Shipping is so insecure we could have driven off in an oil rig

Not many stranger things happen at sea

By Gareth Corfield 18 Feb 2020 at 16:45

Penetration testers looking at commercial shipping and oil rigs discovered a litany of security blunders and vulnerabilities – including one set that would have let them take full control of a rig at sea.
5G & Cyber-Security

User experience and learnings from other “silos” for Smart Ports
Before we begin… Background – in 3 points

1. Post Samsung, led UK Government 5G R&D programme “phase 0” – looking at urban high frequency radio propagation tools

2. We met during a later phase of the 5G Test-bed and Trials programme, exploring how to actually deliver rural areas with 5G secure spectrum services on a project called “5G RuralFirst”

3. We now advise on commercial 5G spectrum and security deployment, bringing knowledge from other industry “silos”
Funded by

Department for Digital, Culture, Media & Sport

5G RuralFirst
We get (former) Ministerial attention!

Image:
The Chancellor 10th September 2018 in Strathclyde University
And (current) international recognition

- DSA Award for Increasing Digital Inclusion – Washington DC, 26th June 2019
From 5GRF to 5GRD!

- We started at a port!
- We have their backing...
- Plus some other “names” you might recognise too!
5G RuralDorset

DCMS 5GTTT Winner - Announced Today!
Why 5G? Why Security?

The “why/why not” for 5G is irrelevant – We’re getting it anyway! This makes the case for 5G security by default overwhelming.

We will:
1. Consider the UK’s need for effectively connected ports
2. Share some recent user experiences and learnings in today’s world – as we prepare for tomorrow’s
3. Look at the policy backdrop and CNI – including freeports
4. Consider – what next?
The UK depends on Imports
Including food...

This Matters
1. The need for effectively connected ports
### 2018 UK Freight Export (k ton)

- Forth (Scotland) = 21,996 k ton
- Tees & Hartlepool = 16,802 k ton
- Grimsby & Immingham = 13,951 k ton
- Southampton = 12,332 k ton
- Milford Haven (Wales) = 11,708 k ton
- Felixstowe = 11,527 k ton
- Dover = 10,058 k ton

### 2018 UK Freight Import (k ton)

- London = 44,771 k ton
- Grimsby & Immingham = 41,666 k ton
- Liverpool = 24,123 k ton
- Southampton = 22,137 k ton
- Milford Haven (Wales) = 19,228 k ton
- Felixstowe = 16,740 k ton
- Dover = 14,885 k ton
UK PSTN switch off date already set
5G is coming to Ports – Did you know?

1. 5G is the Martini service “anytime, any place, anywhere”
2. Integrated fixed and mobile – super bandwidths
3. More “software dependent” then ever – new security risks!
4. ....So guess what’s going to happen next?

Are you ready for this yet? If not start now
2. Some recent experiences and learnings in today’s world
User Experience and Learnings
An Example

No mobile service & no power

“Not expected!”
O2’s All-Day Outage Caused Havoc in Ways Consumers Didn’t Expect

By Nate Lanxon
8 December 2018, 10:12 GMT  Updated on 10 December 2018, 09:31 GMT

London’s bus riders left in the dark about schedule delays
Software-failure impact spread far beyond cell-phone users.

When the U.K.’s second-biggest cell-phone network went down Thursday, it struck transit riders, workers in the gig economy, small businesses and the self-employed.

Among the victims of Telefonica SA-owned O2’s widespread data outage were commuters hoping to use their smartphones to find when the next bus was due. The systems on board all 8,500 London buses, which send live location data back to the city’s transit authority and third-party mapping services, were knocked offline.

Power cut and downpours bring ‘apocalypse’ to streets

For many, the two hours of mayhem caused by Friday evening’s power cuts created scenes reminiscent of a darkly apocalyptic Hollywood film.

Trains rolled to a halt and traffic lights flickered before going blank, leaving drivers second guessing one another on major junctions.

Mobile phone and internet reception went dead as communications masts apparently lost power.
User Experience and Learnings
An Example

No mobile service & no power

1. Reliance on non Critical National Infrastructure v cost?
2. Is this collateral damage an insurable risk?
3. Productivity loss – trucks (ships) can’t unload themselves
User Experience and Learnings
An Example

Travelex

“How not expected!”
24 Jan!!!
User Experience and Learnings
An Example

Travelex

1. What is your disaster recovery plan? “red teamed?” yearly?
2. What inter-industry/gov. cyber collaboration in place?
3. Do you understand your full supply chain?
User Experience and Learnings
An Example

Road Infrastructure

“Not expected!”
User Experience and Learnings
An Example

Road Infrastructure

1. What impact if the “smart city” en-route to port got hacked?
2. Are you engaged with planning beyond the perimeter fence?
3. Can you do just-in-time delay or re-routing cargo in transit?
User Experience and Learnings
An Example
Shipping Industry

“Complete equipment loss”
NotPetya attack totally destroyed Maersk’s computer network: Chairman

Maersk Chairman Jim Hagemann Snabe said while participating on a cybersecurity panel at the conference that his company replaced 45,000 PCs, 4,000 servers and install 2,500 applications. The computer system runs an operation where a ship carrying 20,000 containers enters a port every 15 minutes somewhere around the world. Overall, Maersk handles 20 percent of all world trade, he said.

“We found we had to reinstall our entire infrastructure. It was done in a heroic effort in just 10 days,” he said, adding such a job should take about six months to complete.

A shipping company suffered a ransomware attack that affected certain network systems in one of its regions of operation.

On 25 July, COSCO Shipping Lines disclosed on Facebook that it had suffered a “local network breakdown” in the Americas. The company, which is owned and operated by the Chinese government, said that the incident degraded local email and network telephone services but not its main business operations, including the functionality of all its vessels. COSCO decided to suspend certain connections with other regions out of an abundance of caution.

The shipping giant had not directly revealed the source of the event at the time of publication. But it did retweet a tweet from The Modern Times of LB (Long Beach) attributing the network issues to a ransomware attack.
User Experience and Learnings
An Example

Shipping industry

1. Maersk did brilliantly! 45,000 PCs... 10 days... could you?
2. Do you do threat horizon scanning & report this to Board?
3. What is an “adequately” resourced cyber team?
5G – what it means for transport

1. The Internet of Things means everything is connected to everything
2. Whether on land, sea or air, everything is changing
3. 5G simply multiplies an effect that is already happening throughout all of your operations already – massively

Everything is not just “connected” but “interdependent“ - nearly
Coronavirus: Jaguar Land Rover 'shipping parts in suitcases'

Jaguar Land Rover has flown in parts in suitcases as the effects of coronavirus take a toll on the carmaker's supply chain.

It said it could start to run out of Chinese parts for its UK factories after two weeks.

The virus has killed more than 1,800 people in China sparking a shutdown that has seen factories close across the country.

That is having an impact on global supply chains.
3. **Shipping + Ports = CNI?**
The Policy Dimension
The critical security question is: how to mitigate such vulnerabilities and stop them damaging the British people and our economy?

For 5G and full fibre networks, the Review concluded that, based on the current position of the UK market, high risk vendors should be:

- first of all, **excluded from all safety related and safety critical networks** in Critical National Infrastructure
- secondly, excluded from security critical network functions
- and thirdly, limited to a minority presence in other network functions up to a cap of 35%.

And be subjected to tight restrictions, including **exclusions from sensitive geographic locations**.
DCMS 5GTT – and the Supply Chain

1. From factory or farm
2. To land transport
3. To port A
4. To Loading
5. To Voyage
6. To port B
7. To land transport
8. To destination

Industry 4.0 & 5G Rural First
Autoair (road)
5G RuralDorset (“5GRD”)—Port A
Not yet addressed/5GRD2
5GRD (satellite)...part—Port B
Wales?/You? Ask us!
Rail (Transpennine, Oxf-Cam)
Various

5G Impact – DCMS 5G Test-bed programmes incl. future ones (in italics)
Public Mobile (& Telecoms) networks are not covered by the NIS Directive!

BUT Shipping is CNI in UK

2002 Framework Directive outdated
- has considerably lower penalties
- was written in 2002, as name suggests
- Does not feature the word “cyber”

### UK NIS Implementation definitions of CNI

<table>
<thead>
<tr>
<th>Water Transport Operator</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shipping company</td>
<td>&gt; 5 million tonnes annual freight</td>
</tr>
<tr>
<td>(or)</td>
<td>&gt;30% freight any one major port*</td>
</tr>
<tr>
<td>Harbour Authority</td>
<td>&gt;10m pax annually</td>
</tr>
<tr>
<td>(or)</td>
<td>Is a major port*</td>
</tr>
<tr>
<td>Port Facility Operator</td>
<td>&gt;10m pax annually</td>
</tr>
<tr>
<td>(or)</td>
<td>Is a major port*</td>
</tr>
<tr>
<td>Vessel Traffic Services Operator</td>
<td>&gt;10m pax annually</td>
</tr>
<tr>
<td></td>
<td>Operates at a major port*</td>
</tr>
</tbody>
</table>

### Definition

- *Major Port*
  - >15% total RORO traffic in UK
  - >15% total LILO traffic in UK
  - >10% total liquid bulk in UK
  - >20% total biomass fuel traffic
Opportunities for new thinking
And cooperation
So...
4. What is likely to happen? And what you can do? (3 scenarios)
Course 1 – Wait and Hope

Viable but not prudent
Course 2 – Panic!

Looks a lot like course 1, but with shouting and screaming due to less optimism!
Private ?
Secure ✓

KEEP CALM AND BUILD A 5G NETWORK
Key Take-homes
1. It takes 2 (ports) to tango

- Siloed innovation in ports can give us some benefits, but every ship moves from one port to another
- Closer collaboration is commonsense
2. Interoperability = Competitive Advantage

- 23,000 TEUs of containers arriving at a port in 1 ship – customs, logistics
- Interoperability between port of origin/destination gives efficiencies! (But will the equipment used???)
- These can give your port or operator a key competitive advantage over rivals
3. Public Telco & MNO networks are **NOT CNI grade**

- Not suitable for use in CNI, and not rated as such. Also not held to same standards of NIS Directive as shipping already is!
- As NIS’d CNI, *you bear the risk* of their failure, breach or compromise...
- Private Networks may be an option to consider
4. Spectrum policy means the time to consider private networks is here – 5G

- Manage and control **your** vendor/supply chain risk **yourself**. Many ways to do so. [Know what you buy](#)
- Gain guaranteed QoS, define your own power resilience requirements
- Will struggle to run safety-related use-cases over public networks – drones?
‘No thank you’

Anarchy in the UK
Dave Happy
MD Telint Ltd
(Former VP - Samsung R&D)
MD@Telint.biz

Dr Greig Paul
Lead Mobile Networks & Security Engineer
Telecoms/Mobile/Spectrum consultant
greig@mno.ninja