Expert Meeting on Strengthening Security and Inter-operability along Euro-Asian Inland Transport Corridors

Johnathan Partouche, Tbilisi 12.12.2019

BEYOND THE KNOWN THREATS

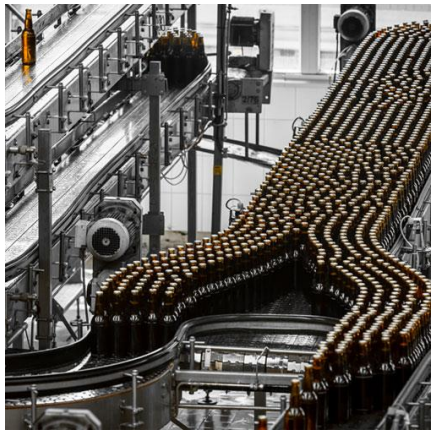
Organization for Security and Co-operation in Europe

UNECE

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

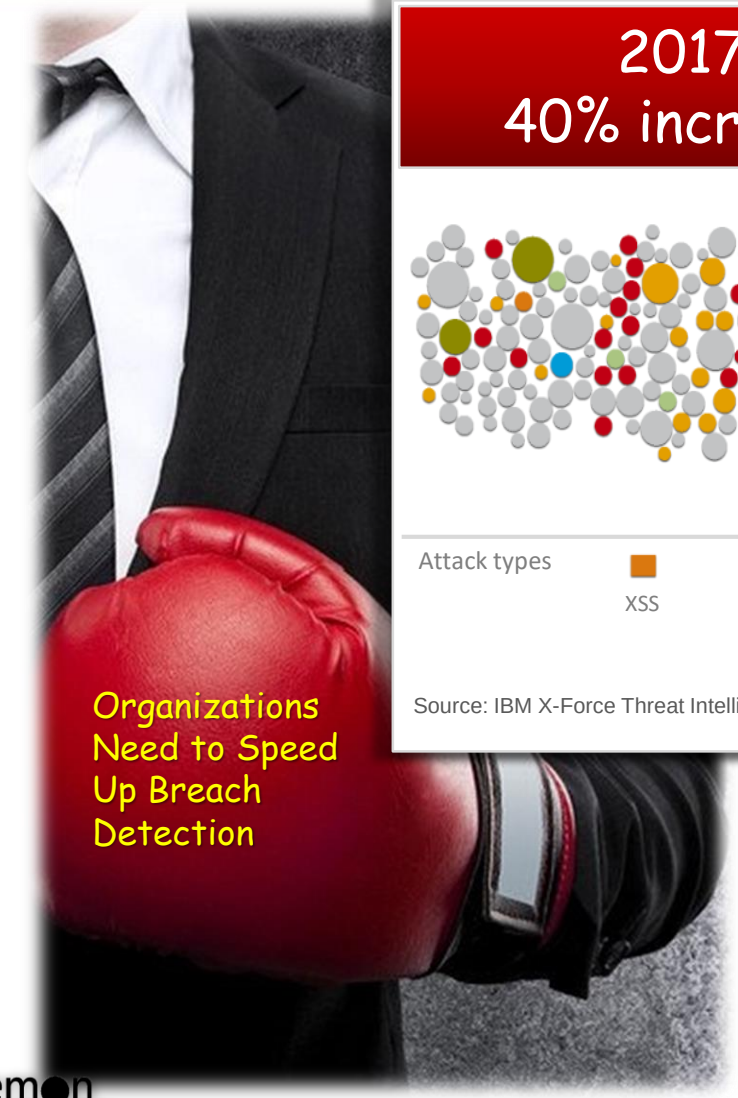
Malicious Email Per User by Industry (per year)

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%

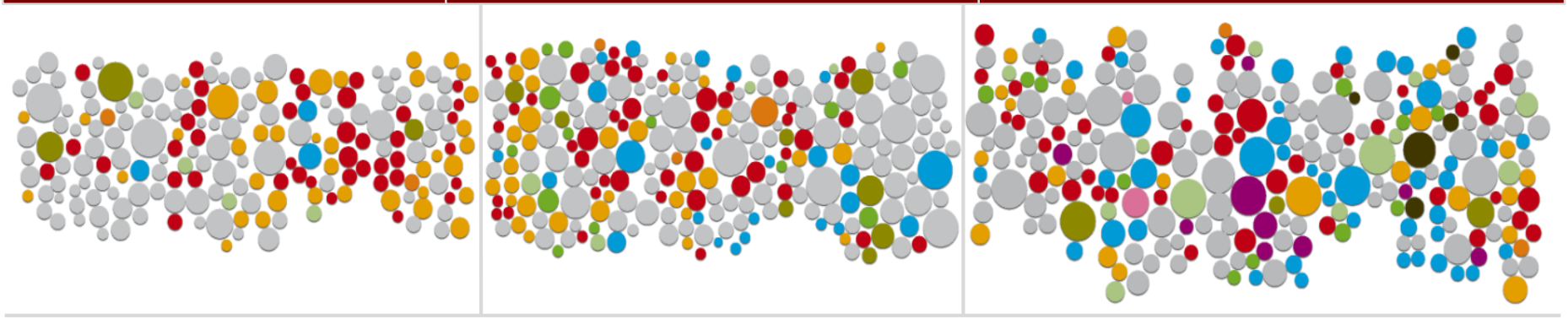
95% of enterprise-network attacks are a result of a spear-phishing campaign

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

Conventional safeguards are not working



2017	2018	2019
40% increase	800,000,000+ records	Unprecedented impact



Source: IBM X-Force Threat Intelligence Quarterly – 1Q 2015

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.

Source: Cost of Data Breach Study, Ponemon Institute

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

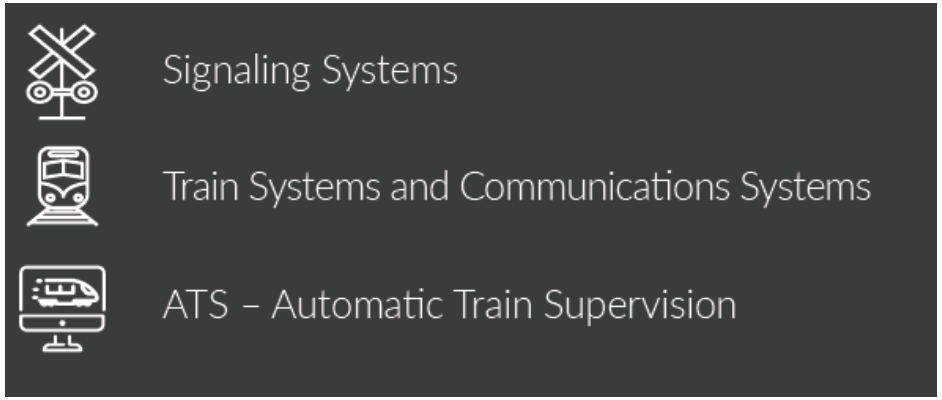
Traditional security practices are unsustainable

85
security tools from
45
vendors
IBM client example

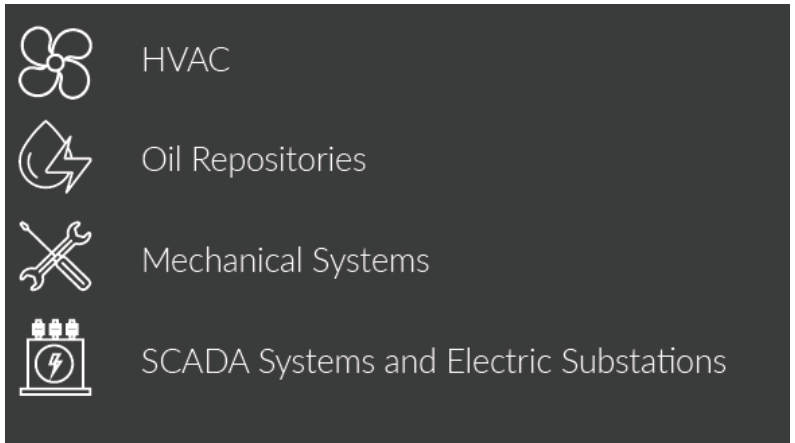
83%
of enterprises have difficulty finding the security skills they need
ESG Research

Cyber threats to increasingly digitalized/ automated transport and logistics systems

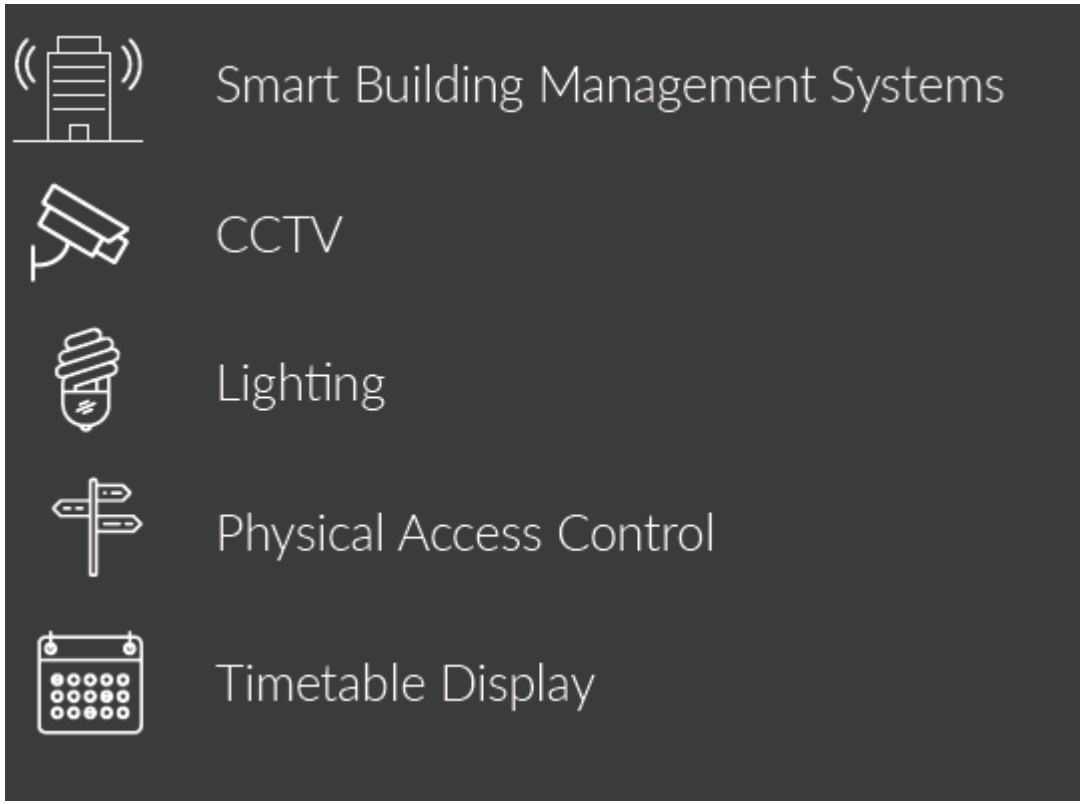
- Train assets



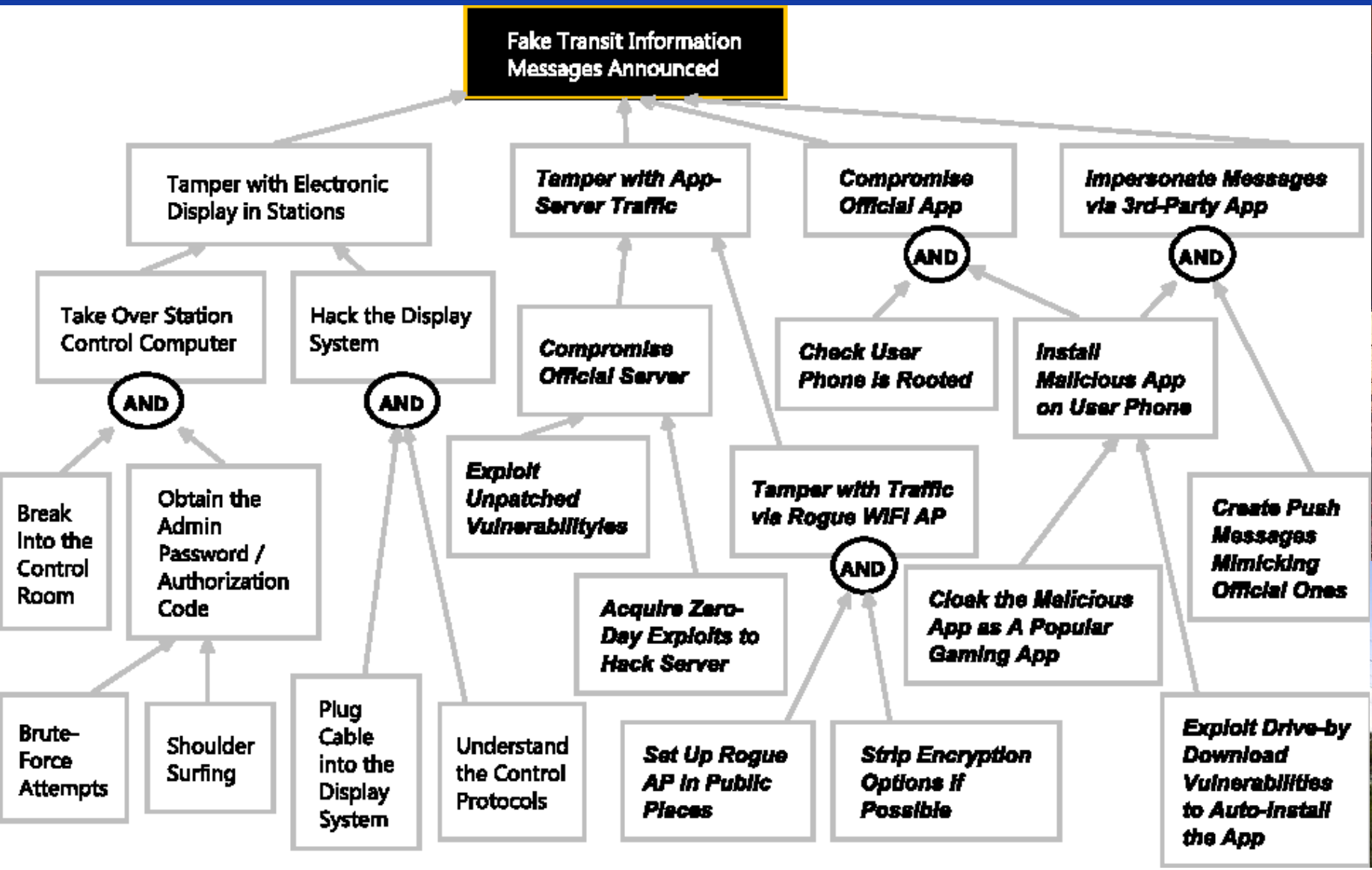
- Infrastructure



- Building Management Systems



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

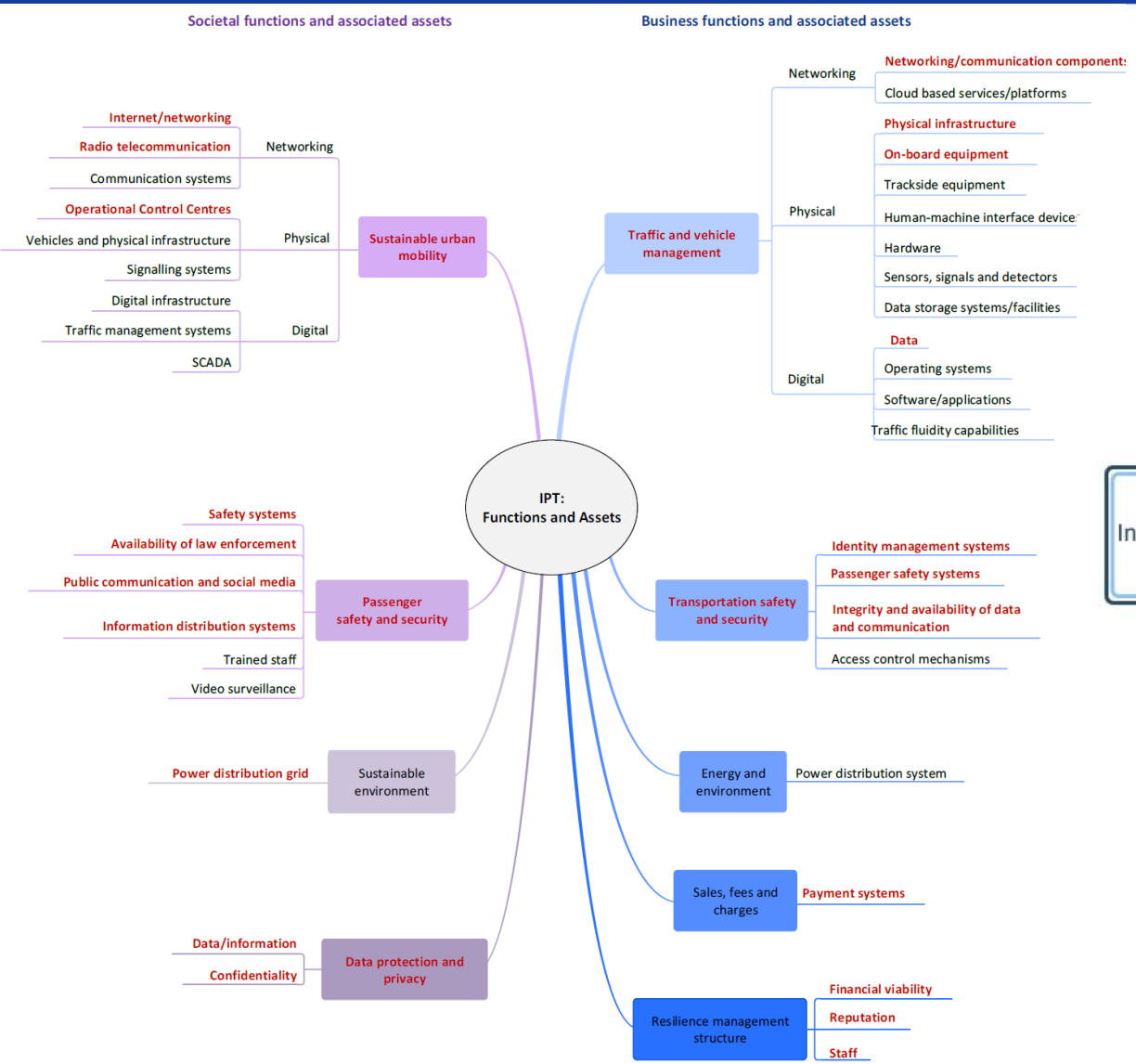
Resource Constraints

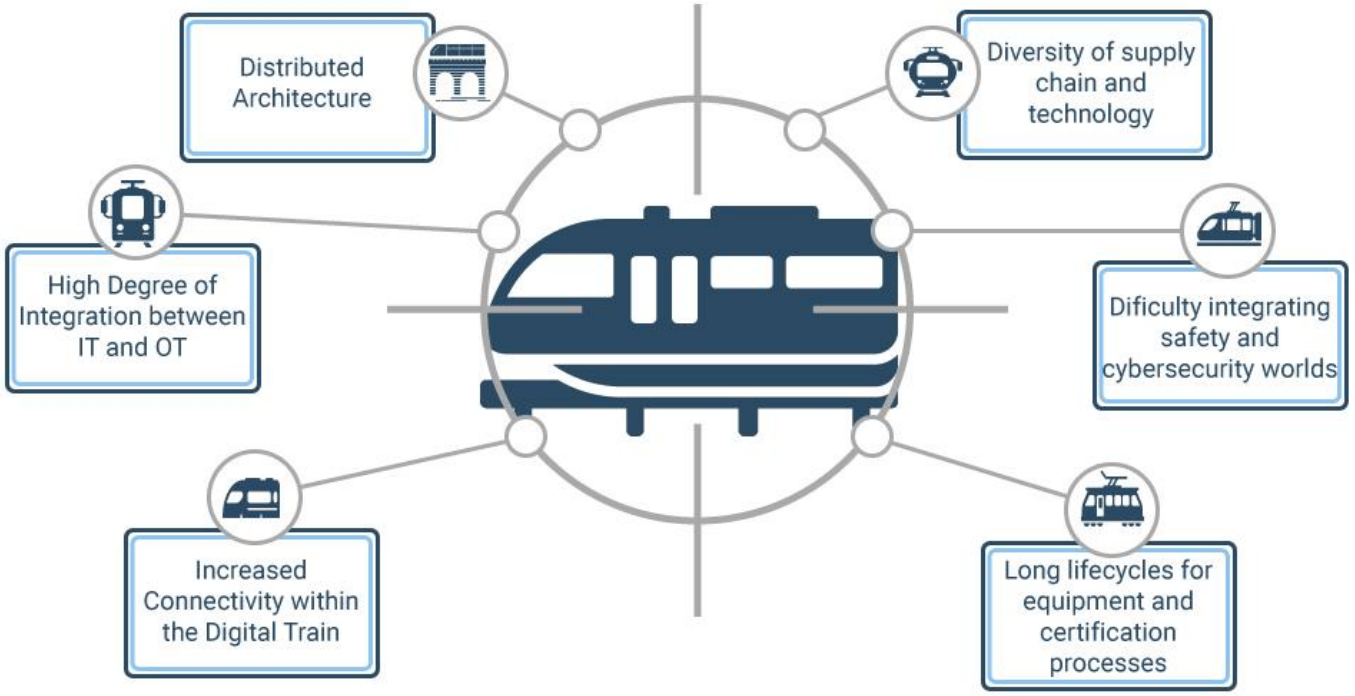
- Struggling security teams
- Too much data with limited skills* & manpower to manage it all
- Managing & monitoring increasing compliance demands

* *Even when security projects are successfully funded, many CISOs encounter roadblocks to implementation, especially when it comes to finding the right skills.*
Source: IBM 2015 CISO Report «From checkboxes to frameworks»

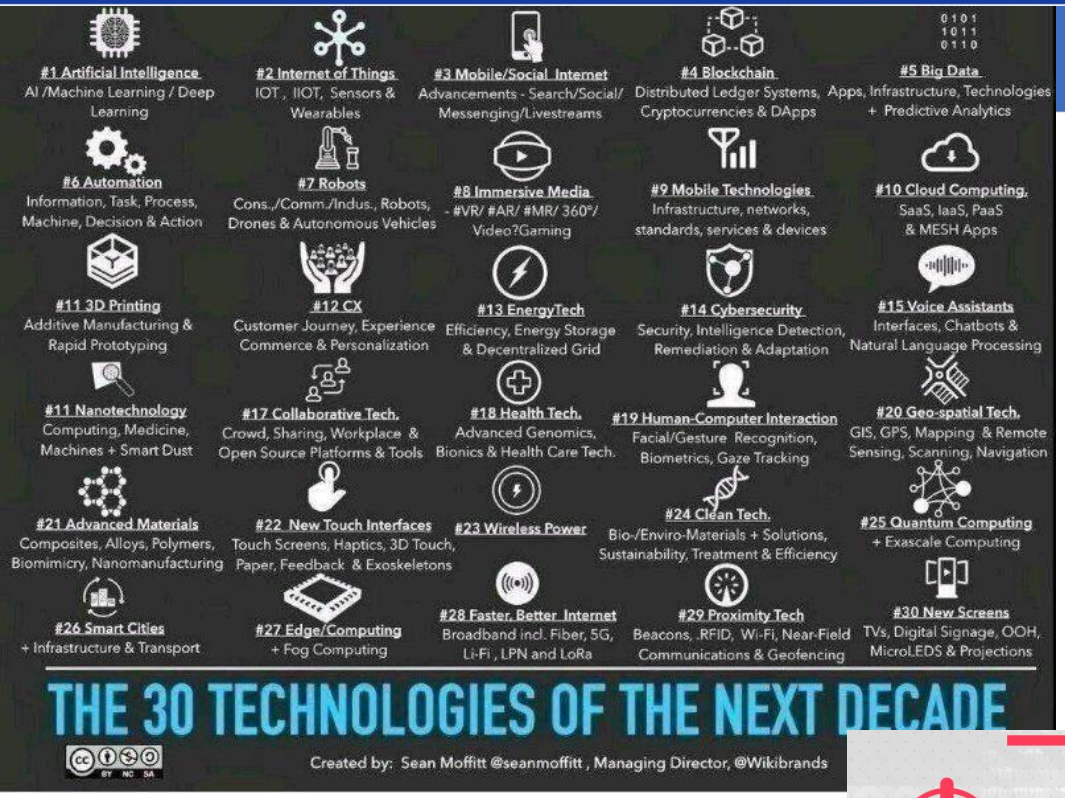
Securing today's transportation infrastructures requires a **new approach** & a **new set of capabilities**.

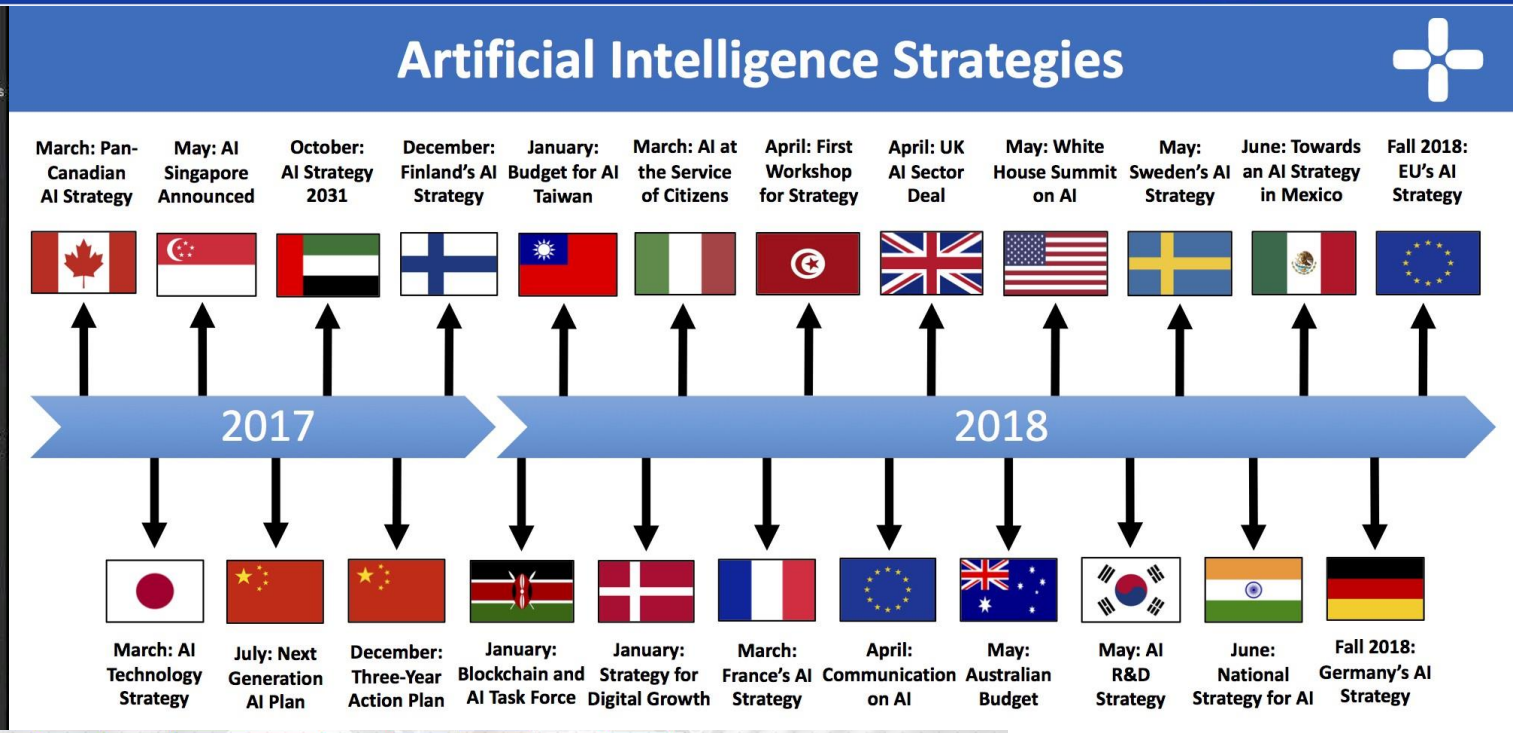
What should Governments and private sector do to effectively address these challenges?





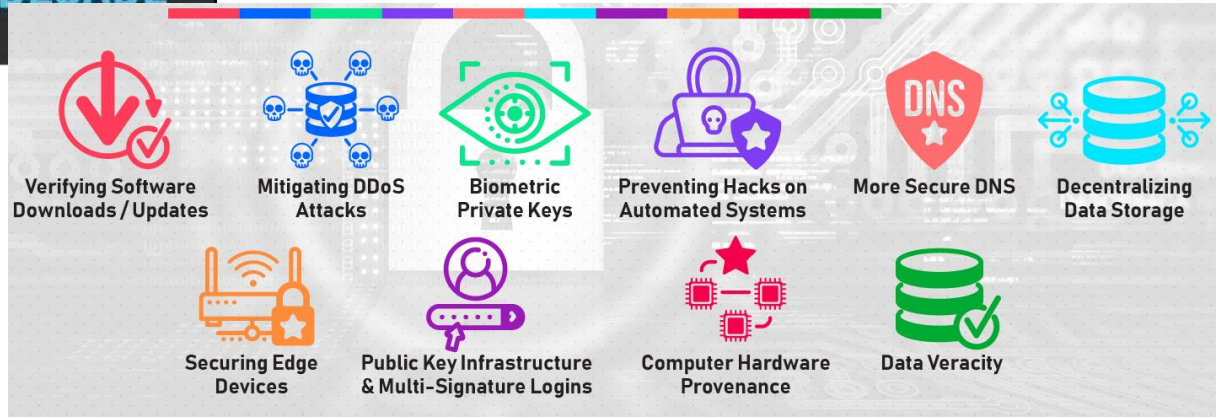
Emerging technologies to secure supply chains





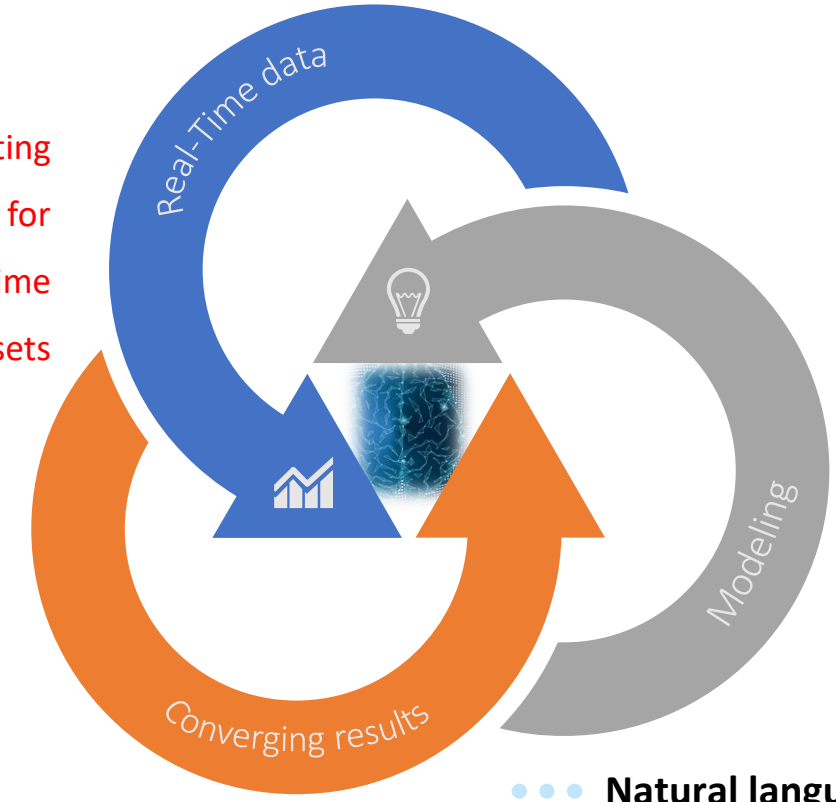
2018-07-13 | Politics + AI | Tim Dutton

How will blockchain impact cyber security?



How will AI will impact cyber security?

Connection to existing data bases for extraction of real-time data sets

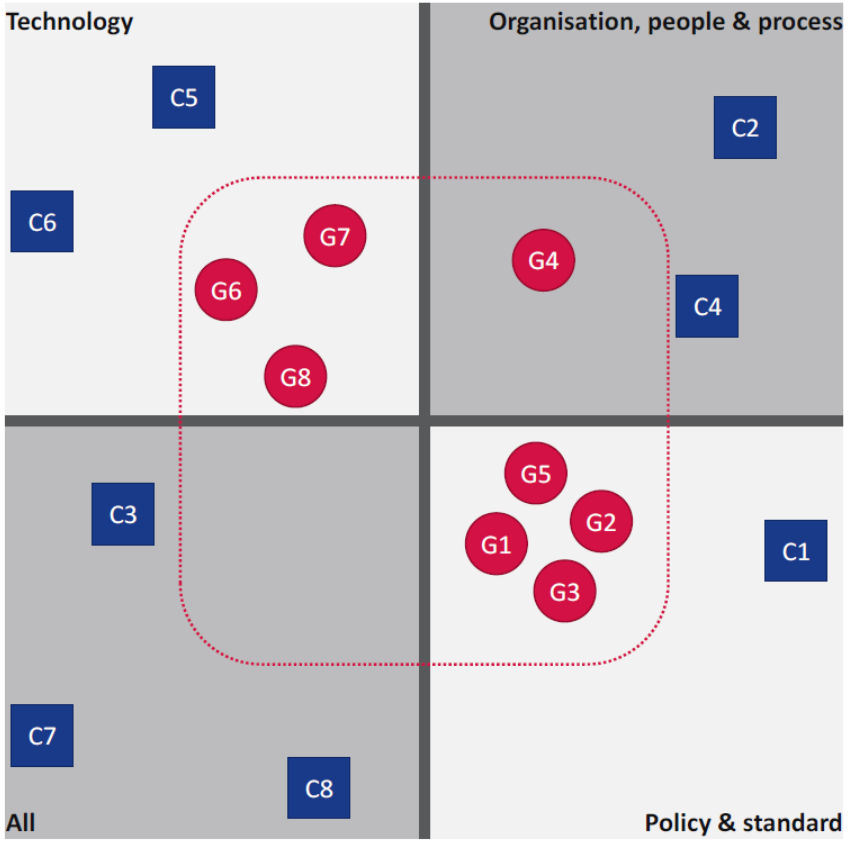


Data Model Acceleration through existing software analysis

Immediate response on most suitable outcomes amongst immense number of possibilities

- **Ingest mass amounts of data**
- **Classify, select, and normalize data**
- **Natural language processing**
- **Training and learning with feedback**
- **Relational analysis visualized through knowledge graphs**

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).[106]

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

References & further reading

“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.