# Consent Form for Interview

# Project Firefly

**Research Invitation?**

Global intelligence and information reports a rapidly emerging security and safety risk threatening Maritime Ports and Shipping with the ability to cause serious harm to current security systems and shut down critical safety functions that could lead to catastrophic failures.

You are invited to take part in an independent research study on security and safety in a maritime setting. With your help and in **complete confidence** I hope to present a clear intelligence picture that might support your enterprise to correctly and accurately assess your own vulnerability. My report once published will be presented to the MCA for wider distribution in the interests of protecting people from harm.

Principal Investigator: David J Sanderson (Independent)
Telephone: 07713880085
Email address: david.sanderson@myport.ac.uk
Title of Project: ***"What are the threat, harm and risks to the Maritime Industry from the criminal exploitation of the electromagnetic spectrum radio frequency range?"***

**Background information should this be of interest to you or skip to the consent field**

A criminal denial of service attack is likely to have a significant impact on maritime safety, security and operations. This could lead to a loss of customer/industry confidence, reputational damage, potentially severe financial losses or penalties, and litigation affecting those companies involved. But importantly it could lead to physical harm to the system, the shipboard personnel or cargo and in the worst case scenario, could lead to a risk to life and/or the loss of the ship.

Let's consider the following scenario;

An organised criminal gang from a location in Kent steal a Bentley motor car with an approximate value of £130.000.

Concerned that the vehicle and or the gang might be subject to wireless tracking/ monitoring the gang place a radio frequency jamming device inside a small brief case and place this inside the boot of their vehicle. The jammer is powerful and is set to disrupt 8 common radio frequencies. This includes Wifi, Bluetooth, GPS, G3 and others.

The vehicle is driven along the strategic road network where they arrange for the vehicle to be packaged inside a shipping container in an industrial estate in central London.

The container is then transported on board an articulated commercial heavy good vehicle and driven to a major seaport, part of the UK's national critical infrastructure. On arrival at the Port the container is placed into holding, where it is then lifted by straddle carrier and placed within the secure compound imbedded with thousands of others. Seven days later the container is lifted from the compound by straddle carrier and placed according to the loading instructions on top of a container ship of the E-class. The vessel sets sail on route to Monrovia in Liberia West Africa, through some of the busiest navigable global waters. The vehicle is to be sold for £25,000 to an official.

How much does your organisation rely on wireless systems and what are the threats, harm and risks to Critical Maritime Infrastructure from criminals whom might choose to exploit the internet of things within maritime operations, intentionally or un-intentionally?

## Consent field

**Please initial box**

- I confirm that I have read and understand the information sheet dated. for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.

- I understand that my participation is voluntary and that I am free to withdraw at any time without giving any reason, (you might wish to add a constraint here- e.g. up to the point when the data are analysed)

- I agree to my interview being audio / video recorded

- I agree to being quoted verbatim

- I agree to the data I contribute being retained for future research

- I understand that data collected during the study, may be looked at by individuals from [company name / University etc)], or from regulatory authorities. I give permission for these individuals to have access to my data.

- I agree to take part in the above study.

Name of Participant: Date: Signature:

Name of Person taking consent : Date: Signature:

When completed: 1 for participant; 1 for researcher ‘s file;

# Interview questions for Maritime Professional

***“What are the threat, harm and risks to the Maritime Industry from the criminal exploitation of the electromagnetic spectrum radio frequency range?”***

**Information in brief**

The Internet of Things (IoT) concept is based on the realisation that almost any electro-mechanical device from a fridge in the galley to an engine management system in the hull to the integrated bridge system can be fitted with wireless microprocessors and data links. Together these enable remote communication either through the mobile network, Wi-Fi or via a physical connection. Information and commands relating to everything from maintenance and replenishment to alerts and avoidance can then be exchanged and acted upon with minimal human interaction.

Today many efficiencies are so very attractive that they are becoming part of our

everyday life. Businesses can gain a competitive advantage by embracing this connectivity underpinning the IoT and integrating digital services into their products to keep pace with the next wave of innovation.

Issues such as compatibility, security, privacy and control continue to generate much discussion. A denial of service is likely to have a significant impact on maritime safety, security and operations. How much does your organisation rely on wireless systems and what are the threat, harm and risks to Critical Maritime Infrastructure from criminals whom might choose to exploit the internet of things with maritime operations or intentionally or un-intentionally.

## Questions

- What is your role and responsibility? Are you still in post as
- Have you received formal advice on the use of Global Navigational Satellites (GNSS) and dependency within your sector, from either NCSC, CPNI or other Government Agencies?
- Do you specifically identify loss of space-based position navigation and timing (PNT), (GNSS), in your risk register(s) or business continuity plan?
- Throughout your systems, please identify your use cases of position and/or time information using GNSS. E. G:
    - Field/remote workers using navigation equipment, and systems for personnel and asset monitoring/tracking;
    - SCADA (remote monitoring) systems at remote sites and within control centres;
    - Computer network equipment and timing systems;
- Are you aware of your ability (in hours/days) to continue to provide operational services meeting your contractual obligations, in the absence of space-based PNT (e.g GPS)
    - i.e. how long can your systems remain in specification without GPS?
- Do you provide guidance to your procurement function to specify measures associated with system resilience (Availability, Integrity, Continuity, Accuracy) when procuring equipment used to deliver services to meet your contractual obligations?
- Look at these picture?

- Do you know what these devices are and what they can be used for? Please explain?

- Describe your organisations level of knowledge regarding the denial of GNSS system availability. Specifically, a denial of services attacks from radio frequency jamming/suppression and spoofing?

- How does your organisation monitor and record adverse radio frequency events?

- Has your organisation or an organisation for which you have knowledge of ever been affected by an adverse radio frequency spoofing or jamming/suppression event? If yes how was this investigated and what was the outcome.

- How resilient were/are your/their organisations responses to such an event
- Was this attack reported beyond your organisation? For example, Ofcom, MCA, security, law enforcement. If this was not reported, can you explain why?

- How would you describe your vulnerability to a future attack?

- In your opinion considering the responsibilities of business, government and academia to manage cyber risks how would you describe their roles in managing future resilience?

- Having under taken this survey do you have any concerns regarding your organisations response to jamming/suppression and spoofing events? Please explain your answer.