ITU RDF 2020

CRITICAL INFORMATION INFRASTRUCTURE (CII)

Presentation by Philip Victor,

Managing Director of Welchman Keen

Wk.

WELCHMAN KEEN

ABOUT US

WELCHMAN KEEN IS A STRATEGIC ADVISORY

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

TECHNOLOGY POLICY

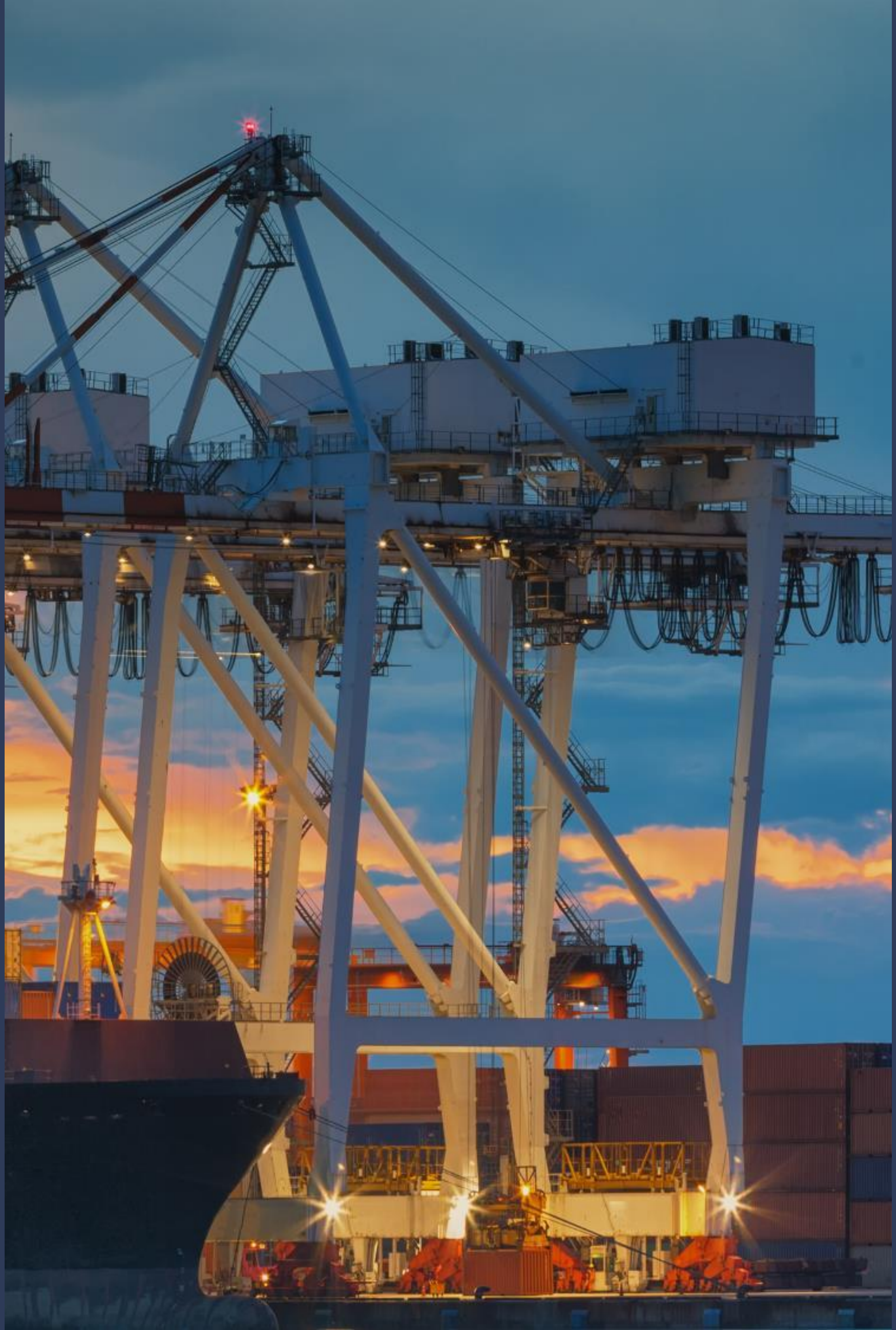
TELECOMMUNICATION INVESTMENT STRATEGY

CYBER RISK AND POLICY

ITU SECTOR MEMBER

SECTION 01

WHAT IS A CRITICAL INFORMATION INFRASTRUCTURE (CII)?



Critical 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)

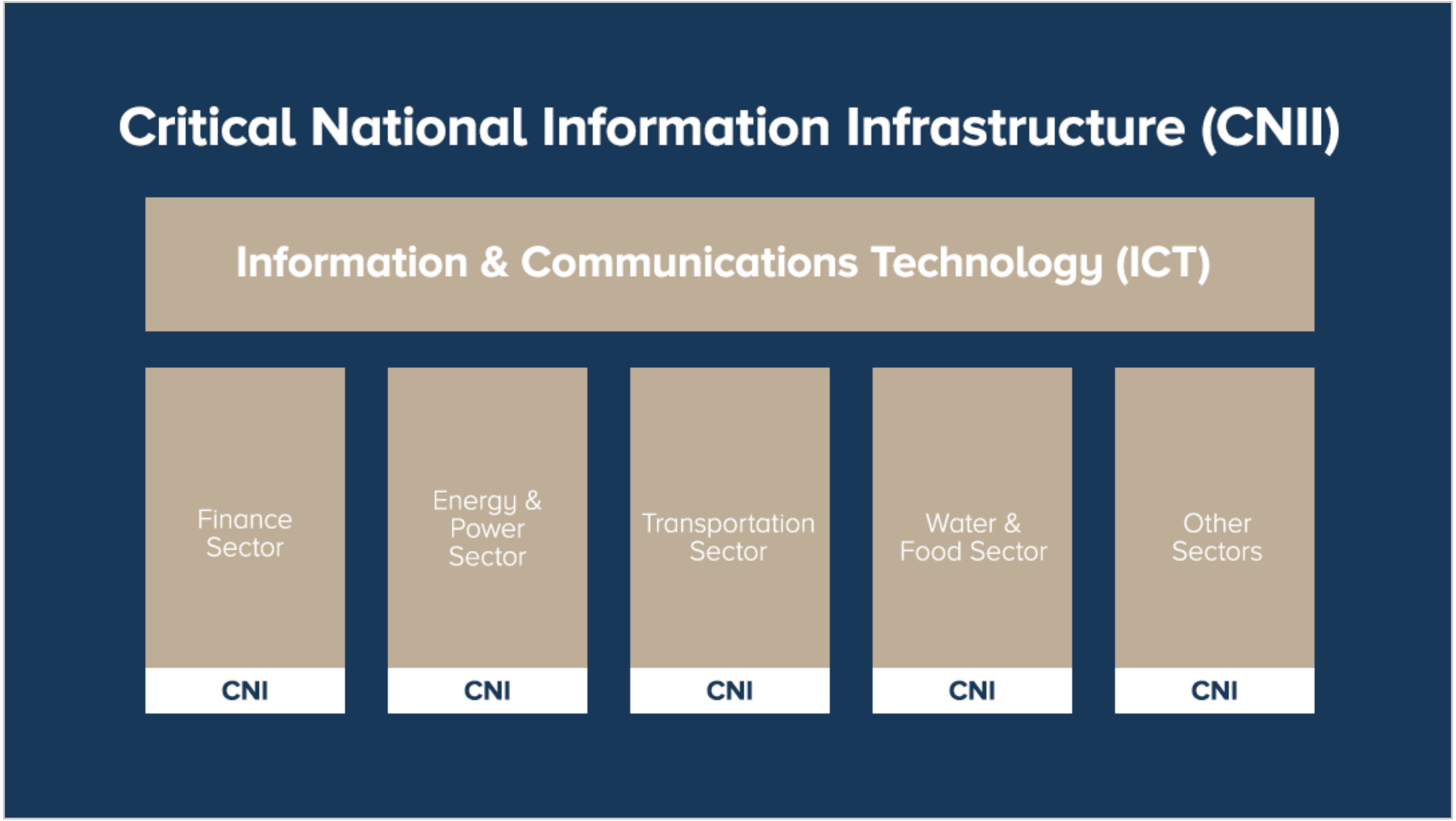
Critical Information Infrastructure (CII)

“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 function of a country’s government.”

SOURCE:

INTERNATIONAL CIIP HANDBOOK 2008/2009

CNI & CNII Integration



Critical National Information Infrastructure (CNII)

Information & Communications Technology (ICT)

Finance Sector	Energy & Power Sector	Transportation Sector	Water & Food Sector	Other Sectors
CNI	CNI	CNI	CNI	CNI

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

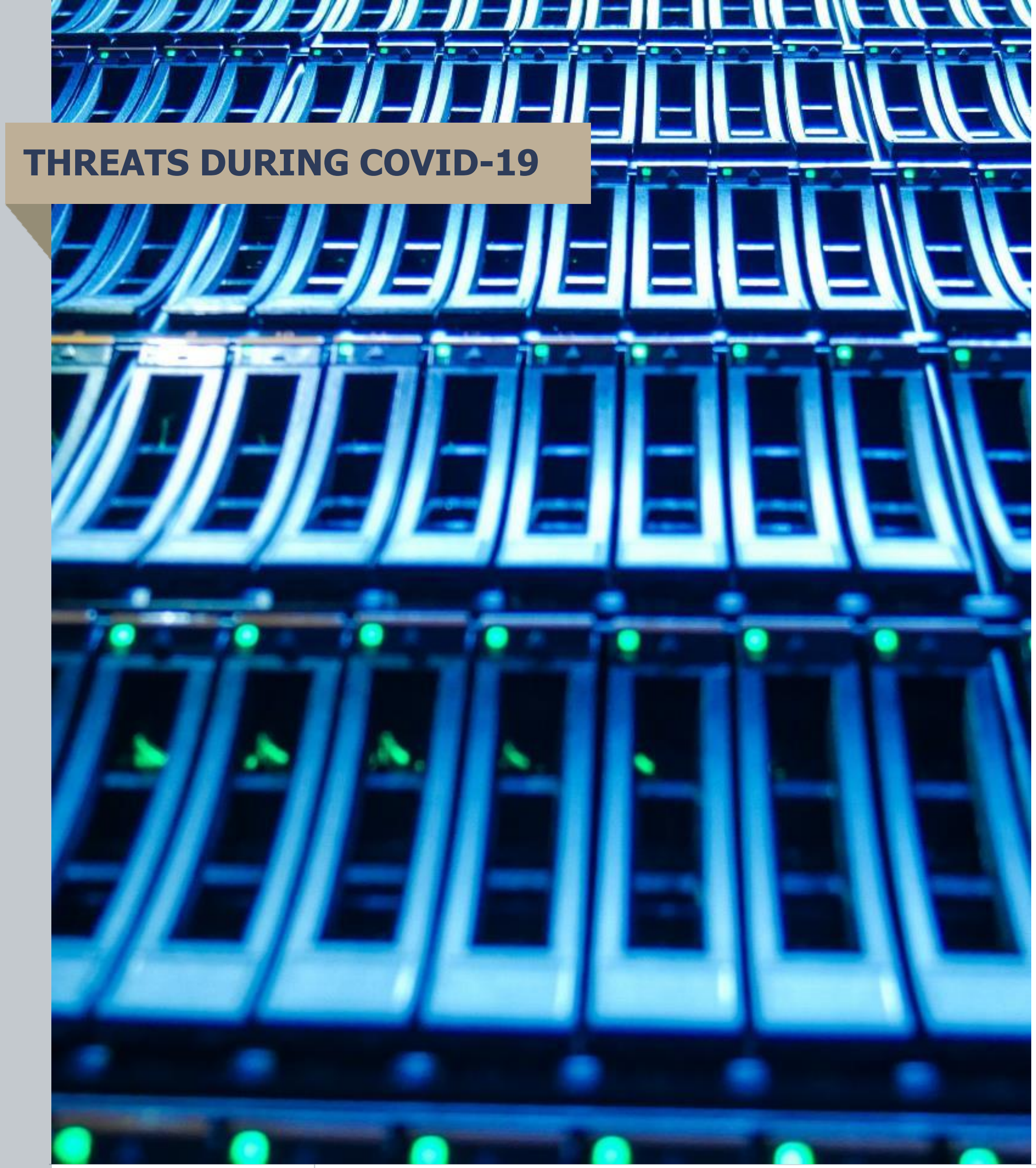
Transportation

Finance

Government

SECTION 02

THREATS AND ATTACKS ON CNII



THREATS DURING COVID-19

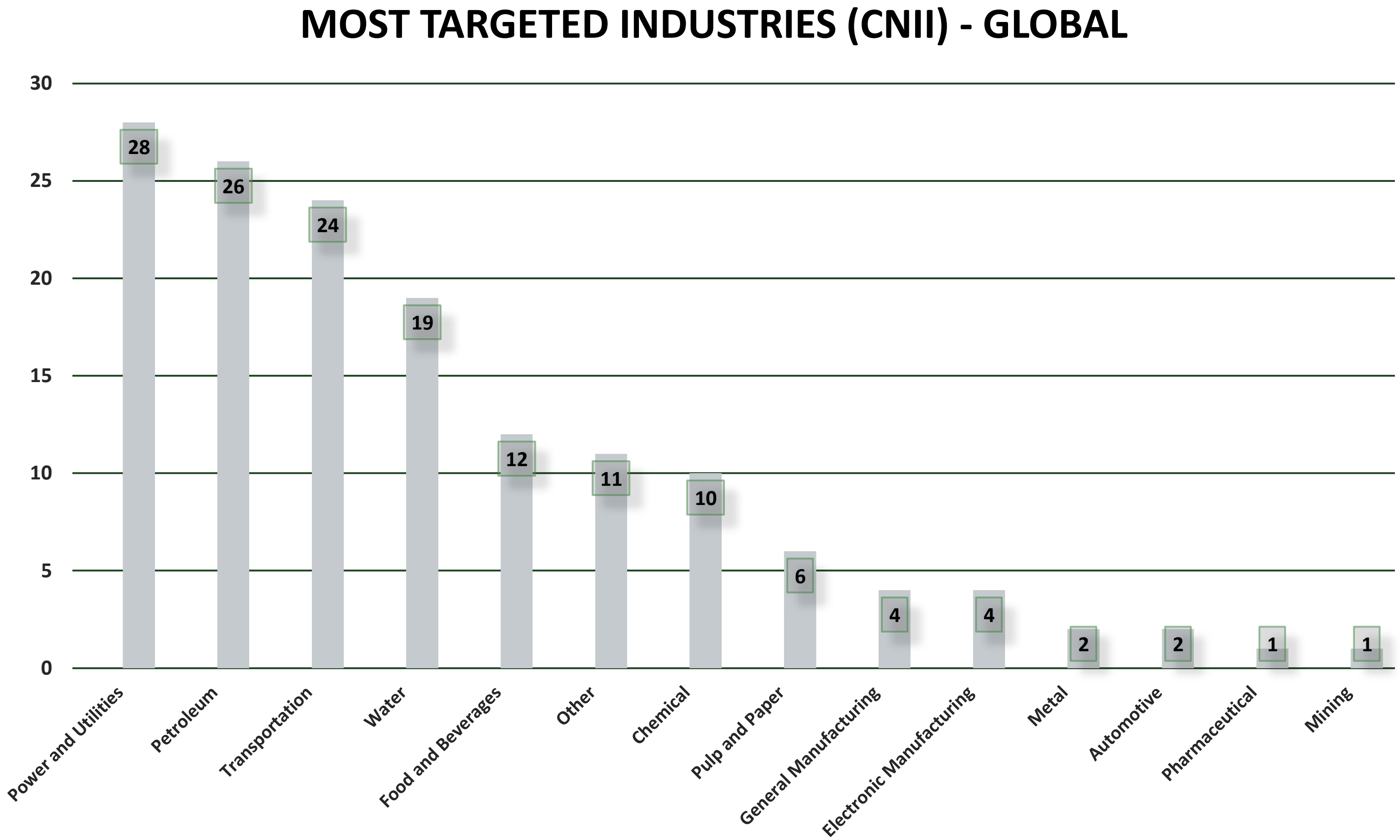
INCREASED CYBER THREATS DURING COVID-19

- ✓ 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.

THREATS AND ATTACKS

Most Targeted Industries

Global Statistics

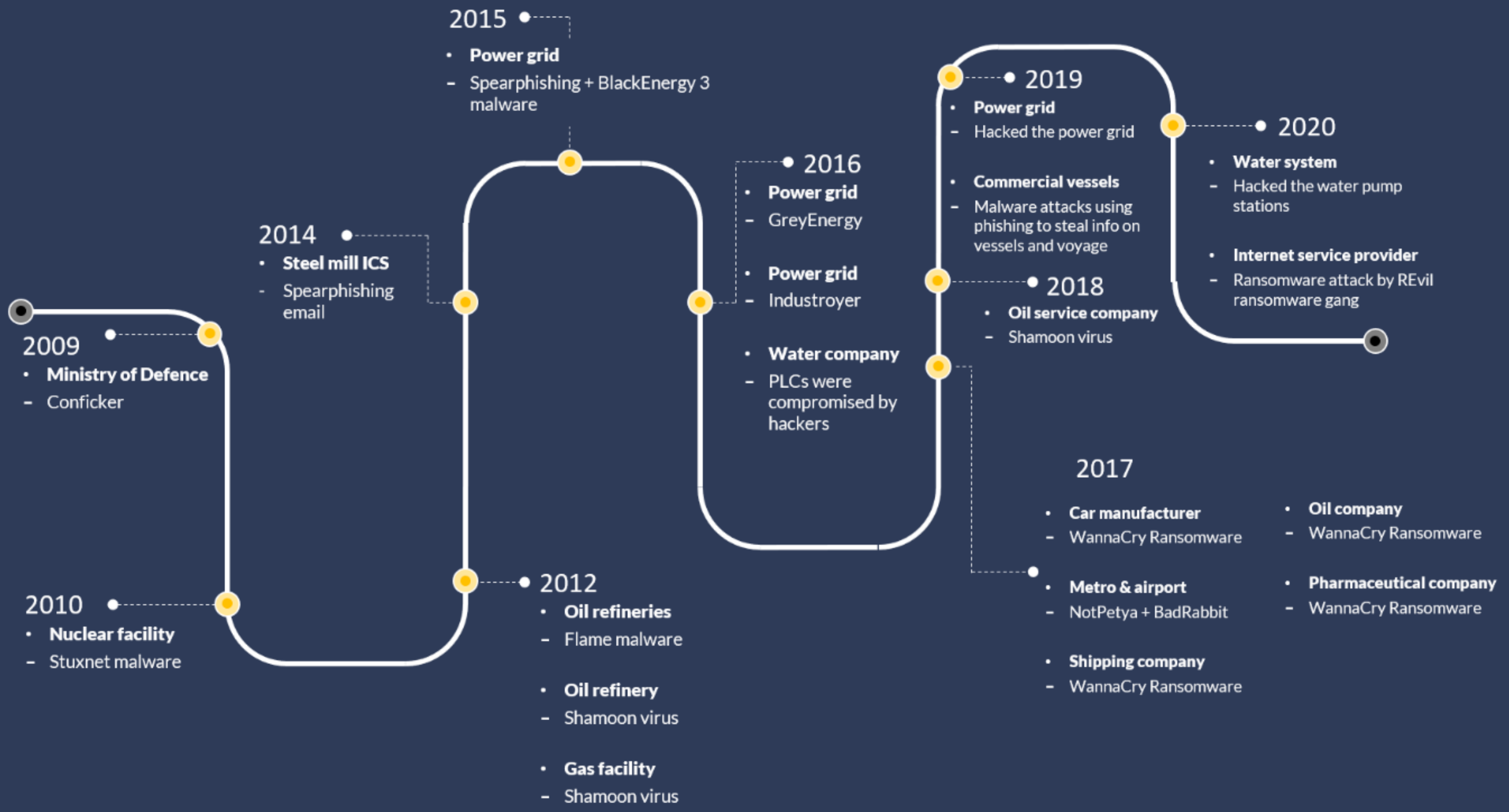


Source: https://www.lanner-america.com/critical-infrastructure/integrating-multi-layer-architectures-mitigate-cyber-vulnerabilities-oil-gas-sectors/

Wk.

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

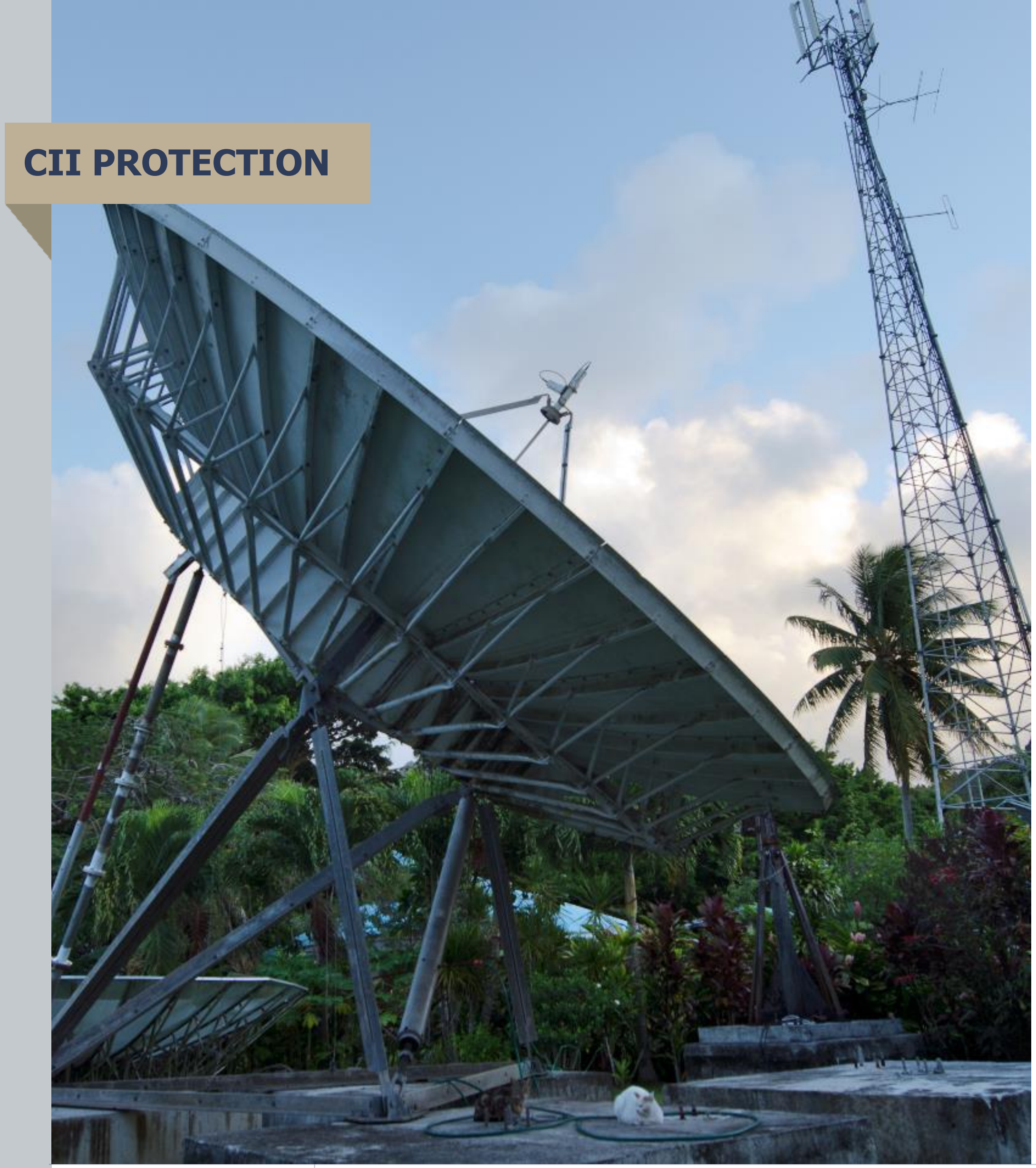
2020
- **Water system**
- Hacked the water pump stations

- **Internet service provider**
- Ransomware attack by REvil ransomware gang

Section 03

ADDRESSING THE THREATS

CII PROTECTION



CIIP for Countries

- ✓ Institutional architecture
- ✓ National risk assessment
- ✓ Identification of critical information infrastructure
- ✓ Strategies, policy, regulation and standards
- ✓ Public-private cooperation
- ✓ Education and capacity building
- ✓ Development of a trusted market
- ✓ National crisis management
- ✓ Monitoring and improvement

CIIP for Operators

- ✓ Define a risk management framework
- ✓ Build and test emergency plans
- ✓ Training and education
- ✓ Supply chain security
- ✓ Information sharing and cooperation
- ✓ Legal compliance
- ✓ Continuous monitoring and assessment of cybersecurity posture

Section 04

MOVING FORWARD

MOVING FORWARD

- ✓ **CNI should have a broader and more holistic approach and mindset in the manner cybersecurity is addressed**
- ✓ **Look beyond technical tools to adopt a new cyber defence strategy**

Section 05

WK CONTRIBUTION

CONTRIBUTION - RDF

WK CONTRIBUTION

- ✓ Whitepaper: Safeguarding Critical National Infrastructure – Risk & Opportunities
- ✓ Webinar and Training (2020– 2022) – Focusing on Small Island Developing States and Pacific Island Countries

Security Awareness Training	**Awareness Training for all employees**	**Leadership Security**
Critical National Infrastructure Training	**CNI Training**	**CNI Workshop**
CNI Sector Specific Training	**Energy, Communications, Transportation, Airport & Seaport, Emergency Services, Healthcare, etc.**	**Industrial Control Systems/SCADA**
Specialized	**Physical security, Incident Response & Handling, Policy & Intl, Cooperation**	**Risk based Approach Framework**

THANK YOU

CRITICAL INFORMATION INFRASTRUCTURE (CII)

Philip Victor – vphilip@welchmankeen.com

WELCHMAN KEEN