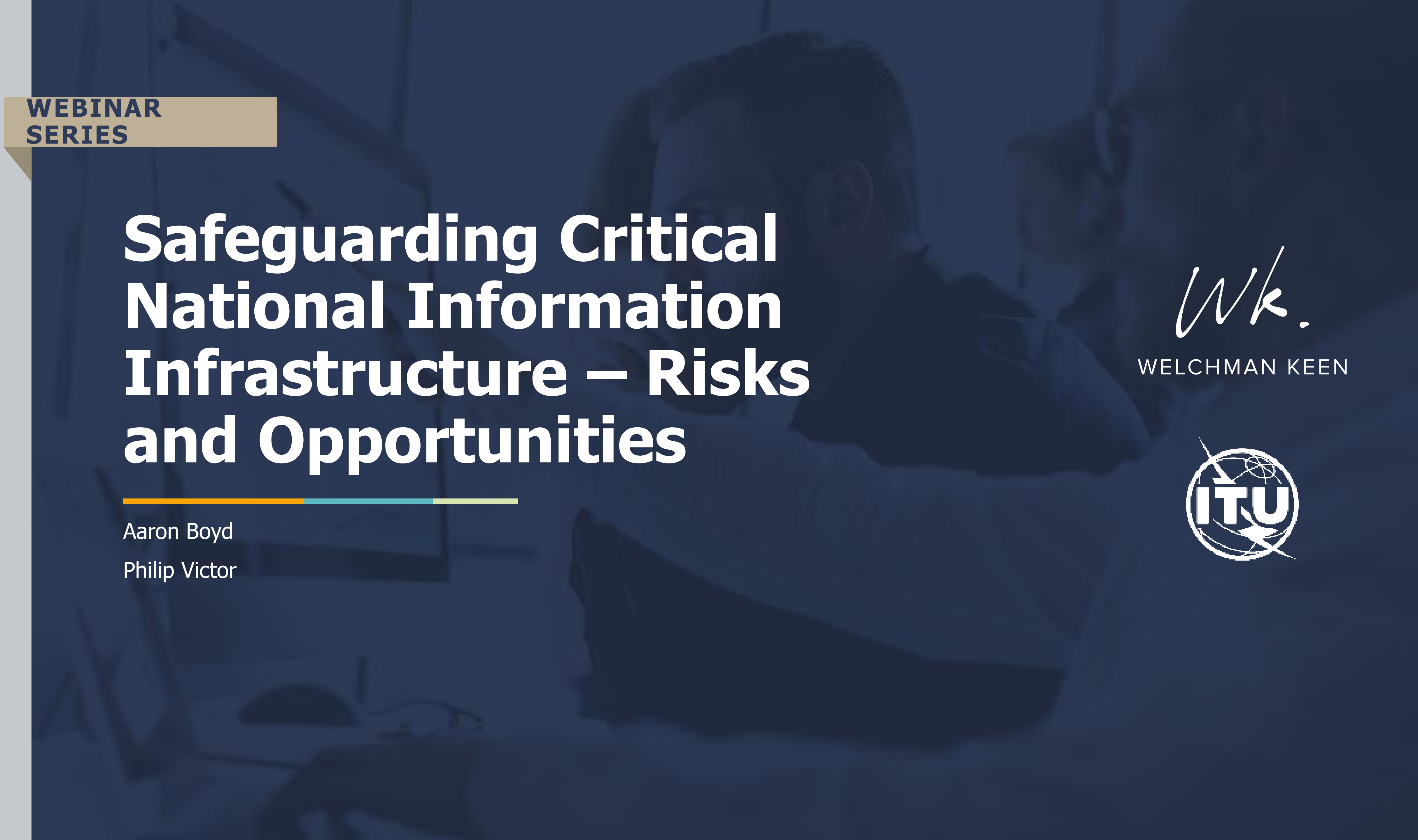


WEBINAR SERIES

Safeguarding Critical National Information Infrastructure – Risks and Opportunities

Aaron Boyd

Philip Victor

WELCHMAN KEEN

ITU

ABOUT US

WELCHMAN KEEN
STRATEGIC ADVISORY

- ✓ As a part of our focus on connectivity, we provide training on a variety of topics.
- ✓ Help to build a country's CNII strategy from the ground up through a measured approach to include what is necessary in achieving their specific objectives.
- ✓ Our key focus on critical national infrastructure (CNII) represents a belief that these pillars hold the key to national, economic, public safety and social well-being.

TECHNOLOGY POLICY

TELECOMMUNICATION INVESTMENT STRATEGY

CYBER RISK AND POLICY

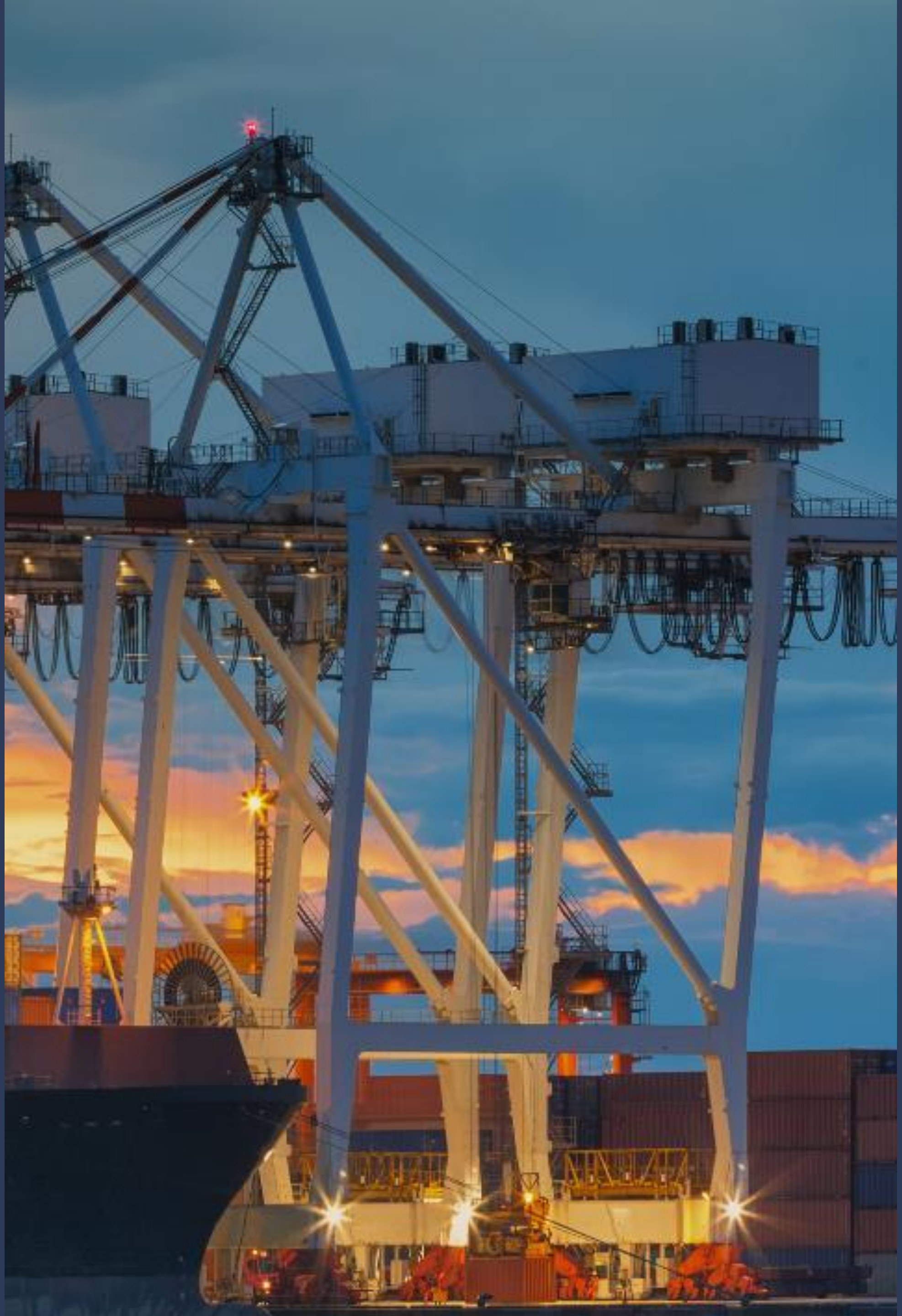
MARKET ACCESS

Wk.

ITU

SECTION 01

WHAT IS CNII?

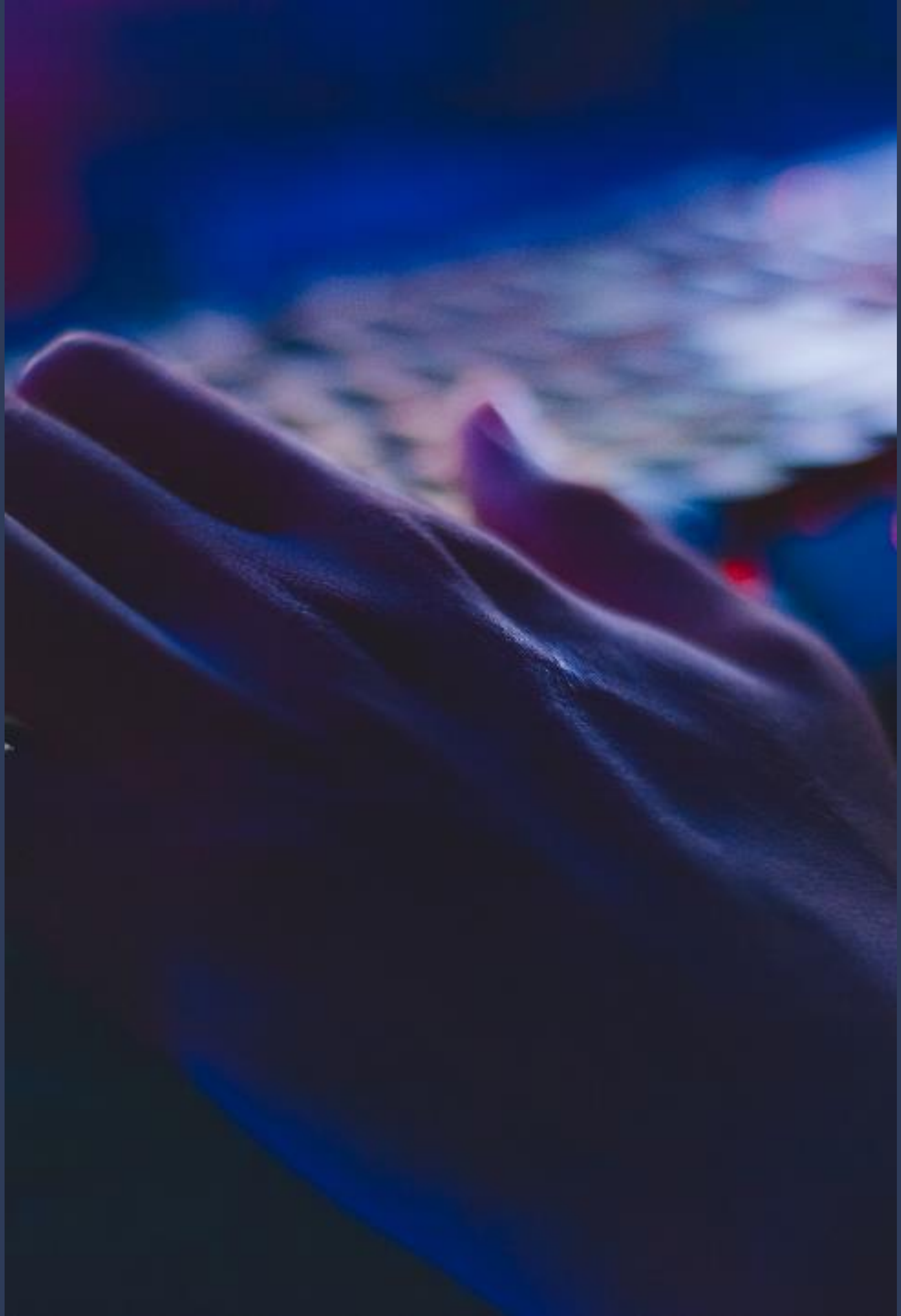


Critical National Infrastructure

"Those infrastructures which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have serious consequences".

Source:

Global Forum on Cyber Expertise (GFCE)



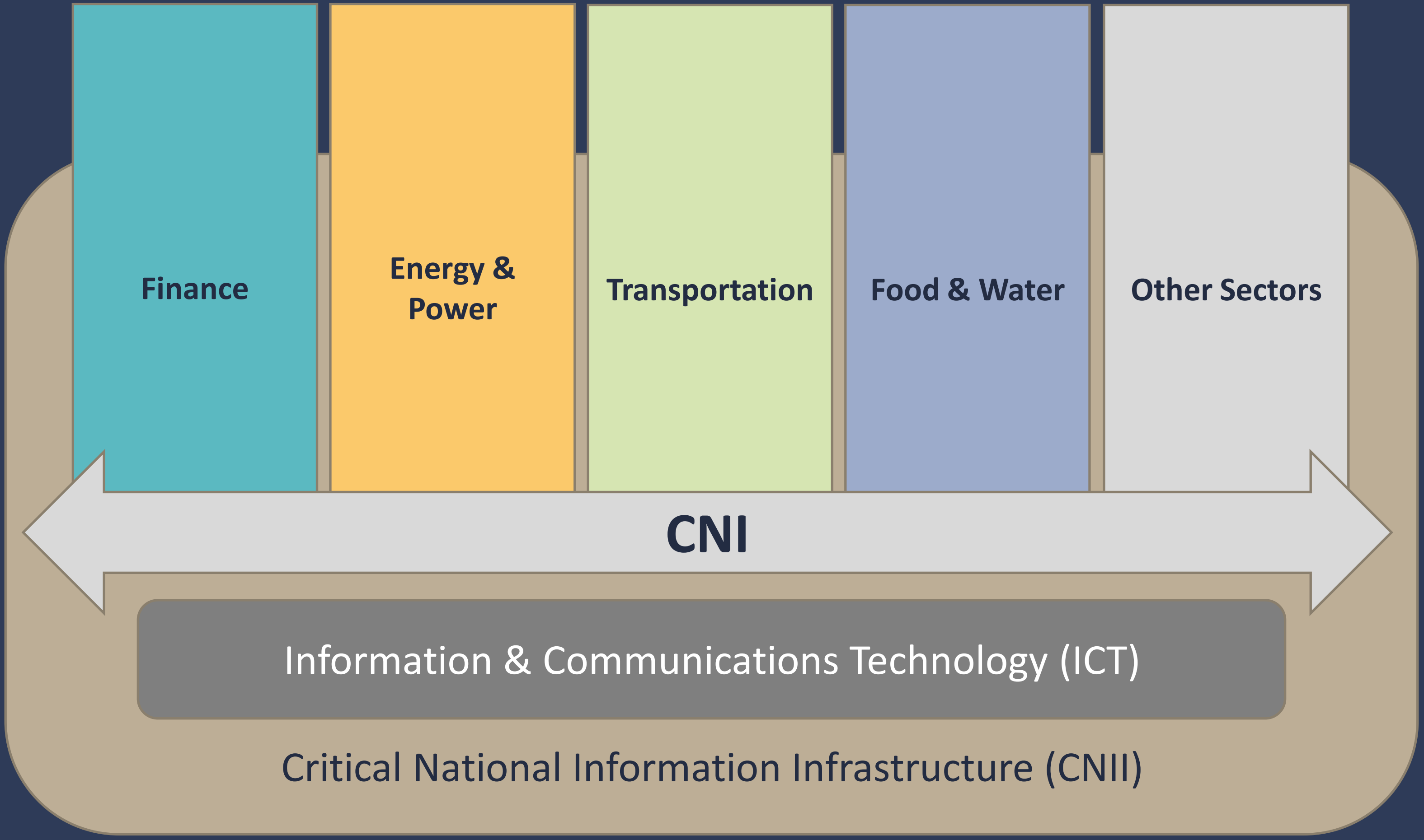
Critical National Information Infrastructure (CNII)

“Material and digital assets, networks, services, and installations that, if disrupted or destroyed, would have a serious impact on the health, security, or economic well-being of citizens and the efficient functioning of a country’s government”

Source:

INTERNATIONAL CIIP HANDBOOK 2008 / 2009

CNI & CNII Integration



Finance

Energy & Power

Transportation

Food & Water

Other Sectors

CNI

Information & Communications Technology (ICT)

Critical National Information Infrastructure (CNII)

CNI Focus

OECD 2015 Security Risk Recommendation:

✓ CNI should focus on the protection of essential services against digital security risk rather than the protection of critical information infrastructures themselves.

Wk.

CNII Sectors

- ✓ A critical sector in one country may not be critical to another, however, there are common sectors that most countries agree on to be categorised as critical and essential.
- ✓ Governments must prioritize these sectors when it comes to its protection as it relies on the availability of funding, technology, and human capacity.

Health

ICT

Energy

Security & Defense

Water

Manufacturing

Food

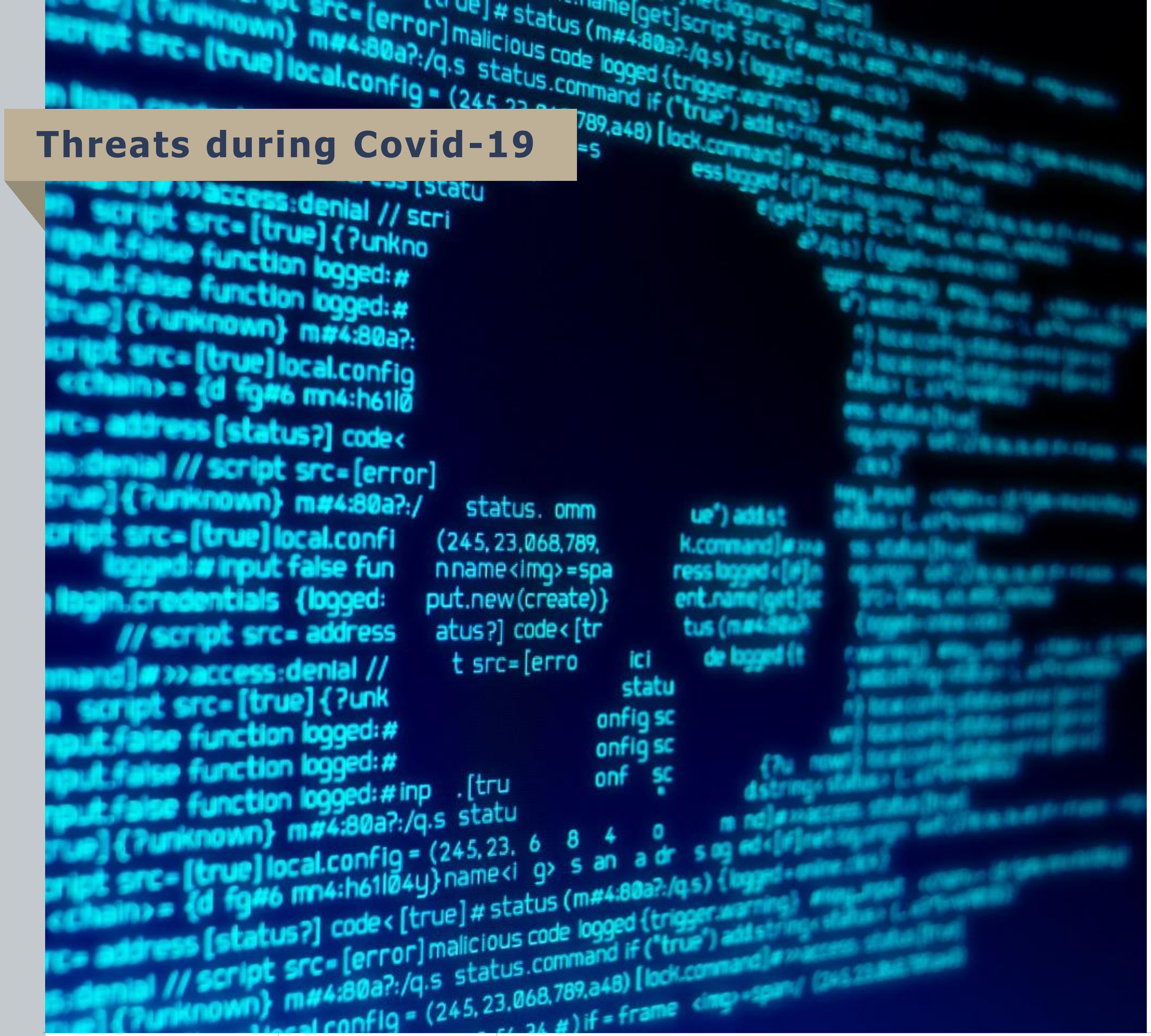
Transportation

Finance

Government

SECTION 02

THREATS AND ATTACKS ON CNII



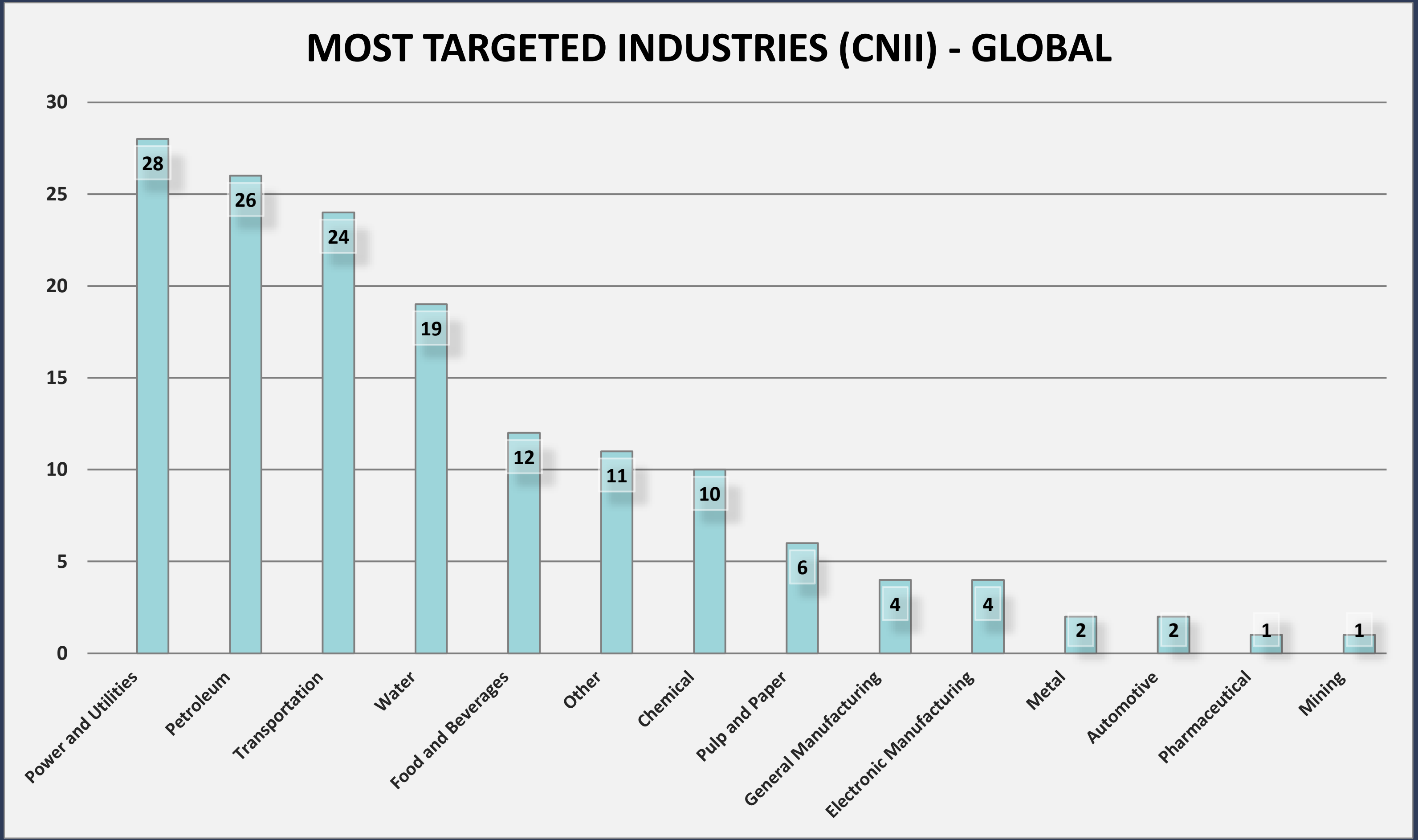
Threats during Covid-19

Increased Cyber threats during COVID-19

- ✓ Recent assessment conducted by INTERPOL, it was revealed that the Covid-19 pandemic has seen a shift of attacks from small businesses to critical infrastructure, government and major corporations.
- ✓ Deloitte reported that COVID-19 is seeing a “next normal” where sectors not classified as critical before are now being viewed as critical.
- ✓ Healthcare and humanitarian organisations such as WHO are being targeted and Check Point Software Technologies reported a 500% increase in attacks toward these organisations.

Most Targeted Industries

Global statistics



https://www.lanner-america.com/critical-infrastructure/integrating-multi-layer-architectures-mitigate-cyber-vulnerabilities-oil-gas-sectors/

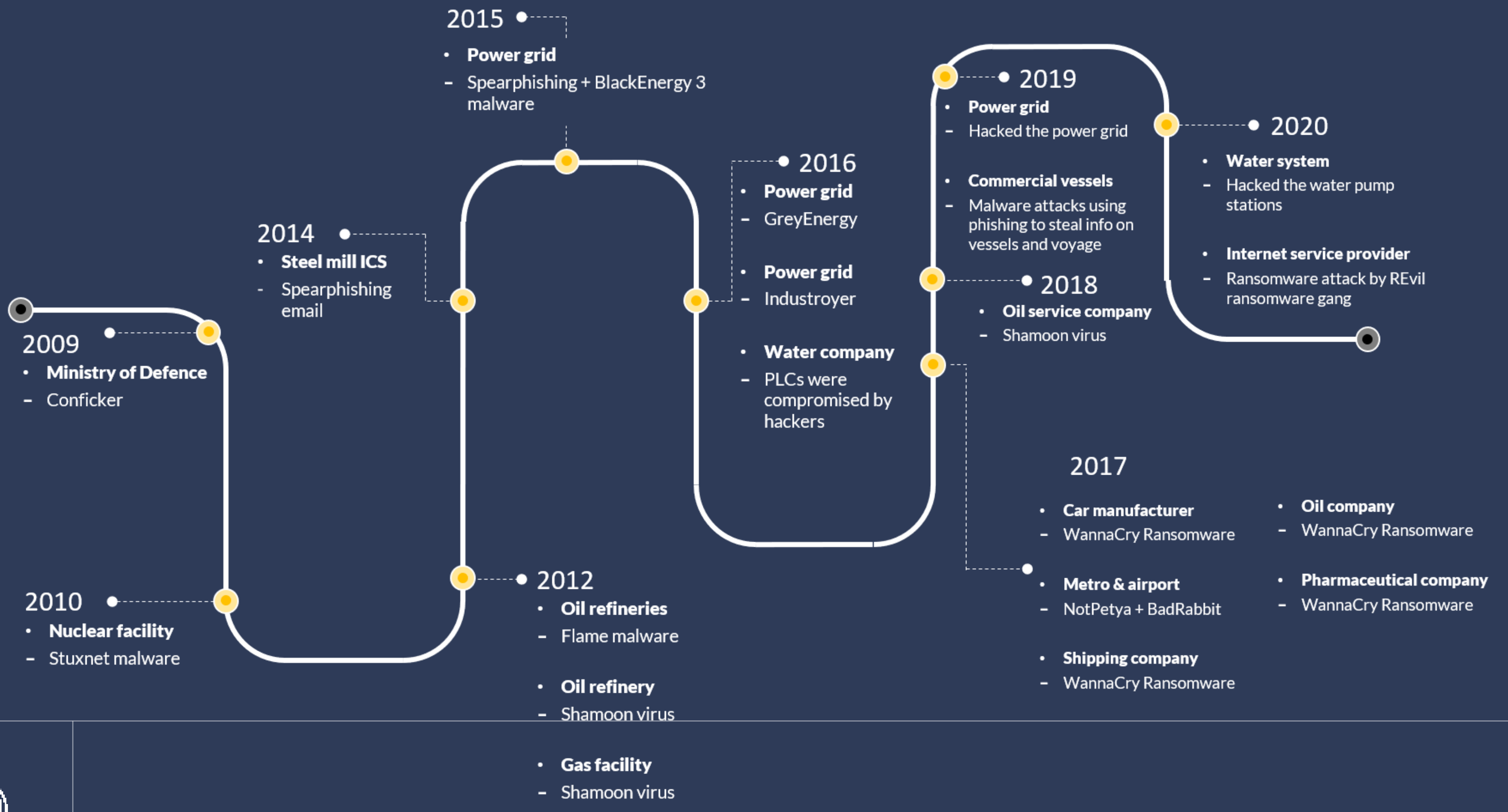
Threats and Attacks

CNII Cyber Attacks

- ✓ **Social engineering**
  - Phishing
    - Spearphishing
    - Whaling
    - Smishing
    - Voice phishing
  - Baiting
- ✓ **Malware**
  - Trojan
  - Spyware
  - Keylogger
  - Ransomware
- ✓ **DDoS**

GLOBAL CNII CYBER ATTACKS

2009 - 2020



2009
- **Ministry of Defence**
- Conficker

2010
- **Nuclear facility**
- Stuxnet malware

2012
- **Oil refineries**
- Flame malware
- **Oil refinery**
- Shamoon virus
- **Gas facility**
- Shamoon virus

2014
- **Steel mill ICS**
- Spearphishing email

2015
- **Power grid**
- Spearphishing + BlackEnergy 3 malware

2016
- **Power grid**
- GreyEnergy
- **Power grid**
- Industroyer
- **Water company**
- PLCs were compromised by hackers

2017
- **Car manufacturer**
- WannaCry Ransomware
- **Metro & airport**
- NotPetya + BadRabbit
- **Shipping company**
- WannaCry Ransomware
- **Oil company**
- WannaCry Ransomware
- **Pharmaceutical company**
- WannaCry Ransomware

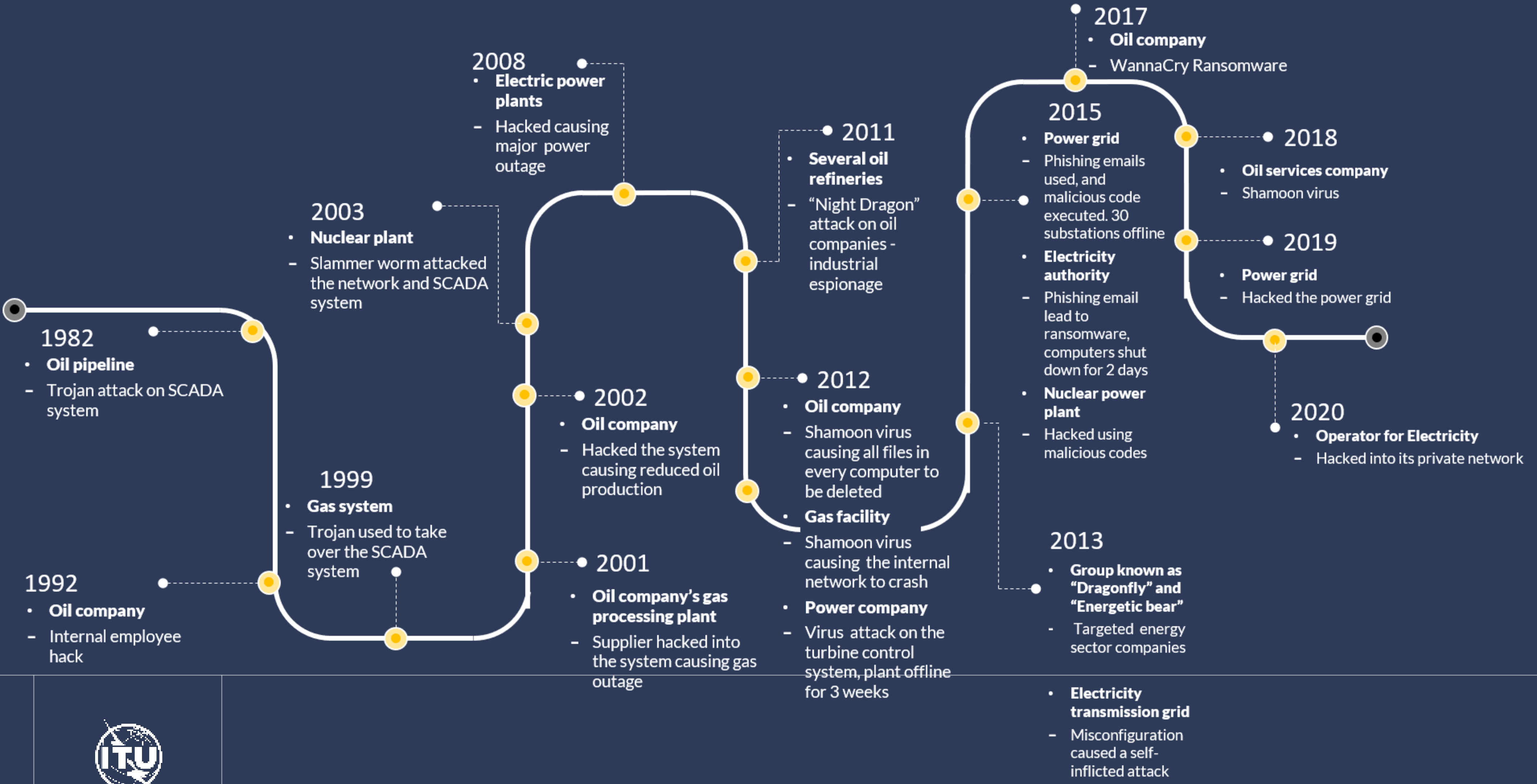
2018
- **Oil service company**
- Shamoon virus

2019
- **Power grid**
- Hacked the power grid
- **Commercial vessels**
- Malware attacks using phishing to steal info on vessels and voyage

2020
- **Water system**
- Hacked the water pump stations
- **Internet service provider**
- Ransomware attack by REvil ransomware gang

CNII CYBER ATTACKS

ENERGY & POWER GRID (1982 – 2020)



1982
- **Oil pipeline**
  - Trojan attack on SCADA system

1992
- **Oil company**
  - Internal employee hack

1999
- **Gas system**
  - Trojan used to take over the SCADA system

2001
- **Oil company's gas processing plant**
  - Supplier hacked into the system causing gas outage

2002
- **Oil company**
  - Hacked the system causing reduced oil production

2003
- **Nuclear plant**
  - Slammer worm attacked the network and SCADA system

2008
- **Electric power plants**
  - Hacked causing major power outage

2011
- **Several oil refineries**
  - "Night Dragon" attack on oil companies - industrial espionage

2012
- **Oil company**
  - Shamoon virus causing all files in every computer to be deleted
- **Gas facility**
  - Shamoon virus causing the internal network to crash
- **Power company**
  - Virus attack on the turbine control system, plant offline for 3 weeks

2013
- **Group known as "Dragonfly" and "Energetic bear"**
  - Targeted energy sector companies
- **Electricity transmission grid**
  - Misconfiguration caused a self-inflicted attack

2015
- **Power grid**
  - Phishing emails used, and malicious code executed. 30 substations offline
- **Electricity authority**
  - Phishing email lead to ransomware, computers shut down for 2 days
- **Nuclear power plant**
  - Hacked using malicious codes

2017
- **Oil company**
  - WannaCry Ransomware

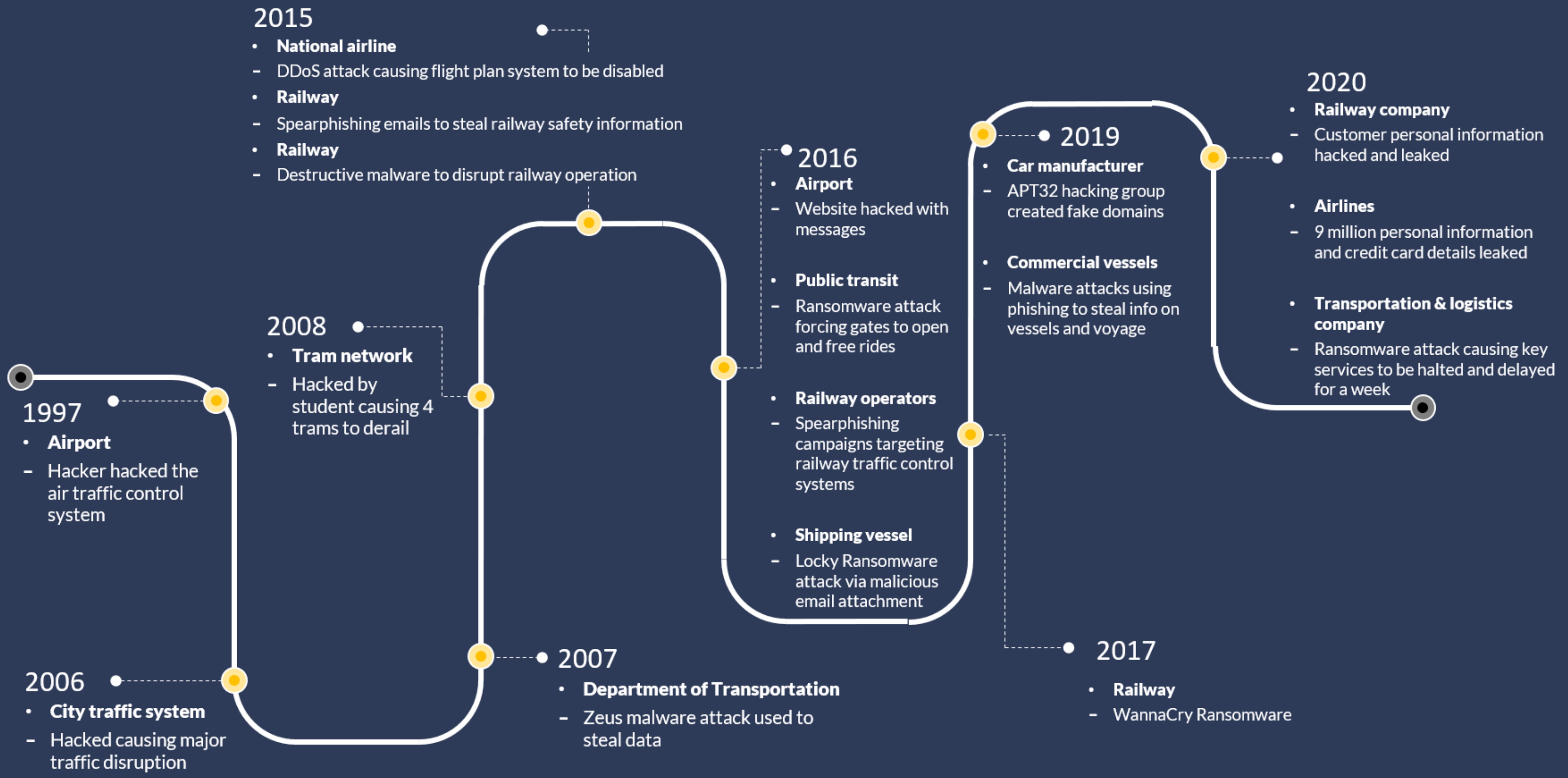
2018
- **Oil services company**
  - Shamoon virus

2019
- **Power grid**
  - Hacked the power grid

2020
- **Operator for Electricity**
  - Hacked into its private network

CNII CYBER ATTACK

TRANSPORTATION (1997 – 2020)



1997
- **Airport**
  - Hacker hacked the air traffic control system

2006
- **City traffic system**
  - Hacked causing major traffic disruption

2007
- **Department of Transportation**
  - Zeus malware attack used to steal data

2008
- **Tram network**
  - Hacked by student causing 4 trams to derail

2015
- **National airline**
  - DDoS attack causing flight plan system to be disabled
- **Railway**
  - Spearphishing emails to steal railway safety information
- **Railway**
  - Destructive malware to disrupt railway operation

2016
- **Airport**
  - Website hacked with messages
- **Public transit**
  - Ransomware attack forcing gates to open and free rides
- **Railway operators**
  - Spearphishing campaigns targeting railway traffic control systems
- **Shipping vessel**
  - Locky Ransomware attack via malicious email attachment

2017
- **Railway**
  - WannaCry Ransomware

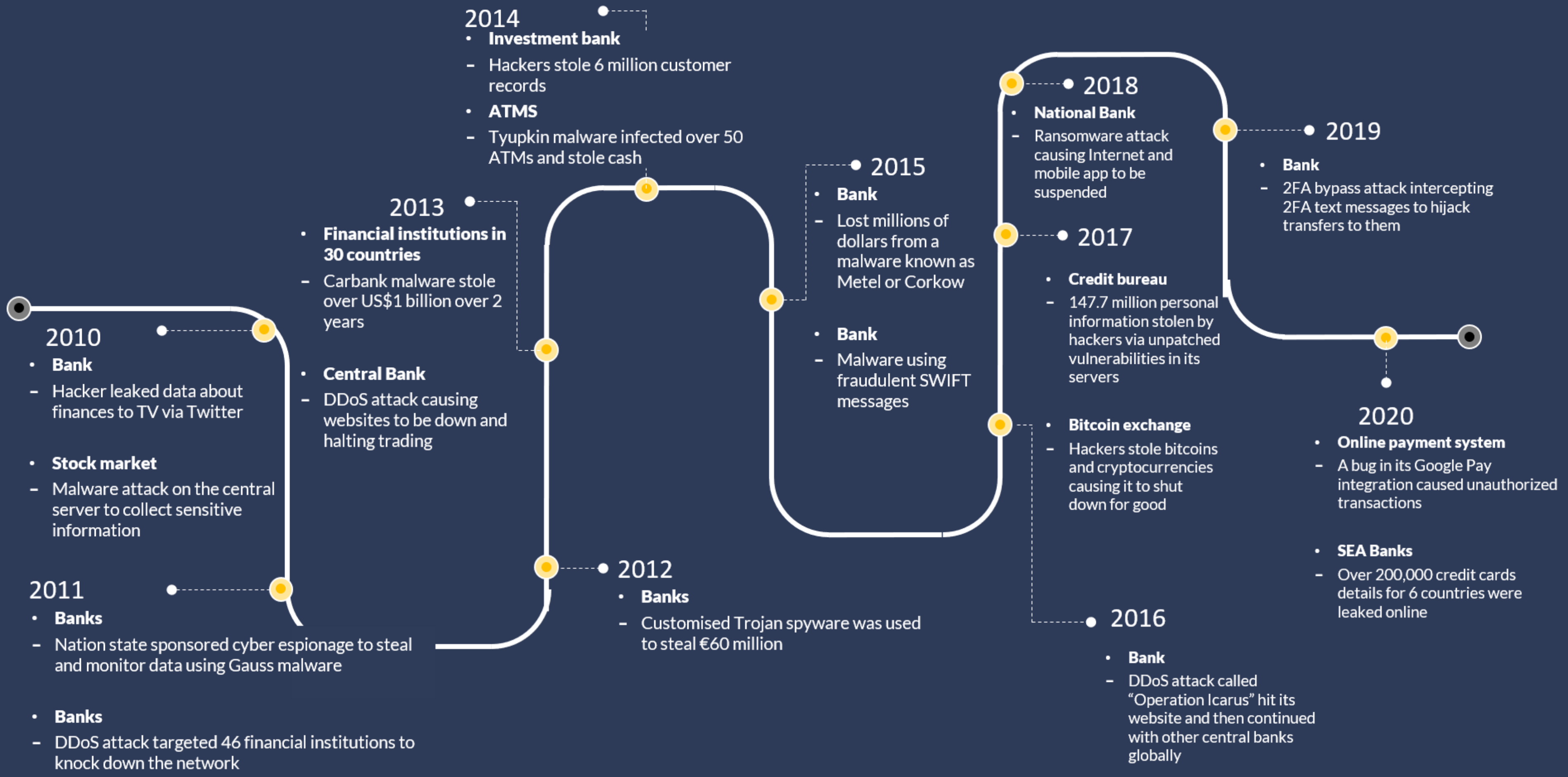
2019
- **Car manufacturer**
  - APT32 hacking group created fake domains
- **Commercial vessels**
  - Malware attacks using phishing to steal info on vessels and voyage

2020
- **Railway company**
  - Customer personal information hacked and leaked
- **Airlines**
  - 9 million personal information and credit card details leaked
- **Transportation & logistics company**
  - Ransomware attack causing key services to be halted and delayed for a week

Threats and Attacks

CNII CYBER ATTACKS

FINANCIAL (2010 – 2020)



2010

- **Bank**
  - Hacker leaked data about finances to TV via Twitter
- **Stock market**
  - Malware attack on the central server to collect sensitive information

2011

- **Banks**
  - Nation state sponsored cyber espionage to steal and monitor data using Gauss malware
- **Banks**
  - DDoS attack targeted 46 financial institutions to knock down the network

2012

- **Banks**
  - Customised Trojan spyware was used to steal €60 million

2013

- **Financial institutions in 30 countries**
  - Carbank malware stole over US$1 billion over 2 years
- **Central Bank**
  - DDoS attack causing websites to be down and halting trading

2014

- **Investment bank**
  - Hackers stole 6 million customer records
- **ATMS**
  - Tyupkin malware infected over 50 ATMs and stole cash

2015

- **Bank**
  - Lost millions of dollars from a malware known as Metel or Corkow
- **Bank**
  - Malware using fraudulent SWIFT messages

2016

- **Bank**
  - DDoS attack called "Operation Icarus" hit its website and then continued with other central banks globally

2017

- **Credit bureau**
  - 147.7 million personal information stolen by hackers via unpatched vulnerabilities in its servers
- **Bitcoin exchange**
  - Hackers stole bitcoins and cryptocurrencies causing it to shut down for good

2018

- **National Bank**
  - Ransomware attack causing Internet and mobile app to be suspended

2019

- **Bank**
  - 2FA bypass attack intercepting 2FA text messages to hijack transfers to them

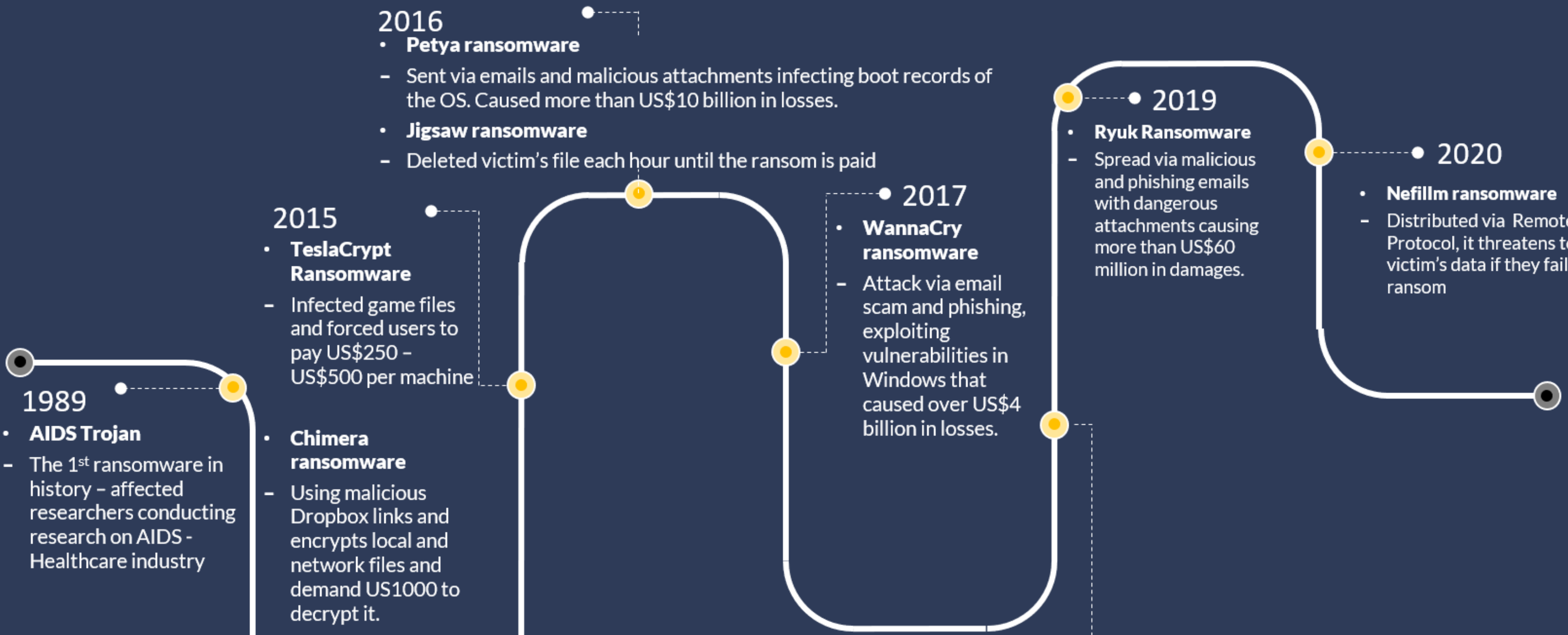
2020

- **Online payment system**
  - A bug in its Google Pay integration caused unauthorized transactions
- **SEA Banks**
  - Over 200,000 credit cards details for 6 countries were leaked online

Threats and Attacks

CNII CYBER ATTACKS

RANSOMWARE (1989 – 2020)



1989
- **AIDS Trojan**
  - The 1st ransomware in history – affected researchers conducting research on AIDS - Healthcare industry

2013
- **Cryptolocker Ransomware**
  - Used a non-standard encryption key that caused more than US$3 million in losses

2014
- **Crypto ransomware**
  - Encrypted files and hid inside the OS. Caused over US$325 million in losses
- **LockerPin**
  - An Android ransomware that shuts down the device and reset the lock screen PIN

2015
- **TeslaCrypt Ransomware**
  - Infected game files and forced users to pay US$250 – US$500 per machine
- **Chimera ransomware**
  - Using malicious Dropbox links and encrypts local and network files and demand US1000 to decrypt it.

2016
- **Petya ransomware**
  - Sent via emails and malicious attachments infecting boot records of the OS. Caused more than US$10 billion in losses.
- **Jigsaw ransomware**
  - Deleted victim's file each hour until the ransom is paid

2017
- **WannaCry ransomware**
  - Attack via email scam and phishing, exploiting vulnerabilities in Windows that caused over US$4 billion in losses.

2018
- **SamSam ransomware**
  - Exploiting the Remote Desktop Protocol and FTP. Over US$40 million in losses

2019
- **Ryuk Ransomware**
  - Spread via malicious and phishing emails with dangerous attachments causing more than US$60 million in damages.

2020
- **Nefillm ransomware**
  - Distributed via Remote Desktop Protocol, it threatens to release victim's data if they fail to pay the ransom

CNII Protection

Trends in CNII Security

- ✓ Many critical infrastructure technologies are based on legacy IT and OT systems which are poorly secured, posing serious risks to utilities, and ultimately national security. Plugging these loopholes and stopping the exploitation of these access points by cyber attackers will play an important role in the cybersecurity of CNI.
- ✓ Data breaches are likely to continue for as long as personal and organizational data remains a valuable black-market commodity. Sensitive data of CNI’s in the wrong hands can prove disastrous leading to huge losses and disruptions to daily life.

OOOOPS, YOUR FILES HAVE BEEN ENCRYPTED!

Send $1,200 worth of bitcoin to this address:

**1BvBMSEYstWetqTFn5Au4
m4GFg7xJaNVN2**

YOUR FILES WILL BE LOST

TIME REMAINING

59:04:25

Trends in CNII Security

- ✓ In the future, as reliance on virtual infrastructure in CNI becomes acceptable; physical redundancies may be abandoned, which would make it easier for an attacker to carry out a devastating breach that can cause real damage. Maintaining physical backups or other physical redundancies can reduce the impact of a successful attack.
- ✓ In 2019, an increasing number of institutions overseeing the critical parts of daily life – suffered IT system shutdowns as a result of ransomware attacks. The repercussions of data breach and denial of service can inflict millions and even billions in losses or disturbing the essential services for maintaining daily life. The trend of ransomware will continue in 2020.

Trends in CNII Security

- ✓ As CNI organizations increase their reliance on mobile devices and on IoT devices, hackers will put more effort into exploiting vulnerabilities.
- ✓ A growing problem is rogue mobile apps that look like trusted brands but are designed to steal sensitive information.
- ✓ In IoT, more and more devices are getting connected to the internet every day without any effective policies and governance leading to many loopholes to be taken advantage of.
- ✓ Challenges with cybersecurity involve device security, data security, and protection of individual’s privacy.

SECTION 03

ADDRESSING THE THREATS

Addressing the threats

- ✓ **Define a risk management framework**
  - ○ Elaborates a continuous and repeatable methodology for identifying, assessing, and responding to cybersecurity risks. (e.g. NIST framework)
  - ○ Organizations can determine their risk tolerance, thus the acceptable level of risk for achieving their supply and organizational goals and are able prioritize remediations and make informed decisions about cybersecurity investments.
- ✓ **Build and test emergency plans**
  - ○ Plans must involve both physical and cyber-attacks to the infrastructure and include the process to defend, mitigate and respond against it.
  - ○ On the national level, the national cybersecurity agency will periodically organise a cyber exercise to simulate potential attack vectors against CNII. This allows CNII to better prepare for such attacks and design appropriate responses to protect, defend and mitigate those threats.

Addressing the threats

✓ **Training, awareness & education**

- Training equips individuals with the necessary skills to perform specific functions within the organisation.
- Employees must be made aware of information security policies and the importance of adhering to them. Communicating this to all employees is vital to ensure they know, understand and comply. The key outcome of security awareness programs and activities is to create a culture of security, change of behaviour and attitude.

✓ **Supply chain security**

- Due to extensive outsourcing, today's supply chain is increasingly complex and externalized, with subsequent additional risks.
- The resilience of a supply chain depends on its weakest link and operators are secure only if their entire ecosystem of partners and vendors is secure.
- Adversaries can use poorly protected partners as attack vectors to compromise critical operators.
- An integrated and sustainable supply chain security objective must be included in business plans, contracts and operations.

Addressing the threats

✓ **Information sharing & cooperation**

- Through information sharing, CNI can reduce and prevent the spread of the attack and minimise the damage to the infrastructure and country.
- Through partnerships, sectors can share information as well as collaborate to solve issues relating to cybersecurity threats and attacks.
- Alliances also help to share skills within the sectors where some unique skills may be required from the government or private sector. (e.g. FIRST)

✓ **Legal compliance**

- Legal compliance ensures that operators meet critical security standards identified by national decision makers.

✓ **Continuous monitoring & assessment of cybersecurity posture**

- The digital risk landscape is in constant evolution and need to build repeatable processes to monitor and assess the cybersecurity maturity level on an ongoing basis.
- Assessment should consider the risk-related adequacy of the processes, people, and technology, in order to identify cybersecurity substantial gaps and determine appropriate remedies to resolve weaknesses.
- CNI must examine the general preparedness of the operator, and the ability to detect and to respond to incidents and ensure business continuity.

National Policies

CNII National Policies

To build a robust tower around CNI, you will need:

- ✓ A national strategy
- ✓ Legal foundations
- ✓ Incident response capability
- ✓ Industry-government partnerships
- ✓ A culture of security
- ✓ Information sharing mechanisms
- ✓ Risk management approach

SECTION 04

MOVING FORWARD & CONCLUSION

CNI must have:

- ✓ A shift of mindset in the manner cybersecurity is addressed.
- ✓ Look beyond technical tools to adopt a new cyber defense strategy.

Conclusion

Conclusion

- ✓ Be prepared – training & vulnerability assessment.
- ✓ Design sector specific resources & initiatives.
- ✓ Cooperate with agencies on a national, regional and international level.
- ✓ Expand information sharing.
- ✓ Build robust national policies & strategies.

THANK YOU

Safeguarding Critical National Information Infrastructure – Risks and Opportunities

Aaron Boyd – aboyd@welchmankeen.com

Philip Victor – vphilip@welchmankeen.com

Wk.
WELCHMAN KEEN

ITU