New Technology Threats to Smart Ports

Smart Ports all depend on using technology. But can technology also damage or even paralyse them?

David Nordell
Director
Synapse Cyber Strategy

The main vulnerability: everything is on the network and can be attacked through the network

Money is not cyber attackers' only motive

- Criminals seeking profit – typically ransom
- States using cyber as a weapon of war or conflict
- Terrorist groups, sometimes acting as proxies for states
- Espionage, whether political or business-oriented
  - Market-sensitive information and intellectual property
- Sabotage of competitors
- Politics – protest movements and other activists
- Curiosity and personal prestige
- Personal revenge

The attacker's motivation and identity don't necessarily matter

- Almost any type of successful attack on your systems, is likely to cause business disruption and financial loss
- State actors and terrorist groups may also carry out cyber attacks to earn money for future operations:
  - North Korea is believed to have hacked South Korean and other targets in order to finance acquisition of weaponry and other technology
- Ransomware or other 'normal' attacks may be carried out as cover for longer-term espionage or sabotage operations

Most of the biggest ports are in conflict zones

Top 9 container ports are in China or South & East China Seas

The whole Arabian Gulf is full of oil & gas ports

Eastern Mediterranean is now gas-rich

Offshore oil infrastructure in Black Sea

Most of Africa suffering from religious & ethnic terrorism

In all these regions, ports are tempting targets to cause economic damage

No. 1 Risk: Combination of 5G and IPv6

- 5G extends cellular wireless instead of wired Internet & optical fibre
  - Makes it easy to network every smart device regardless of location
- IPv6 massively extends address space for anything and everything connected to the network
  - Every IoT device will have it own IP address
  - Every security camera, intrusion alarm, container crane & tractor, oil control valve etc. can be monitored and controlled individually
  - Both legitimately and maliciously
- Most IoT devices supplied & installed with default passwords
- Both new technologies have known security vulnerabilities
  - New ‘unknown’ vulnerabilities being discovered all the time

So what can go wrong?

- Skilled hackers can turn off individual cellular devices or whole networks
- Redirect voice or video streams
- Create false alarms by controlling the 5G alarm channel

- Existing security tools still being updated to deal with 5G, IPv6
  - Easier to steal data unnoticed
- Most security staff not fully trained on how to configure and test new technologies

So what about Huawei?

- Huawei has near-monopoly position in 5G market, for both handsets and network equipment
- Ericsson & Nokia was behind in market share, more expensive
- Company must by Chinese law act in accordance with government (Communist Party) directives
- Back doors have been discovered in past; can be exploited by hackers as well as Chinese intelligence or proxy actors
- British government pushing back against US ban on Huawei
  - MI5 says no significant threat to national security; GCHQ a little less sure
  - Both intelligence agencies being less than frank, for political reasons

Is this just my (or Trump's) personal paranoia?

"Among the various potential actors, non-EU states or state-backed [actors] are considered as the most serious ones and the most likely to target 5G networks."

"In this context of increased exposure to attacks facilitated by suppliers, the risk profile of individual suppliers will become particularly important, including the likelihood of the supplier being subject to interference from a non-EU country."

Joint statement by EU and Finland, October 2019

But how about using the news as a cyber weapon?

Thank you for your attention

David Nordell

Director

Synapse Cyber Strategy

david@synapse-cyberstrategy.com

+44 (79) 8879-2163