Cyber-risks in maritime container terminals: Analysis of threats and simulation of impacts

Abstract

Container Terminals (CTs) are the transportation nodes at which containerised freight is transshipped between ships and overland transport. CTs are a vital element of a country's transportation infrastructure and in the UK they are classed as part of the country's Critical National Infrastructure (CNI).

This article explains the dependence of modern CTs on Information and Communications Technology (ICT) and suggests that this dependence may pose a greater threat to CT operations than it does to other comparable elements of CNI. This opinion is formed by examining the cyber-based threat-actors who may be motivated to disrupt CT operations and the vulnerabilities that they may seek to exploit.

Finally, the article demonstrates how the impact of cyber-attacks against CTs can be modelled using Discrete Event Simulation (DES) techniques. It is suggested that the outputs from these simulations could be used to identify and prioritise vulnerabilities at CTs and to support justifications for investment in new and improved control measures.

The modern container terminal

Shipping currently accounts for the movement of approximately 90% of world trade and Container Terminals (CTs) are instrumental in this endeavour. Recent trends in CT operating models have resulted in the development of ever larger facilities which act as regional hubs for intermodal freight distribution. The result of this trend is that the largest CTs have become increasingly central to global supply chains. The corollary is that they present an increased risk to these supply chains if their operations are disrupted.

As the global economy has expanded the volume of freight being shipped has increased accordingly. CTs have had to transform in recent years to achieve the throughputs required to support globalisation. This transformation has been heavily reliant upon ICT.

Figure 1 illustrates a typical CT and shows the stages through which containers flow as part of the transhipment process. (The word “section” refers to specific areas of the container yard.) The process sequence remains much the same today as it did in the earliest days of CTs in the 1960s. However, the equipment and technology employed at each of these stages has changed dramatically and today's CTs are now heavily automated. Two of the most significant developments in CT operations are described below.

1. Automation of Mechanical Handling Equipment (MHE). Modern CTs employ automated systems in every stage of the transhipment process. Semi and fully automated quay-side cranes, yard cranes and Automated Guided Vehicles (AGVs) are commonly used to unload, stack and move containers. The operational benefits of automated equipment, when compared to manually
Figure 1: Loading and unloading processes of containers at a typical container terminal.

operated MHE, are clear: they have shorter cycle times, wider operating windows (in terms of weather conditions and hours worked) and lower error rates.

Automation relies on the use of Industrial Control Systems (ICS) to manage the operation of MHE. These ICSs consist of complex networks of sensors and actuators which are integrated with MHE assemblies so that cranes and vehicles can undertake tasks autonomously. There is also a requirement for robust data network links between MHE and control rooms, these links provide a command and control channel and carry a near constant stream of data relating to tasking instructions and situation reporting.

Whilst the operational benefits of automation are evident, and much heralded, there has been much less discussion about the vulnerabilities it presents. MHE ICS and their associated network links are subject to the same risks that affect other ICS systems and general data networks. Evidence of the seriousness of these vulnerabilities can be seen in the STUXNET attack. MHE control systems and network links need to be suitably hardened to control these risks. Failure to do so leaves them over-exposed to cyber-threats.

2. The employment of Terminal Operating Systems. The intelligent movement of containers throughout the transhipment process has reduced double handling (non-productive container moves) and optimised process flow. This has been achieved through the use of intelligent planning and system integration tools that are known as Terminal Operating Systems (TOS). TOS software sequences container movements and plans storage in order to maximise the utilisation factor of MHE and to ensure that containers are placed on stacking yards in a manner that is appropriate for their collection time and mode of onward transportation. TOSs are able to achieve far higher container throughput than could be achieved by manual planning.

TOS software relies on the accurate identification of containers via Optical Character Recognition and RFID technology, and on the integrity and availability of the planning data that is held on central databases. Any loss, corruption or malicious modification of this data could prevent containers from being located within the CT or could result in containers being shipped to the wrong locations. This risk is not merely theoretical: criminal gangs operating around a major European CT were found to be using similar techniques to mask smuggling operations. The networks that host TOS data and communications need to be hardened in order to protect confidentiality, integrity and availability. Failure to do so leaves a CT exposed to the loss of TOS functionality.

In summary: the modern CT has evolved from a largely manual transhipment process in the 1960s, to a highly automated process today. This automation has delivered significant operational benefits but has also exposed CTs to cyber-based threats which could pose serious risks to operations.
When considering cyber-based threats to CTs it is necessary to identify those groups or individuals who may be motivated to disrupt a CT’s operation. The UK’s Cyber Security Strategy identifies 4 generic categories of threat-actor which may be motivated to harm a nation’s interests through malicious activity in cyber-space. These categories are: criminals, states, terrorists and hacktivists. Each of these threat-actor categories have different motivations, aims and capabilities and must be considered independently when it comes to identifying likely threat vectors. Table 1 provides an overview of the characteristics of each of the 4 threat-actor classifications and suggests possible motivations for them to conduct cyber-attacks against CTs. It also includes a fifth category - the insider - for the purpose of analysing the threat-actors relevant to CTs. CTs are particularly susceptible to the insider threat as they are often large, multi-occupancy sites which are difficult to physically secure. The result of this is that there are many ‘insiders’ able to move relatively freely around CTs.

It is reasonable to assume that facilities of strategic national importance which present opportunities to all categories of cyber-threat will at some point be subject to cyber-attack, whether overtly or covertly. Consequently, the issue of cyber-security at CTs, and ports in general, needs to be taken seriously.

The vulnerabilities

In order to successfully disrupt a CT a malicious actor will seek to exploit a vulnerability. The nature of the vulnerability will depend upon the attacker's technical ability, location and intent. Vulnerabilities provide the means by which an attacker will gain access to, and move within, the network and also by which they will exploit systems in order to achieve their goals.
There are a combination of generic factors which are peculiar to the CT context. These factors are likely to result in CTs being at a higher risk of cyber-attack relative to other elements of a country’s CNI. These factors are: the relative lack of a cyber-security culture in the companies that own and operate CTs, the difficulty in physically securing CTs, the high degree of centrality of CTs as nodes in the shipping network, and the very rapid adoption of automation in recent years.

1. **Inadequate cyber-security culture.** The security culture at ports has evolved to meet the predominant threats. Historically those threats have been smuggling and theft. Several commentators, including the US coastguard, have argued that ports authorities have been very slow to recognise and take account of the relatively recent emergence of cyber-threat. Evidence of continued high levels of investment in physical security relative to cyber-security measures at ports supports this assertion.

   This tendency is in contrast to other CNI sectors such as the power industry and banking which have long been conscious of cyber-threat and, although far from perfect, have tended to deploy ICT in a manner which has taken account of the associated risks. The result is that CTs could be considered to be ‘soft’ targets relative to other sectors of CNI - soft targets present ‘low hanging fruit’ to would-be attackers.

2. **Geographical and physical security of CT sites.** Typically, CTs are large sites on which a number of discrete organisations operate as a port-community. The community is often served by an extensive site-wide WAN which is carried long distances on structured cabling and/or WiFi and is often maintained and operated by several different organisations. Securing a WAN under these conditions is difficult and this can lead to the possibility of inadequately secured network access points that could be exploited by insiders.

3. **High degree of centrality in the shipping network.** CTs are critical nodes and are often highly central to the transportation networks of which they are a part. The result is that regional and international transportation network resilience is often low as it is highly dependent on a small number of key nodes.

   As with most CNI assets the most serious consequence of a cyber-attack would be the loss of availability of data and equipment. Such loss would mean that CT operators were unable to ‘see’ and control automated equipment over their networks and operations would be disrupted. Causing denial of service of equipment in this manner is a relatively simple objective for an attacker to achieve. Methods to achieve it include launching cyber-based Denial of Service (DOS) attacks, sabotaging network infrastructure and jamming WiFi signals. Hence, from the attacker’s perspective, the ‘barrier to success’ is set relatively low.

4. **Rapid adoption of ICT in recent years.** It is common for expensive equipment such as cranes and AGVs to receive technology refreshes during their operational lifetime. A refresh, or mid-life upgrade, aims to enhance equipment capabilities by upgrading assemblies and incorporating new technologies. Control systems upgrades have been very common for equipment at CTs in recent years. Unfortunately, it has often been the case that the investment in ICS has not been accompanied by investment in the legacy network ICT infrastructure to safely support it. Examples include failure to partition enterprise and ICS networks, failure to update firewalls and failure to update Information Security Management Systems to take account of new equipment.

These factors, which are commonly occurring across many CTs worldwide, are frequently implicated in poor CT cyber-security and could lead to exploitable vulnerabilities.

**Impact modelling**

The case has been made that CTs are likely to present attractive and potentially vulnerable targets to the full range of cyber-based threat actors. If this finding were to be accepted by CT operators the logical response would be to implement control measures in order to reduce vulnerabilities. Modelling and quantifying the impact of the risks faced by insecure CTs is a useful means of justifying the financial...
investment that CT operators must make to reduce vulnerabilities. The following paragraphs describe how Discrete Event Simulation (DES) can be used to model the impact of cyber-based attacks against CTs.

DES uses a system of event scheduling and calendar sequencing to calculate the movement of entities through a process. In the case of CT modelling these entities represent containers. DES simulates the passage of entities from one stage of a process to the next and limits the capacity of the process based upon the availability of resources. In the case of CT modelling the resources are MHE and storage space. DES models of real-world CTs can be constructed by setting model parameters to match those of real facilities. These parameters include: the quantity and pattern of container inflow, the quantity of MHE, and the cycle times of key equipment.

DES enables the effect of cyber-attacks to be modelled in terms of reductions in the availability of resources (which could be achieved in a real attack by remotely disabling equipment) and by increases to the duration of each activity (which could be achieved in a real attack by modifying ICS control parameters in order to increase cycle times).

By modelling the throughput of containers under both normal and abnormal (simulated cyber-attack) conditions it is possible to quantify the impact of a range of cyber-based attacks. Dependent upon the nature of the attack these effects could range from a marginal reduction in container throughput to complete disruption of a CT operation. Figures 2 and 3 are copies of plots taken from the simulation of an attack against a fictitious CT. They demonstrate the type of information that can be provided through DES simulation. Figure 2 shows the fluctuation in the number of containers (described as the occupancy rate) stored on a CT yard under normal operating conditions over a 7-day period - under normal conditions the occupancy rate remains within acceptable limits. Figure 3 shows the number of containers which would be stored on the yard in the event of a cyber-attack which successfully disabled a yard crane. In this case the occupancy rates continues to grow as the crane that has been disabled is an off-loading crane responsible for moving containers off the yard onto overland transport. This situation presents a threat to CT operations as the yard will be unable to accept any further inflow when the container yard reaches capacity.

![Figure 2: DES simulation of container yard occupancy under normal conditions for model CT.](image)

Use of DES simulations in this way provides easily interpretable simulations of attack impact. Models can be quickly tailored to provide accurate simulations of specific facilities and the results are likely to be useful in supporting the case for investment in additional control measures.

**Conclusion**

This article has explained the reliance of modern Container Terminals (CTs) on networked Information Communication Technology (ICT) and Industrial Control Systems (ICS) and why CTs may be considered as a ‘soft’ target by potential attackers. Reducing the vulnerabilities in CT ICT networks will
require investment in hardware, software and processes in order to harden them. This article, and the thesis on which it is based, suggest that Discrete Event Simulators (DES) could be used to model the impact of cyber-attacks against CT networks. Simulation allows the impact of cyber-attacks to be described in terms of the reduction of a CTs ability to process containers - this is a metric that is easy to interpret and could prove useful in supporting business cases.

**Biographies**

*Peter Beaumont* completed his BEng in Mechanical Engineering at Southampton University in 1998. He then worked as a military engineer in the British Army until 2015. On retirement from the Army he completed the MSc in Information Security at Royal Holloway, University of London and graduated with a distinction. He is currently studying for a PhD in cyber security at Royal Holloway where he is undertaking research into the security of Industrial Control Systems.

*Stephen Wolthusen* received his Dipl.-Inform. degree in computer science in 1999 and completed his Ph.D. in theoretical computer science in 2003, both at TU Darmstadt. He is currently a Reader with the ISG, and also Full Professor of Information Security (part-time) at the Norwegian University of Science and Technology, Norway. His research focuses on models of adversaries and resilient networks, with applications in defence networks and particularly in critical infrastructure networks and control systems security. He has led a number of national and European projects, including the Internet of Energy project. He is author and editor of several books, as well as over 130 peer-reviewed publications, and is currently vice-chair of the IEEE Task Force on Network Science.