30 YEARS | INSTITUTE FOR SECURITY STUDIES

Maritime cyber security:

Research from Africa

Maritime cyber security

Main messages:

- The scope of what it means to be seaworthy in this new age is constantly evolving
- Maritime security is increasingly becoming dependent on cyber security, and the ability of states to protect their maritime assets and critical infrastructure against cyber-attacks
- Around 80% of South Africa's trade is seaborne. For all intends and purposes, SA can be seen as an island. We are dependent on well-functioning maritime infrastructure, which needs to be protected, including from cyber threats

Digitalisation in the maritime sector

Ports	Ships	Offshore Oil and Gas
• Paperless port system • IoT Smart Port • Automated Container Terminals • Blockchain technology • AI cargo handling process	• Electronic Chart Display and Information System (ECDIS) • Global Maritime Distress and Safety System (GMDSS) • Global Positioning System (GPS) • Remote engine and cargo control	• Dynamic positioning systems • Oil pumps • Sensors

Digitalisation in the maritime sector

- ## Qingdao Automatic Port (China)

Qingdao Automatic Port: Asia's first fully-automated port

news.cgtn.com/news/3d637a4d77594464776c6d636a4e6e62684a4856/share_p.html

New breakthroughs have been made at the container terminal in China's port city of Qingdao. It's Asia's first fully-automated port, and has set a record in terms of operation efficiency, processing more than 30 containers per hour by a single crane. CGTN's Cui Hui'ao takes a look at what this means for the future of the shipping business, and regional economic integration.

Nearly 1800 containers, handled in just 9 hours. The speed it takes to unload a cargo ship here is now the fastest in the world.

- ## Port of Busan (South Korea) – blockchain technology

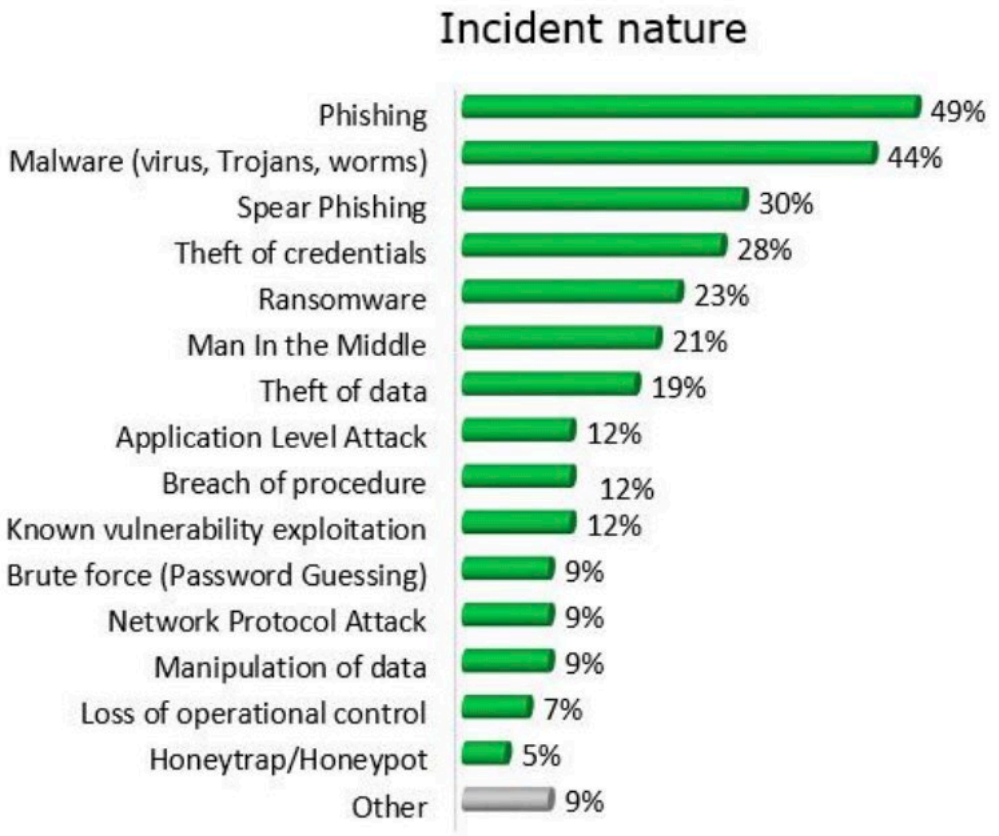
Currently, drivers use paper for container documents and have to wait at the terminal gate while it's checked. Instead, the documentation will be shared using blockchain.

One of the most significant efficiency savings relates to quantity checks which take 1 to 2 days and will become real-time using the blockchain system.

Maritime cyber security

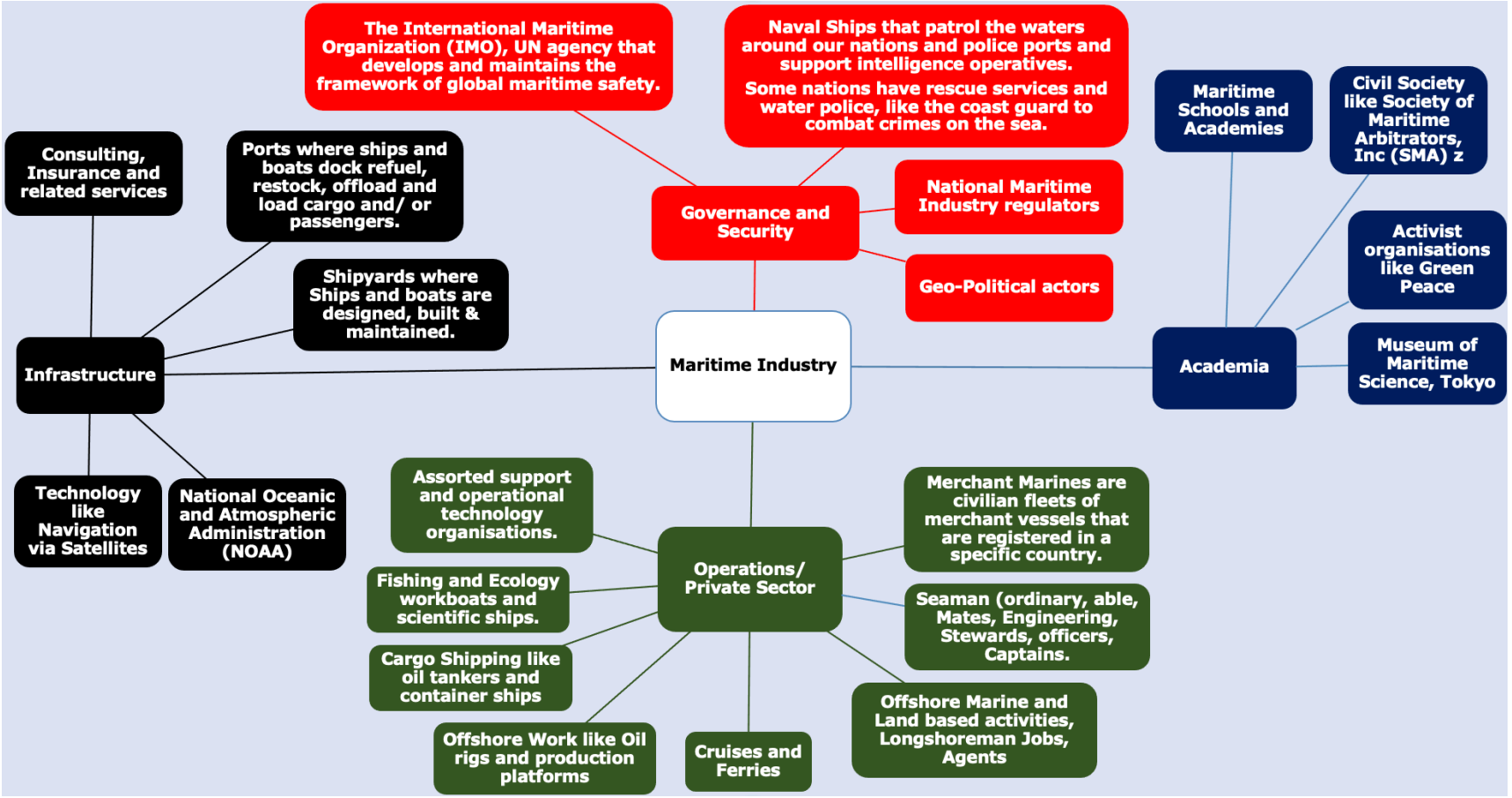
- New technologies expose the maritime sector to new cyber security risks and vulnerabilities
- Currently, only around 53 of global container terminals are automated (4% capacity), but it is an upward trend. Maritime sector is a latecomer to the digitalisation trend
- In 2020 alone, there was an alleged 400% increase in the number of incidents targeting the maritime sector around the world
- We do not know the real scope of the problem

Types of maritime cyber security incident



IHS Markit, Fairplay and BIMCO Maritime Cyber Security survey, 2018

Maritime sector



Source: Abdul-Hakeem Ajijola

Source: Abdul-Hakeem Ajijola

Maersk cyber attack (2017)

- NotPetya was a state-sponsored cyber attack in Ukraine, deliberately designed to destroy the ability to access or process data, but disguised as ransomware. Although Ukraine was the target of the attack, NotPetya was so virulent it rapidly spread affecting 1000s of companies.
- It took Maersk more than 90 days to recover from the attack
- Estimated US $350 million in damages due to the attack

- Lesson 1: Cyber environment is interconnected

- Lesson 2: Cyber environment is defined by insecurity

Other notable examples

- Port of Antwerp, Belgium (2011-2013)
  - Drug trafficking
- The Port of San Diego (2018)
  - Ransomware attack
- Shahid Rajaee attack, Iran (2020)
  - Cyber warfare

Way forward

- Africa is in a privileged position
- Risk assessment in maritime industries
- A whole-of-government approach and getting cyber experts on board as part of the process
- Cooperation between private and public sector
  - Information and coordination centers
  - National Maritime Cyber Security strategy

30 YEARS | INSTITUTE FOR SECURITY STUDIES

www.issafrica.org

@issafrica

Maritime Cyber in National Risk and Resilience

Noëlle van der Waag-Cowling SIGLA

Stellenbosch UNIVERSITY
IYUNIVESITHI
UNIVERSITEIT

Threats to Societal Security Post 2020

- An era of increasing geopolitical tension and polarization
- Accelerating climate change and habitat destruction
- Possible start to an age of pandemics
- The growth of emerging and asymmetric threats made possible by technological innovation
- Proliferation of threat actors both state and non state
- Increasing risk of strategic miscalculation

Is the contemporary security landscape different?

The Global Interconnectedness of threats and threat actors

The convergence of physical and digital threats in modern societies

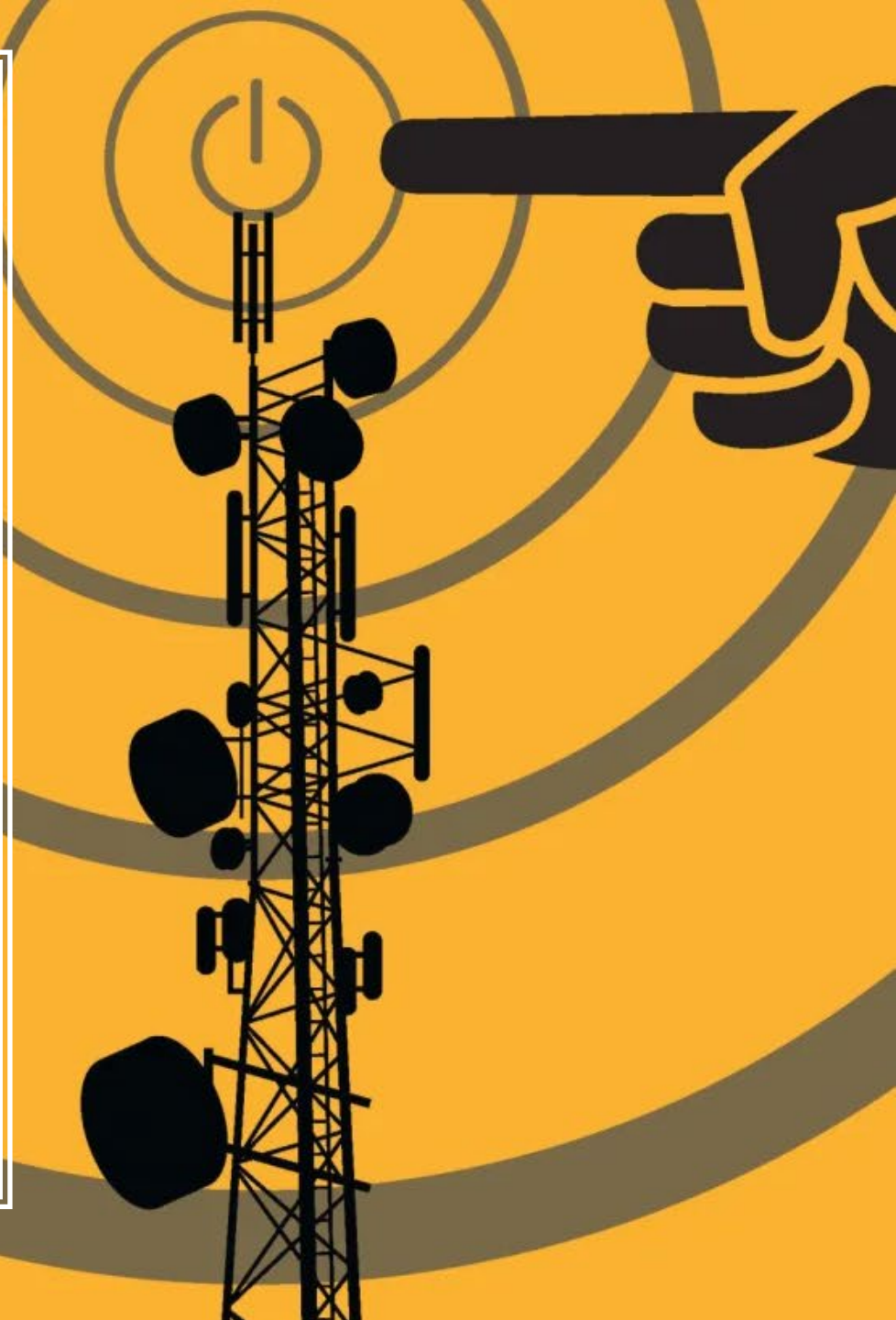
The disruptive, destabilizing and persistent nature of hybrid threats to societies

The convergence of physical and digital threats in modern societies

- This was inevitable as our physical and digital worlds merge
- A growing problem as digital technologies are increasingly interlinked with operational technologies and industrial control systems
- Further compounded by digital power concentration
- Defined by humankind’s ability to weaponize almost anything

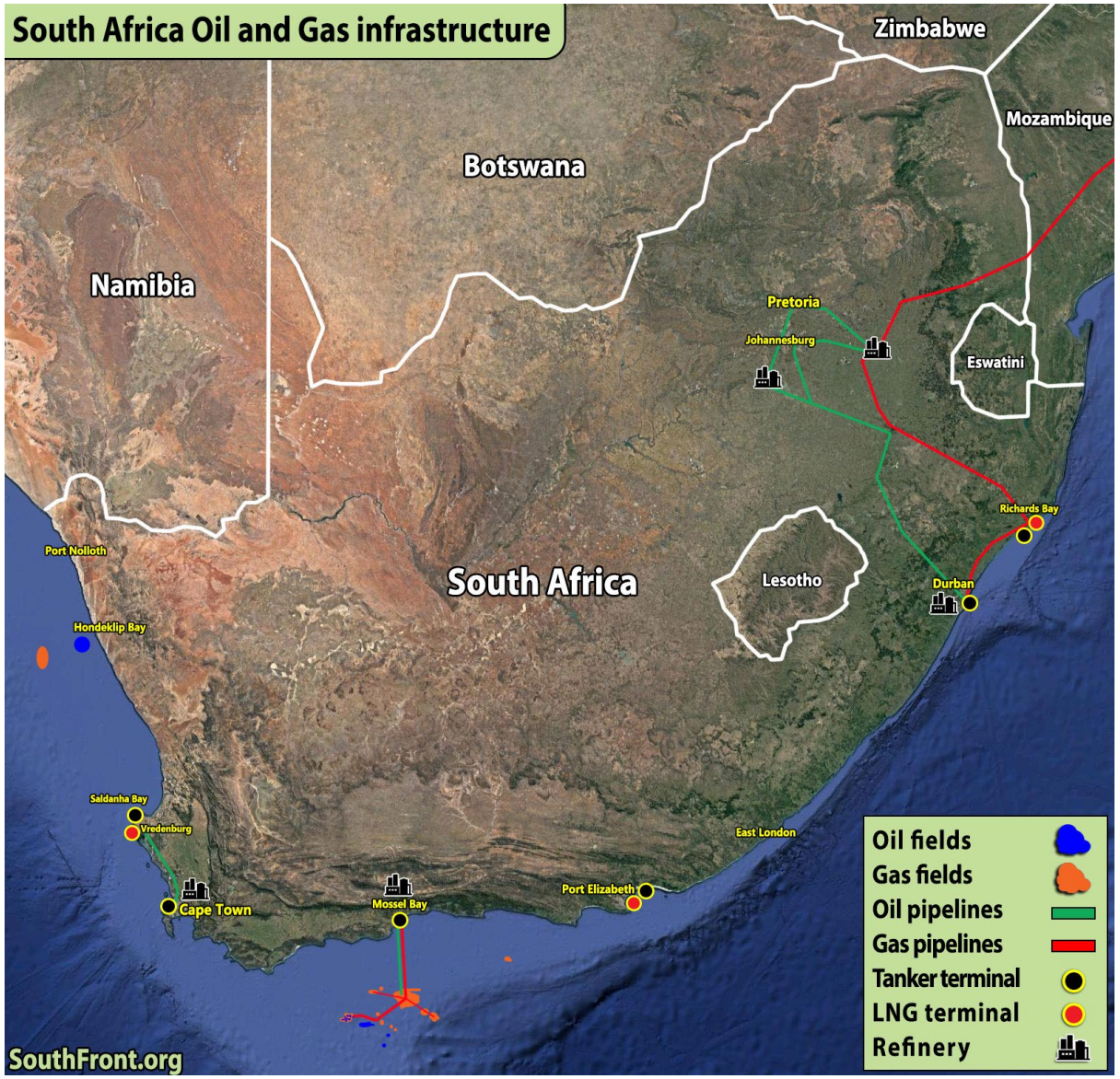
Digital Threats in an age of Insecurity

- South Africa’s maritime sector has a high degree of cyber dependency
- Cyber operations are used to disrupt and degrade operational environments
- On a national level the danger lies in the accumulation of cyber risk
- Its important to note that cyber and information operations are frequently used to augment other threat vectors



Interconnectedness means contagion

- South Africa has extremely high concentrations of risk as well as massive single points of failure
- Many elements of NCI completely controlled by Private Sector/SOEs
- Inadequate state cyber capabilities and response result in the ‘privatisation of national security risk’ phenomenon
- **The intersection of cyber security, maritime security, energy, supply chain and food security**



What do we need?

- **Accurate real time awareness of our Maritime IT Estate**
- **Multi-Stakeholder Approach**
- **Operational Maritime CSIRT**
- **Capacity Building**
- **International Standards Implementation (NIST/ISO/IMO)**

- **Business case/Security case**
- **Transition from a reactive national posture to a stable, anticipatory approach(Defend Forward)**


IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER