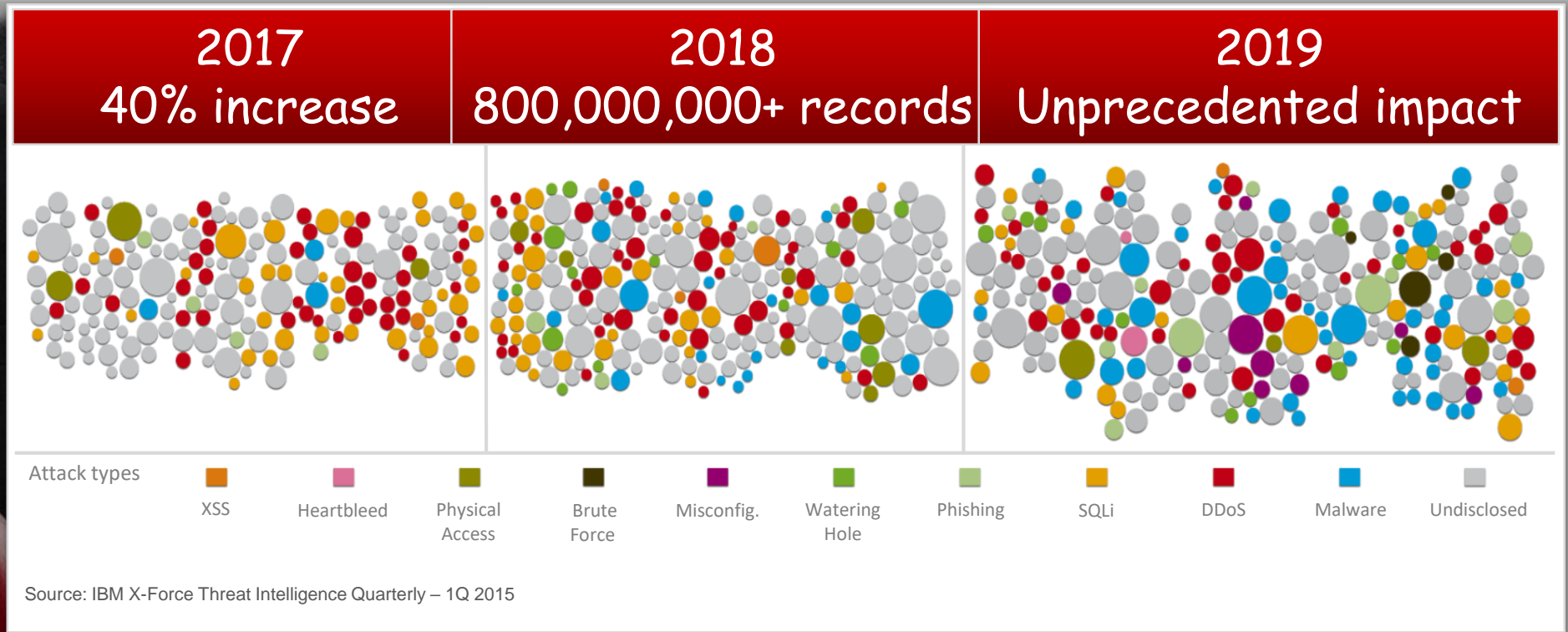
(Network World, citing Alan Paller, Director of Research at SANS, 2013)



# Conventional safeguards are not working



Organizations  
Need to Speed  
Up Breach  
Detection



# 256 days

average time to detect APTs  
Malicious attacks can take an average of 256 days to identify

# \$3.8M

average cost of a data breach  
Average consolidated total cost of a data breach (benchmark study of 350 companies spanning 11 countries), a 23 percent increase annually since 2013.



# Because new technologies introduce new risks

70%



of security executives have cloud and mobile concerns

*IBM CISO Survey*



614%

Mobile malware growth in just one year

*Juniper Mobile Threat Report*

Traditional security practices are unsustainable

85



security tools from

45



vendors

*IBM client example*

83%



of enterprises have difficulty finding the security skills they need

*ESG Research*

# Cyber threats to increasingly digitalized/automated transport and logistics systems



- Train assets



Signaling Systems



Train Systems and Communications Systems



ATS – Automatic Train Supervision

- Infrastructure



HVAC



Oil Repositories



Mechanical Systems



SCADA Systems and Electric Substations

- Building Management Systems



Smart Building Management Systems



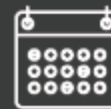
CCTV



Lighting



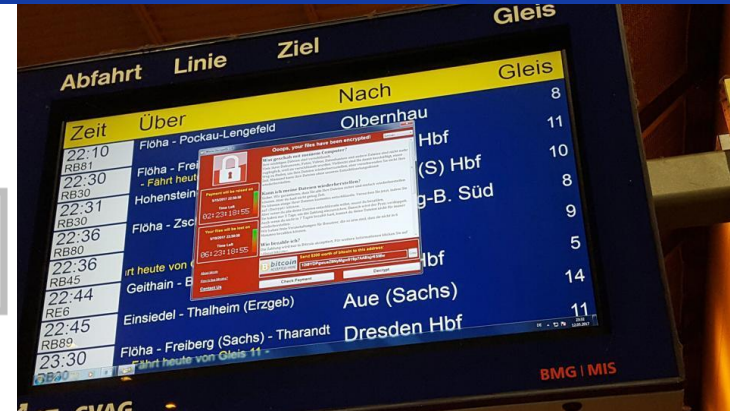
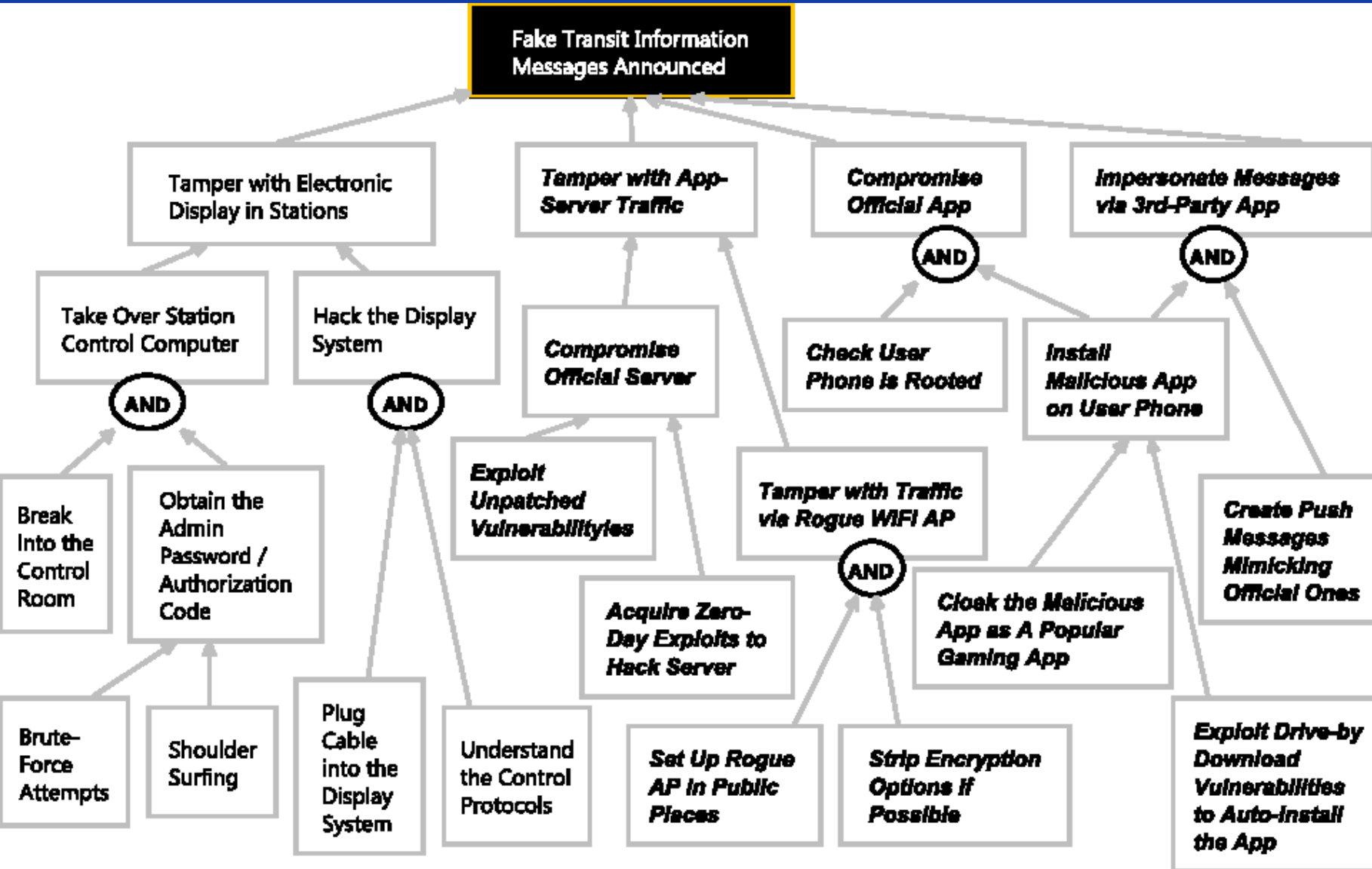
Physical Access Control



Timetable Display



# Damages to economic development, security and stability of States





# Because of those challenges

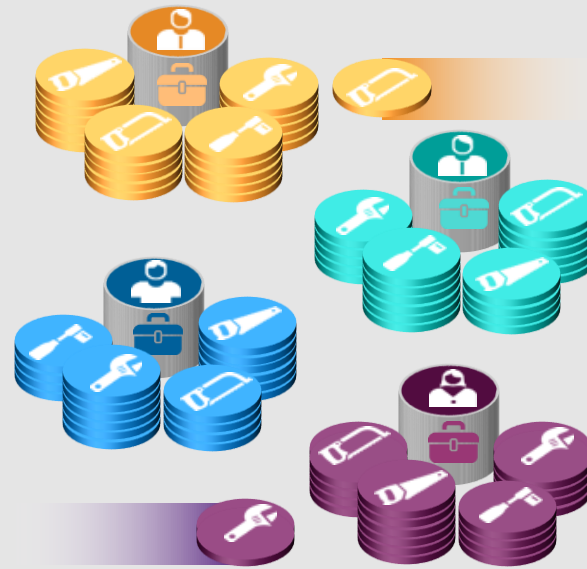


## Escalating Attacks



- Increasingly sophisticated attack methods
- Disappearing perimeters
- Accelerating security breaches

## Increasing Complexity



- Constantly changing infrastructure
- Too many products from multiple vendors; costly to configure and manage
- Inadequate and ineffective tools

## Resource Constraints



- Struggling security teams
- Too much data with limited skills\* & manpower to manage it all
- Managing & monitoring increasing compliance demands

\* Even when security projects are successfully funded, many CISOs encounter roadblocks to implementation, especially when it comes to finding the right skills.



Securing today's transportation infrastructures requires  
a **new approach** & a **new set of capabilities**.



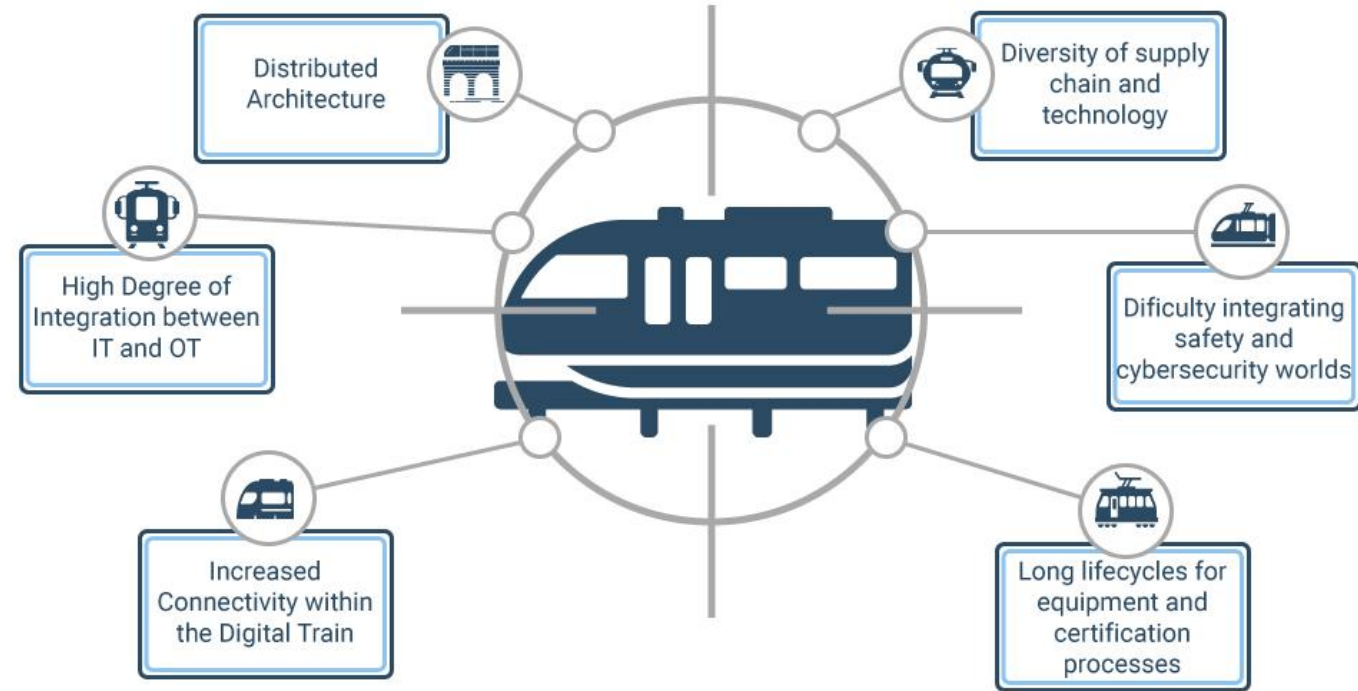


# What should Governments and private sector do to effectively address these challenges?



Societal functions and associated assets

Business functions and associated assets



# Emerging technologies to secure supply chains

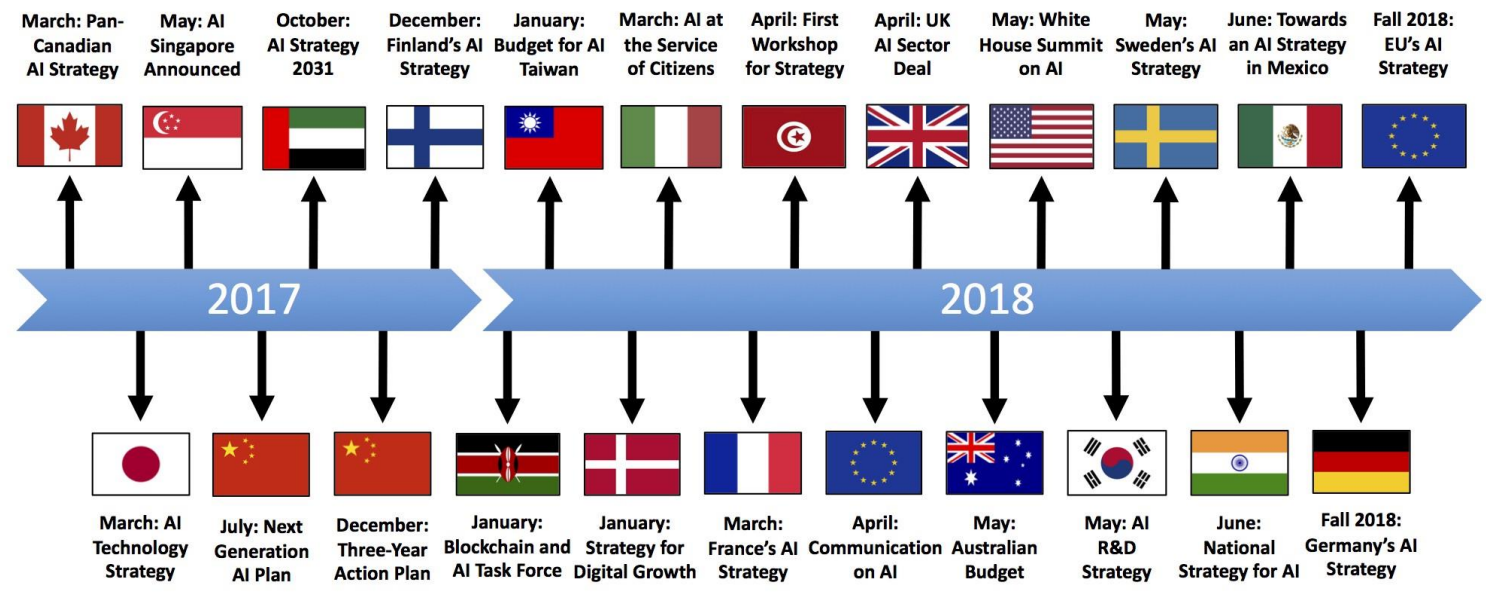


### THE 30 TECHNOLOGIES OF THE NEXT DECADE

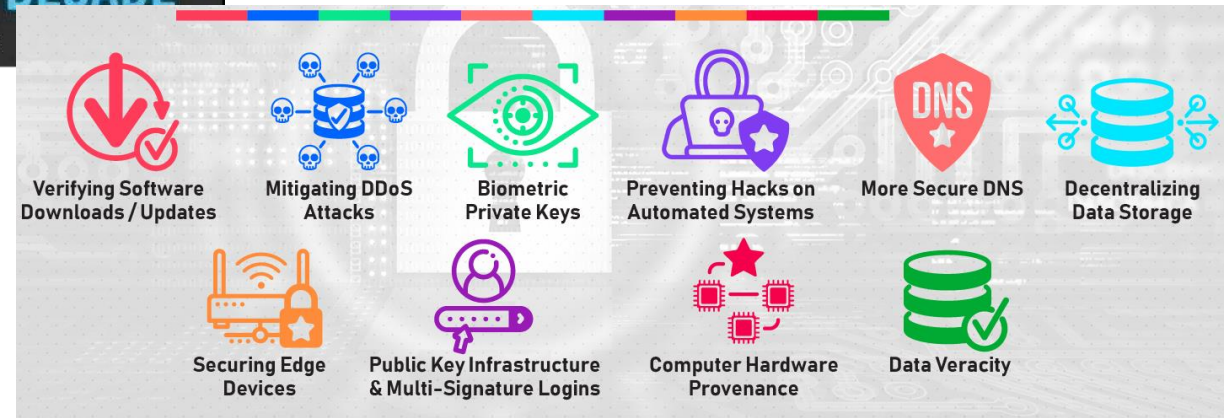
- #1 Artificial Intelligence: AI / Machine Learning / Deep Learning
- #2 Internet of Things: IOT, IIOT, Sensors & Wearables
- #3 Mobile/Social Internet: Advancements - Search/Social/Messaging/Livestreams
- #4 Blockchain: Distributed Ledger Systems, Apps, Infrastructure, Technologies, Cryptocurrencies & DApps
- #5 Big Data: 0101, 1011, 0110. + Predictive Analytics
- #6 Automation: Information, Task, Process, Machine, Decision & Action
- #7 Robots: Cons./Comm./Indus., Robots, Drones & Autonomous Vehicles
- #8 Immersive Media: -VR/ #AR/ #MR/ 360°/ Video?Gaming
- #9 Mobile Technologies: Infrastructure, networks, standards, services & devices
- #10 Cloud Computing: SaaS, IaaS, PaaS & MESH Apps
- #11 3D Printing: Additive Manufacturing & Rapid Prototyping
- #12 CX: Customer Journey, Experience Commerce & Personalization
- #13 EnergyTech: Efficiency, Energy Storage & Decentralized Grid
- #14 Cybersecurity: Security, Intelligence Detection, Remediation & Adaptation
- #15 Voice Assistants: Interfaces, Chatbots & Natural Language Processing
- #16 Nanotechnology: Computing, Medicine, Machines + Smart Dust
- #17 Collaborative Tech: Crowd, Sharing, Workplace & Open Source Platforms & Tools
- #18 Health Tech: Advanced Genomics, Bionics & Health Care Tech.
- #19 Human-Computer Interaction: Facial/Gesture Recognition, Biometrics, Gaze Tracking
- #20 Geo-spatial Tech: GIS, GPS, Mapping & Remote Sensing, Scanning, Navigation
- #21 Advanced Materials: Composites, Alloys, Polymers, Biomimicry, Nanomanufacturing
- #22 New Touch Interfaces: Touch Screens, Haptics, 3D Touch, Paper, Feedback & Exoskeletons
- #23 Wireless Power: Bio-/Enviro-Materials + Solutions, Sustainability, Treatment & Efficiency
- #24 Clean Tech.
- #25 Quantum Computing: + Exascale Computing
- #26 Smart Cities: + Infrastructure & Transport
- #27 Edge/Computing: + Fog Computing
- #28 Faster, Better Internet: Broadband incl. Fiber, 5G, Li-Fi, LPN and LoRa
- #29 Proximity Tech: Beacons, RFID, Wi-Fi, Near-Field Communications & Geofencing
- #30 New Screens: TVs, Digital Signage, OOH, MicroLEDs & Projections

Created by: Sean Moffitt @seanmoffitt, Managing Director, @Wikibrands

## Artificial Intelligence Strategies

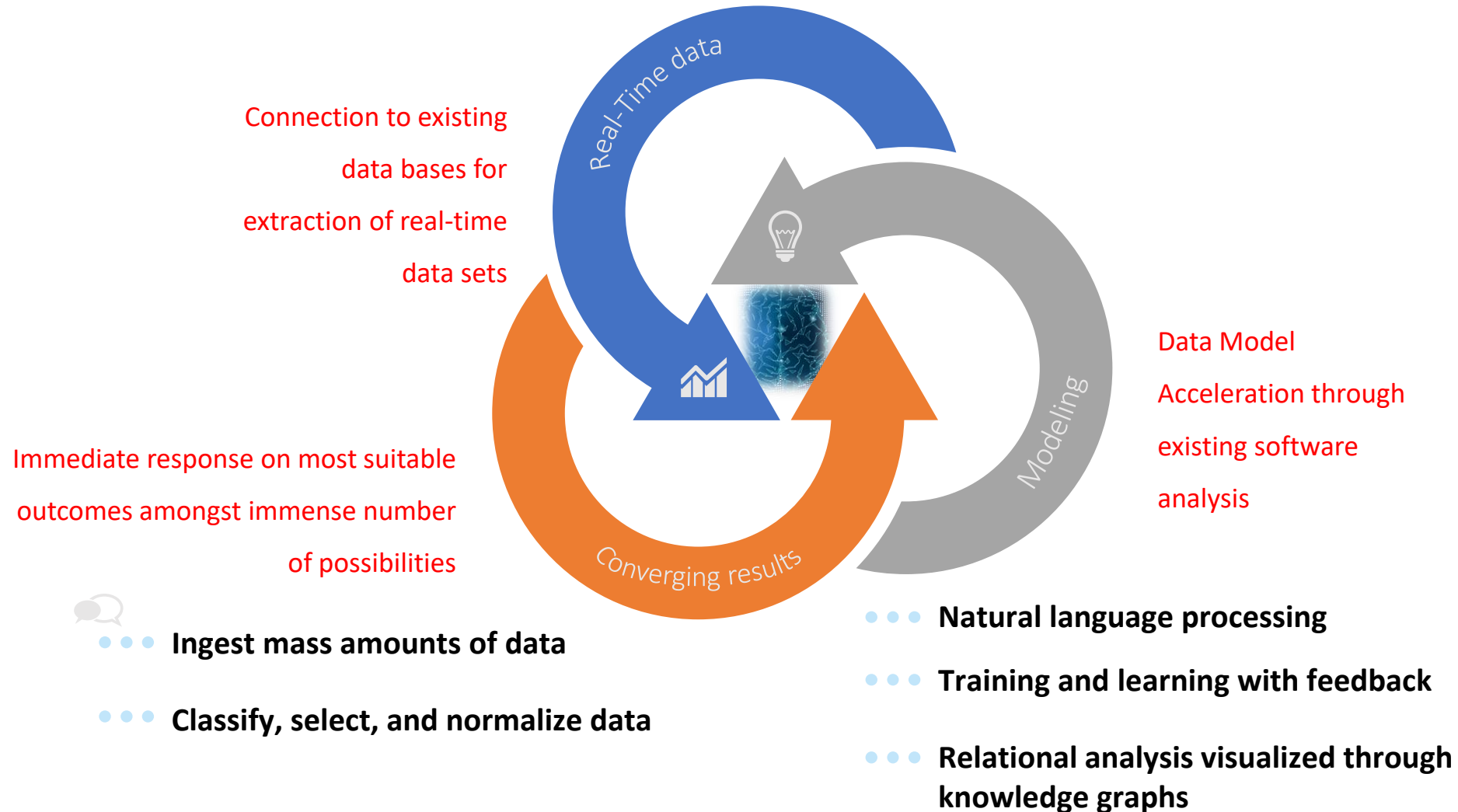


How will blockchain impact cyber security?

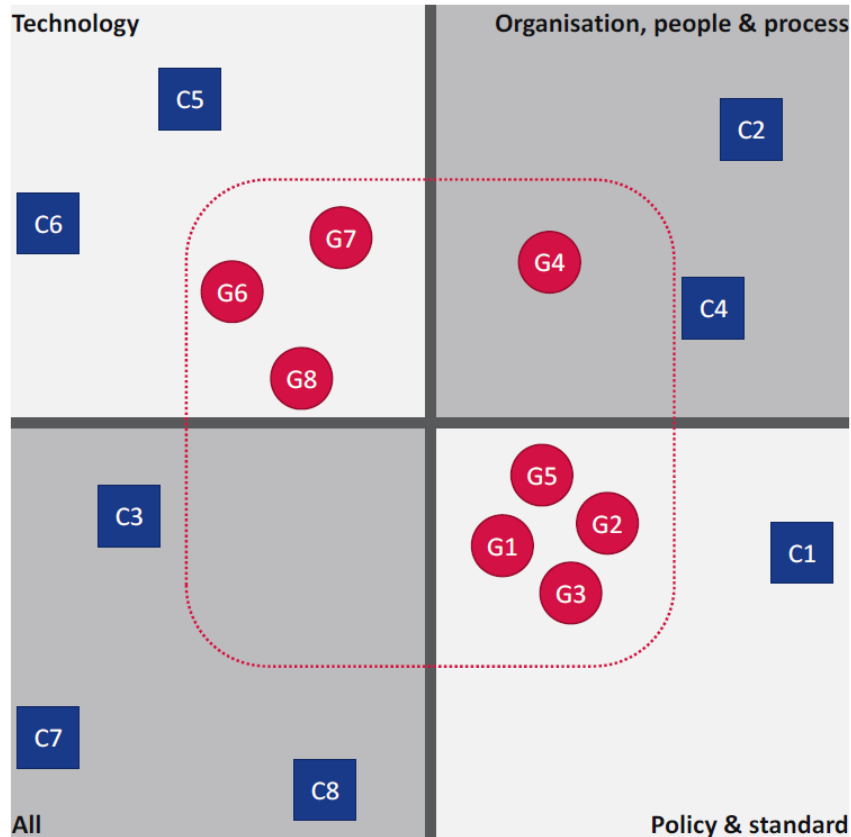




# How will AI will impact cyber security?



# Development of cyber threat mitigation measures at national and international levels



- Gaps and challenges that are mainly related to technology;
- Gaps and challenges that are mainly related to organisation, people and process;
- Gaps and challenges mainly concerning policy and standard; and
- Gaps and challenges concerning a mix of all the previous areas (*i.e.* affecting all the previously mentioned areas).<sup>106</sup>

As the figure indicates, challenges and gaps tend to concentrate in both the *technology and tools* area and *policy and standards* area.

## Challenges

- C1** Difficulties to integrate security for safety
- C2** Inadequate importance and spending being afforded to cyber security
- C3** Inadequate checking for countermeasures
- C4** Unwillingness to collaborate and exchange information on cyber security
- C5** Slow phasing out of legacy systems
- C6** Inadequate data exchange between IPT and SC operators
- C7** Weak situational awareness of cyber threats
- C8** Resistance to security adoption

## Gaps

- G1:** Lack of a common EU approach to IPT
- G2:** No integration of security in current guidelines or strategies for IPT
- G3:** Lack of common definitions and formalised cyber security policies
- G4:** Lack of corporate governance for IPT security
- G5:** No specific security standards for IPT
- G6:** Lack of advanced interdependent analysis tools
- G7:** Lack of advanced risk assessment tools
- G8:** Lack of advanced real-time and multi-stakeholder-enabled security technologies





*“Human beings' reason through analogies, and policymakers often reach for analogies from the past to make sense of the present.”*

Crisis Instability and Preemption: The 1914 Railroad Analogy, author Francis J. Gavin, **UNDERSTANDING CYBER CONFLICT 14 ANALOGIES, GEORGE PERKOVICH & ARIEL E. LEVITE, 2017 Georgetown University Press, Washington D.C.**