Scientia Militaria
2023, VOL. 51, NO. 3, 133-160
DOI: 10.5787/51-3-1429

IOT and IIOT Security for the South African Maritime and Freight Transport Sectors

Barend Pretorius
University of KwaZulu-Natal

Brett van Niekerk
Durban University of Technology

Abstract

The advent of the Fourth Industrial Revolution (4IR) has seen a rapid increase in connected smart devices known as the Internet of Things (IoT). While this 'revolution' is most noticeable in commercial devices, there has also been an evolution in industrial devices, known as the Industrial Internet of Things. As Africa – and in particular South Africa – is racing to compete in the 4IR, various sectors, including the transport sector, are introducing innovative projects. However, the Internet of Things and the Industrial Internet of Things present cybersecurity risks. Cybersecurity itself is also considered a key component of the 4IR; yet, organisations often neglect to consider the security implications of the Internet of Things.

The current research aimed to evaluate and prioritise cyber threats, vulnerabilities, and risk related to the Internet of Things and the Industrial Internet of Things in the South African physical transport sector. This article focuses on the responses to a questionnaire to obtain quantitative data from those with experience in the related fields. The threats and vulnerabilities of concern are illustrated, and the risks are evaluated based on the perceived impact of such risks and the likelihood of the Internet of Things and the Industrial Internet of Things being compromised. While no clear leaders of risk were found, the top three risks based on the perceived severity and likelihood are unavailability of Internet of Things and Industrial Internet of Things devices and/or networks, damage to reputation, and cyberespionage.

Keywords: critical infrastructure protection, cybersecurity, Industrial Internet of Things (IIoT), Internet of Things (IoT), transport sector security.

Introduction

The Fourth Industrial Revolution (4IR) has seen advances in technologies contributing towards an information-based society; in particular, there has been an increase in the number of connected devices, known as the Internet of Things (IoT) for consumer items and the Industrial Internet of Things (IIoT) within the industrial setting. The IoT has shown potential benefits in agriculture, city management, transportation, business and healthcare. Research on IoT deployments indicates that the IoT shows promise in addressing or advancing the United Nations' Sustainable Development Goals (Marchant, 2021). However, the IoT also poses risks, particularly regarding cybersecurity. The rapid growth and hyper-connectivity due to the IoT increase the attack surface compared to 'traditional' cybersecurity (Chen, 2016), and the potency of the attacks is increasing (Dooley, 2017). In addition, Townsend (2019) reports that attacks against the IIoT had already begun in 2019, and that organisations were not adequately prepared for them.

The transport sector also is benefitting from the IoT and IIoT, but is also experiencing security challenges. The sector has seen increasing attention from malicious actors in cyberspace (Van Niekerk, 2017), and introducing the IoT and the IIoT may bring with it vulnerabilities, and further increase the attack surface against smart transportation systems (Awan, Memon, Shah & Pathan, 2020; Pretorius & Van Niekerk, 2020). Akpan, Bendiab, Shiaeles and Karamperidis (2022) highlight that limited research has been done on cybersecurity in the maritime sector despite the importance of the sector. In a South African (SA) context, limited studies have been conducted on IoT and IIoT security in the transport sector.

The aim of this study was to investigate the perceptions of IoT and IIoT security in the SA transport sector. In particular, the study sought to evaluate the perceived threats, vulnerabilities, and associated risks of introducing IoT and IIoT to the SA transport sector in order to prioritise the most significant risks. Data were gathered through a close-ended questionnaire, soliciting responses from experts with experience in the sector identified using convenience and snowball sampling.

The article continues with the literature review in the next section, providing an overview of the IoT and the IIoT in general and in the transport sector, and discussing cybersecurity incidents in the sector and those related to the IoT and the IIoT. The methodology section describes the research process in more detail, followed by a presentation of the results. The results are discussed, and the article is then concluded.

Literature review

This section provides an overview of the IoT and the IIoT, followed by a focus of the IoT and the IIoT within the maritime and transport sectors. Specific cybersecurity incidents related to the IoT and the IIoT, in the transport sector, are discussed.

The IoT and IIoT

The IoT can be defined as a "network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment" (Gartner, 2022: n.p.). The term first emerged in 1999, and in the early 2000s the first 'smart' devices were being produced (Marchant, 2021). The IIoT can be considered the intersection between the IoT and traditional operational technology or industrial control systems (Henning, 2017; Pretorius & Van Niekerk, 2020; Sullivan, 2020). In the broader sense, the IoT is revolutionary, as devices not traditionally networked or connected are now becoming so (for example television sets and fridges), whereas the IIoT is evolutionary, as many industrial systems had already been connected and provided with remote access (Bowne, 2015). Chan (2017) elaborates on some of the differences between the IoT and the IIoT, for instance –

- the IIoT needs to have more interoperability and scalability than IoT as they operate with existing legacy systems and large-scale industrial networks;
- the IIoT requires greater precision than IoT and low latency to cater for real-time monitoring of industrial processes; and
- the IIoT requires greater resilience, reliability and serviceability to be able to operate in harsh environments and minimise downtime than IoT.

While the IoT and IIoT provide many benefits, such as improved productivity and data availability, they also introduce security concerns into the corporate and industrial environments (Marchant, 2021; Sullivan, 2020). Chan (2017) mentions that the IIoT requires more security than commercial IoT due to the placement of IIoT in critical industrial processes. Many connected devices may however contain vulnerabilities, some of which are not disclosed by the manufacturers, something that Solomon (2022) calls "insecure-by-design". Johnson (2017: n.p.) as well as Ku and Weiss (2017) indicate that security IIoT is particularly challenging. Some security concerns in terms of the IoT and the IIoT are authentication, insecure protocols for data transfer, insecure data storage, insecure gateways and interfaces, and supply chain risks relating to vulnerabilities in the IoT and IIoT or in individual components of these (Ku & Weiss, 2017; Sullivan, 2020).

Cybersecurity incidents related to the IoT and the IIoT

A number of cybersecurity incidents have occurred due to insecure IoT and IIoT devices. This section discusses selected incidents to illustrate the range of threats and vulnerabilities relevant to IoT and IIoT devices. The most prominent cybersecurity incident was the Mirai botnet, which was used to conduct a series of DDoS (distributed denial-of-service) attacks word wide in over 160 countries worldwide in 2016 (Forrest, 2016; Kan, 2016; Woolf, 2016). The 100 000 infected IoT devices that targeted the service provider Dyn, were reportedly comprising mostly digital video recorders, CCTV cameras, and home routers from over 160 countries. This was followed by a DDoS attack on a Liberian telecommunication provider, with traffic reportedly reaching 500GB/s. At the time, the series of DDoS attacks were the largest ever recorded, and variants of the Mirai were reported to have spread to 500 000 devices that were compromised due to weak default passwords (Forrest, 2016; Kan, 2016; Woolf, 2016).

In another incident, an undisclosed university suffered a DDoS attack due to IoT and IIoT devices in the network being compromised. The attackers gained control of the devices by using the manufacturer's default passwords, which were then changed and brute force attacks were conducted to compromise other devices. Approximately 5 000 devices, such as smart lightbulbs and connected vending machines, were compromised and then used to conduct a DDoS against the domain name server of the university (Cimpanu, 2017). In 2017, a connected temperature sensor in a fish tank at a casino was used as an entry point into the network and stole 10GB of data (Schiffer, 2017).

Common commercial IoT devices found in a household and in businesses have been compromised and/or concerns were raised about their security. Digital road signage and billboards have been hacked to display messages with warnings about weak default and hardcoded passwords that could be used to compromise such devices (Kovacs, 2014). A fridge has been seen to have sent spam e-mails, and the Federal Bureau of Investigation (FBI) released a warning about insecure baby monitors and toys as well as the risk of smart TVs or entertainment systems with a camera and microphone, which have raised privacy concerns (Chen, 2016; Lomas, 2015; Schiffer, 2017; Starr, 2014; Vaughan-Nichols, 2019). In addition, there have been cases where video conferencing systems have been compromised and large quantities of information stolen from the organisations. This further illustrates the potential use of IoT devices for espionage – if the audio and video could be accessed, the attackers would be able to steal sensitive corporate information (Darktrace, 2016).

IoT or IIoT devices themselves may not necessarily be the entry point. Vendors and third-party services may be compromised in order to gain access to the organisation. A major example of this is the United States (US) market chain Target, where cybercriminals managed to steal 40 million credit-card records in 2013 after entering Target via the Heating, Ventilation and Air Conditioning (HVAC) contractor. This was one of the largest data breaches at the time, and is estimated to have cost Target over US$200 million (Zimmerman, 2017).

The above incidents illustrate a number of vulnerabilities, risks and threats related to IoT and IIoT. These can be seen to include DDoS attacks affecting networks, stolen data, privacy and espionage. Vulnerabilities may include insecure protocols, device authentication, with third parties as well as devices contributing to breaches.

IoT and IIoT in the maritime and related sectors

There are a number of benefits to IoT in the maritime sector, including automation, real-time monitoring, analytics for optimisation, improved communication and connectivity for vessels at sea, which have the potential for cost savings (Burkhalter, 2022; Kapkaeva, Gurzhiy, Maydanova & Levina, 2021; KVH Watch, 2021). The concept 'smart ports' implies enhanced productivity, automation, and intelligent infrastructure based on technologies, such as IoT and artificial intelligence (Min, 2022; Molavi, Lim & Race, 2019). Molavi et al. (2019) also indicate that a measure of a 'smart port' is an interface with intelligent railways. Ayyagari (2018) describes a number of benefits of IoT in railways, which are similar to those in the maritime sector, namely improved monitoring translating into better safety and reliability, predictive maintenance, and analytics to aid optimisation.

Cybersecurity for the transport sector is crucial due to its critical nature. The importance of the sector is highlighted in the *Australian Security of Critical Infrastructure Act (No. 29 of 2018)*, by the US Cybersecurity and Infrastructure Security Agency (CISA) (2020), and also by Theoharidou, Kandias and Gritzalis (2011). Akpan et al. (2022) raise a number of challenges for cybersecurity in the maritime domain, particularly in terms of automated ships due to the large number of systems for navigation, radar, communications, propulsion and the associated industrial control and IT networks. Many of these automated ships with demonstrated vulnerabilities make cybersecurity of a connected vessel difficult. Similarly, automated ports could also face these challenges, as well as railways and pipelines, which often have interfaces with the maritime sector. Cybersecurity incidents demonstrating the possibly attack methods and consequences are illustrated in the next section.

Cybersecurity incidents in the maritime and related sectors

The number of cybersecurity incidents affecting the transport sector has been increasing from 2008 to 2016, and the majority of the incidents during that period had affected the maritime sector (see Van Niekerk, 2017). This section discusses select incidents to illustrate the types of threats that have been experienced within the sector since 2001.

Port operations have been affected by cybersecurity incidents, such as a DDoS attack disrupting the Port of Houston in 2001 (McCue, 2003). Ransomware affected port operations at Transnet in South Africa in 2021 (Gallagher & Burkhardt, 2021), and the NotPetya affected A.P. Møller-Maersk's port operations globally (Cimpanu, 2018). A major port terminal in Iran was disrupted by a cyberattack in 2020, attributed to a nation-state (Warrick & Nakashima, 2020). Ports have also been disrupted due to signal jamming of global positioning systems (GPSs), such as in an undisclosed European port in 2015 and the Port of Shanghai in 2019; the latter also experienced spoofing of both GPS and Automatic Identification System (AIS) signals (Goward, 2019; Knox, 2015). In addition to operational disruptions, criminals have used cyberattacks to track shipping containers with smuggled goods, as in the Port of Antwerp in 2013 (Dunn, 2013).

In addition to ports, sea-going vessels have also been affected by cyberattacks. A series of oil rigs were affected by cybersecurity incidents, including malware disrupting the navigation systems resulting in the rig drifting off position, and hackers tilting an oil rig in 2014 resulting in a disruption of operations (CyberKeel, 2014; Knox, 2015; Swanbeck, 2015; Wagstaff, 2014). In addition, in 2009, a disgruntled insider at Pacific Energy Resources platforms offshore of Huntington Beach disabled the safety systems of oil rigs (Kravets, 2009).

Delays in passenger rail services have been experienced due to malware (CSX Corporation in 2013), ransomware (San Francisco in 2016), DDoS (Denmark in 2018), and a network intrusion that affected the signals (United States in 2011), indicating a range of threat types that could cause disruptions (Fletcher & Bye, 2022; Miller & Rowe, 2012; Ragan, 2012). One of the earliest attacks against a rail system occurred in Poland in 2008, when a team built a device in order to switch the points on the tram system remotely, resulting in a derailment (Ismail, Sitnikova & Slay, 2015).

Pipelines have also experienced disruptions on the back of cyberattacks, most notably the ransomware infection at Colonial Pipelines in 2021, which resulted in significant social ramifications (Kerner, 2022). In 1999, a disgruntled insider at Gazprom aided attackers with a backdoor, which affected the flow control systems (Miller & Rowe, 2012). Wiper malware rendered corporate computers ineffective at Saudi Aramco in 2012, but did not affect industrial systems (Bronk & Tikk-Ringas, 2013). Between 2011 and 2012, a cyberespionage operation stole operational data from US pipeline organisations (Clayton, 2013).

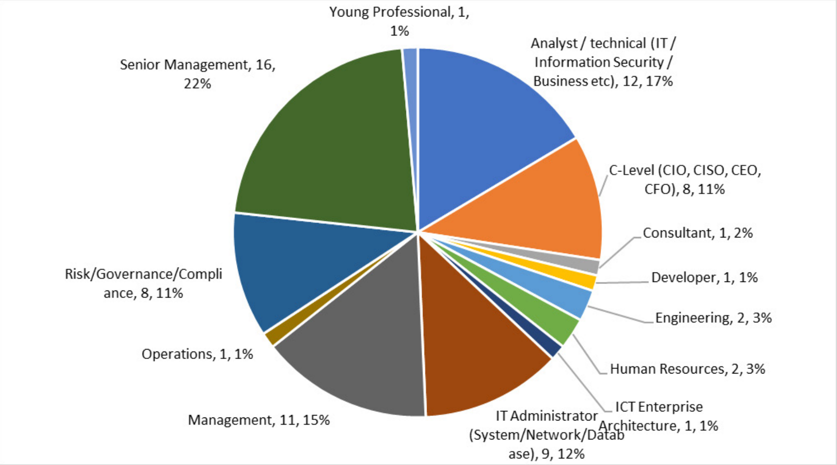
The above incidents illustrate that the transport sector has been affected by numerous threat types, including DDoS, malware, ransomware, signal jamming, as well as other system intrusions. Threat actors include insider threats, state actors, cybercriminals, and individual perpetrators.

Methodology

The current study sought to evaluate the perceptions of IoT and IIoT security within the SA transport sector, particularly to determine whether there are any specific areas of concern. The focus of this article is on the qualitative responses received for the technical factors, namely the threats, vulnerabilities and associated risks of compromised IoT and IIoT. Due to limited information available on individuals who have experience in terms of IoT and IIoT and security in the sector, non-probabilistic sampling was appropriate, and convenience sampling was used and enhanced with snowball sampling. An online questionnaire was distributed to organisations in the transport sector and through professional bodies to solicit responses. This article presents the results of an exploratory analysis of the responses received regarding the technical factors of IoT and IIoT security within the SA transport sector. Limitations of the study arose from the fact that a small population with specialised knowledge was targeted; therefore, the results may not be generalisable outside of the SA transport sector.

Results

This section presents the results from the questionnaire relating to the technology factors influencing IoT and IIoT security in the transport sector of South Africa. A total of 73 responses were received; however, eight of these did not have any experience in terms of either IoT or IIoT, and were therefore excluded, leaving 65 valid responses, as illustrated in Table 1.



Note: CIO = Chief Information Officer; CISO = Chief Information Security Officer

Figure 1: Job profiles of the respondents

The respondents indicated a variety of experience with IIoT, as illustrated in Figure 2. As is evident, the majority of respondents were familiar with IIoT from an IT perspective (38%), followed by security experience (18%) and governance, risk and compliance (17%).

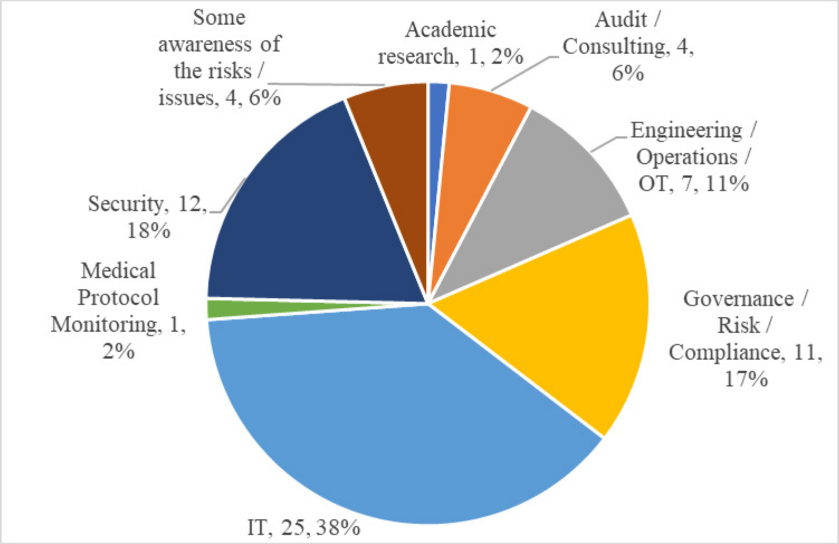


Figure 2: Respondents' experience with IIoT

Figure 3 illustrates the number of years of experience the respondents had with IIoT. The vast majority had less than five years of experience (77%), with 29% having less than one year of experience, and 29% having two to five years of experience. This illustrates the emerging nature of IIoT and its introduction into the environment.

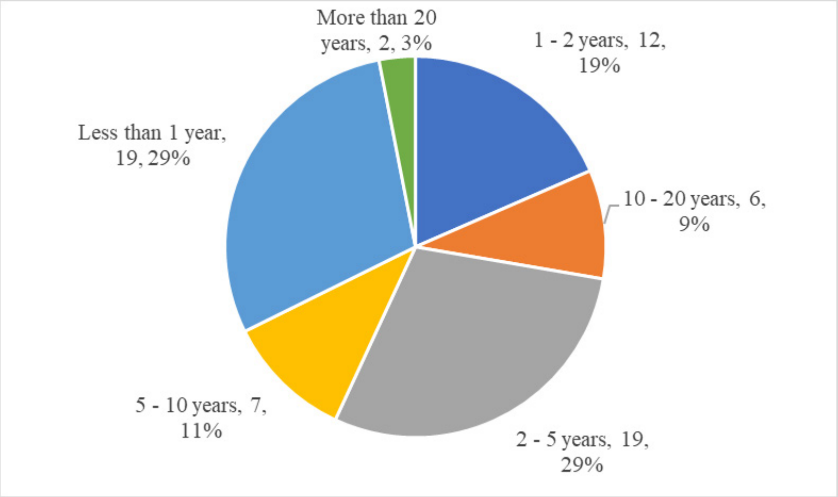


Figure 3: Years of experience with IIoT

Respondents were asked to identify the types of IoT and IIoT present in their environments. Figure 4 illustrates that the vast majority of the respondents had boardroom and/or video conferencing equipment (80%) and CCTV or smart cameras (74%). IIoT is not as prevalent, with ICS and SCADA being indicated the most (60%), followed by vehicle tracking and monitoring (58%). These trends illustrate initial commercial IoT has more penetration in organisations than IIoT.

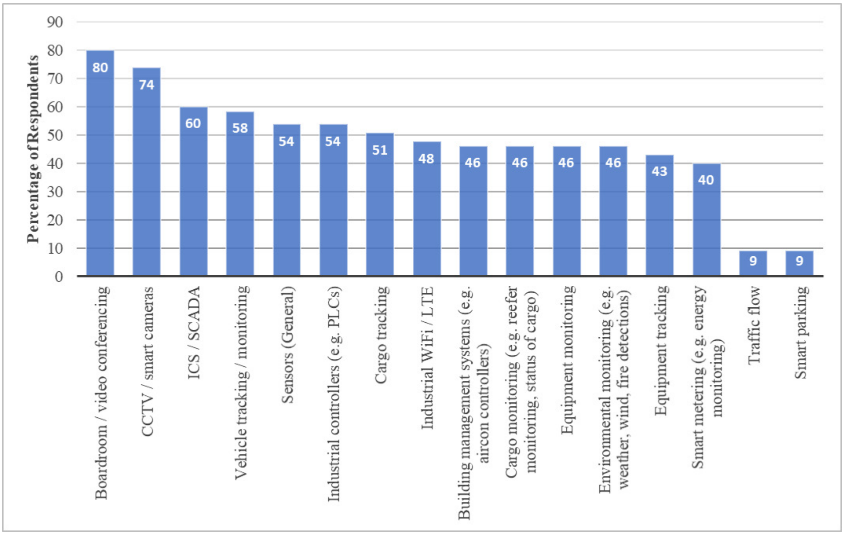


Figure 4: Type of IoT and IIoT devices in the workplace

Perceived IoT and IIoT threats in the South African transport sector

To assess the IoT and IIoT threat landscape with relevance to the SA transport sector, respondents were asked to rate –

- the impact IoT and IIoT will have on the threat landscape;
- the top three perceived threats; and
- whether (at the time) any of the threats had been exploited.

The respondents were asked to rate the impact that IoT and IIoT would have on the threat landscape in the transport sector in South Africa, rating possible threat categories as *Introducing new threats* (5), *Increasing existing threats* (4), a *Slight increase in existing threats* (3), *No change in threats* (2) and *No threat/not relevant* (1). Figure 5 shows the prevalence of responses, and Table 2 provides the descriptive statistics. From the responses, it was noted that the top three threats perceived to be introduced by IIoT are *Remote access*, *Cyber espionage*, and *Signal jamming attacks*. The top threats to be affected by IoT and IIoT (either increasing existing threats or introducing new threats) were *Remote access* with a mean of 4.0, *Cyber espionage* with a mean of 3.9 and *Ransomware* with a mean of 3.8.

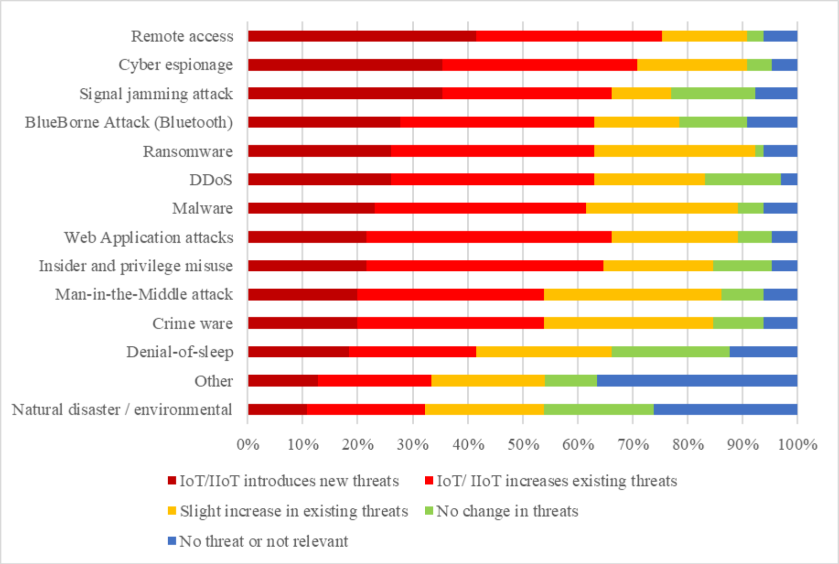


Figure 5: Existing and new threats introduced by IoT and IIoT

Table 2: Frequency and descriptive statistics table of threats

	DDoS	Insider and privilege misuse	Cyber espionage	Web application attacks	Malware	Natural disaster environmental	Crime ware	Denial-of-sleep	Ransomware	Man-in-the-middle attack	Remote access	Signal jamming attack	BlueBorne attack (Bluetooth)	Other
No threat or not relevant	2	3	3	3	4	17	4	8	4	4	4	5	6	23
No change in threats	9	7	3	4	3	13	6	14	1	5	2	10	8	6
Slight increase in existing threats	13	13	13	15	18	14	20	16	19	21	10	7	10	13
IoT/ IIoT increases existing threats	24	28	23	29	25	14	22	15	24	22	22	20	23	13
IoT/IIoT introduces new threats	17	14	23	14	15	7	13	12	17	13	27	23	18	8
Mean	3.7	3.7	3.9	3.7	3.7	2.7	3.5	3.1	3.8	3.5	4.0	3.7	3.6	2.6
Std. deviation	1.1	1.1	1.1	1.0	1.1	1.4	1.1	1.3	1.1	1.1	1.1	1.3	1.3	1.5

Respondents were asked to select three threats from the list in the question that they perceived to be a top threat related to IoT and/or IIoT. The top three threats selected were *Malware,* which was selected by 35 of the respondents*, Insider and privilege misuse* and *Distributed denial of service (DDoS)* was joint second with 29 each and third was *Cyber espionage* with 28. More detailed results are provided in Figure 6.

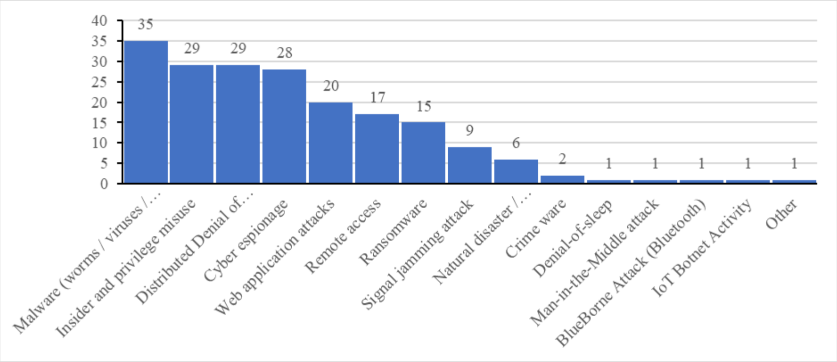


Figure 6: Top three threats related to IoT and IIoT

The respondents were asked to indicate if any of the treats occurred in their organisation's IoT and IIoT environment, and the responses are shown in Figure 7. The largest response showed that respondents were unsure or that a threat might have materialised (36%); followed by an indication that a threat had materialised (29%); while 26% of respondents indicated that they did not have a threat occurring in their IoT and IIoT environment. Some respondents were unable to disclose whether a threat had occurred (9%). The fact that more respondents could confirm a threat than those confirming a threat had not occurred showed that the IoT and IIoT environment in the SA transport sector is susceptible to cyberattacks. The following section discusses the perceived vulnerabilities.

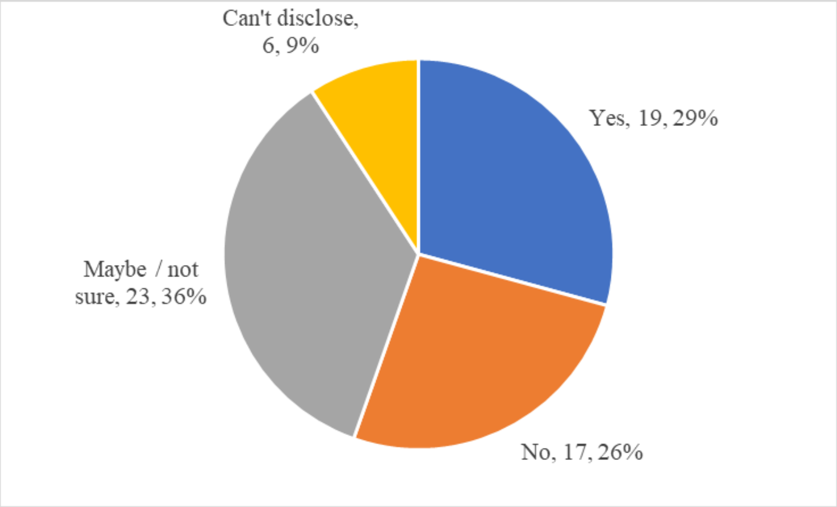


Figure 7: Occurrence of threats

Vulnerabilities related to IoT and IIoT

Respondents were asked to rate a number of vulnerabilities related to IoT and IIoT. Figure 8 and Table 3 show the responses and frequency of the vulnerabilities from Very low (1) to Very high (5) severity. From Figure 8, the top vulnerabilities related to the IoT and IIoT environment in the SA transport sector, ranked on the number of 'Very high' and then 'High' ratings, are:

- *No or delay in Patching / firmware updates*;
- *No or Weak Password*; and
- *Insecure mobile interface*.

From Table 3, the top three vulnerabilities based on the mean of the ratings are:

- *No or delay in Patching / firmware updates* with a mean of 3.8;
- *Insecure Default Settings* with a mean of 3.69; and
- *Insecure mobile interface* with a mean of 3.66.

All of these can be considered a *Medium Risk* moving towards *High*.

The vulnerabilities that appeared to be of least concern are:

- *Lack of physical hardening* and *No privacy protection* both with a mean of 3.3,
- *Insecure network perimeter* and *Insecure network services*, both with a mean of 3.4.

This implies the feedback overall considers most vulnerabilities introduced by IoT and IIoT as *Medium*.

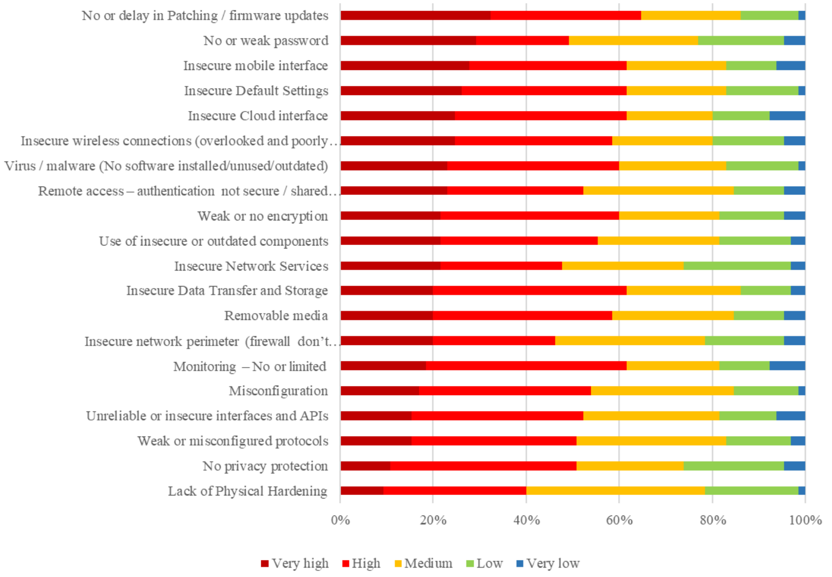


Figure 8: Vulnerabilities related to IoT and IIoT

Table 3: Frequency and descriptive statistics of the vulnerabilities

	Very low	Low	Medium	High	Very high	Mean	Std. deviation	Variance
No or weak password	3	12	18	13	19	3.5	1.2	1.5
No or delay in Patching / firmware updates	1	8	14	21	21	3.8	1.1	1.2
Misconfiguration	1	9	20	24	11	3.5	1	1
Weak or no encryption	3	9	14	25	14	3.6	1.1	1.2
Removable media	3	7	17	25	13	3.6	1.1	1.2
Insecure default settings	1	10	14	23	17	3.7	1.1	1.2
Weak or misconfigured protocols	2	9	21	23	10	3.5	1	1

	Very low	Low	Medium	High	Very high	Mean	Std. deviation	Variance
Unreliable or insecure interfaces and APIs*	4	8	19	24	10	3.4	1.1	1.2
Virus / malware (no software installed/unused/ outdated)	1	10	15	24	15	3.6	1.1	1.1
Insecure wireless connections (overlooked and poorly configured)	3	10	14	22	16	3.6	1.2	1.3
Lack of physical hardening	1	13	25	20	6	3.3	0.9	0.9
Remote access – authentication not secure / shared passwords for vendors	3	7	21	19	15	3.6	1.1	1.2
Monitoring – no or limited	5	7	13	28	12	3.5	1.1	1.3
Insecure network perimeter (firewall don't exist/misconfigured, direct connections to internet)	3	11	21	17	13	3.4	1.1	1.3
No privacy protection	3	14	15	26	7	3.3	1.1	1.2
Insecure network services	2	15	17	17	14	3.4	1.2	1.3
Use of insecure or outdated components	2	10	17	22	14	3.6	1.1	1.2
Insecure data transfer and storage	2	7	16	27	13	3.6	1	1
Insecure cloud interface	5	8	12	24	16	3.6	1.2	1.5
Insecure mobile interface	4	7	14	22	18	3.7	1.2	1.4

Note: API = Application Programming Interface

Risks of unsecured IoT and IIoT (impact)

Respondents were asked to rate risks of IoT and IIoT based on **impact** – *Insignificant* (1) to *Extreme/catastrophic* (5) – and **likelihood** – *Very low* (1) to *Very high* (5). Figure 9 shows the respondents' rating of the impact of compromised IoT and IIoT devices, and Table 4 provides descriptive statistics of the potential impact.

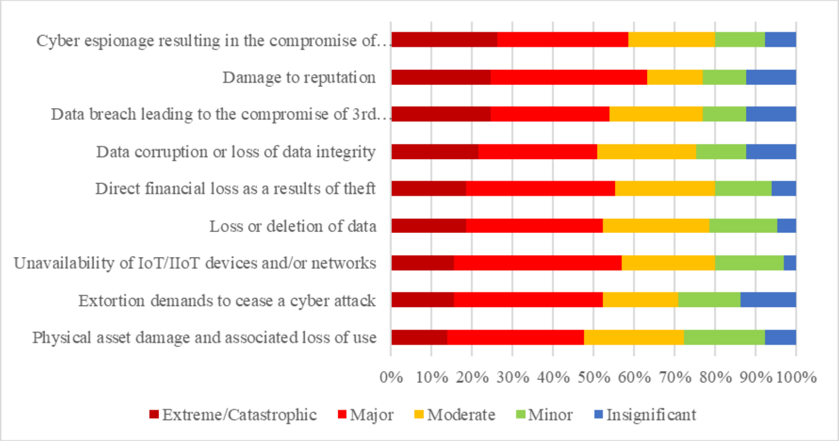


Figure 9: Risk (impact) related to IoT and/or IIoT

From the responses, the top three risks that have the most impact in terms of IoT and IIoT in the transport sector of South Africa are:

- *Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information* with a mean of 3.57;
- *Damage to reputation* with a mean of 3.52; and
- *Unavailability of IoT/IIoT devices and/or networks* with a mean of 3.49.

These are all *Moderate* impacts.

The three risks that are of least concern regarding their potential impact if compromised are:

- *Extortion demands to cease a cyber attack* with a mean of 3.25;
- *Physical asset damage and associated loss of use* with a mean of 3.26; and
- *Data corruption or loss of data integrity* with a mean of 3.35.

Again, these are all *Moderate* impacts, implying that, in general, IoT and IIoT will result in a *Moderate* impact to the organisation if compromised.

Table 4: Frequency and descriptive statistics of risks (impact)

	Physical asset damage and associated loss of use	**Unavailability of IoT/IIoT devices and/or networks**	**Loss or deletion of data**	**Data corruption or loss of data integrity**	**Data breach leading to the compromise of 3rd party confidential information, including personal information**	**Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information**	**Extortion demands to cease a cyber attack**	**Direct financial loss as a result of theft**	**Damage to reputation**
Very low	5	2	3	8	8	5	9	4	8
Low	13	11	11	8	7	8	10	9	7
Medium	16	15	17	16	15	14	12	16	9
High	22	27	22	19	19	21	24	24	25
Very high	9	10	12	14	16	17	10	12	16
Mean	3.26	3.49	3.45	3.35	3.43	3.57	3.25	3.48	3.52
Std. deviation	1.2	1.0	1.1	1.3	1.3	1.2	1.3	1.1	1.3
Variance	1.4	1.1	1.3	1.7	1.7	1.5	1.7	1.3	1.7

For the likelihood of an impact occurring, respondents were asked to rate each category from *Very low* (1) to *Very high* (5). Figure 10 shows the likelihood of the risks due to compromised IoT and IIoT devices ranked according to the most responses for *Very high*, *High*, with *Very low* being the lowest priority. The top three risks by likelihood arranged according to Very high and High responses are *Damage to reputation*, *Cyber espionage*, and *Data breach leading to a compromise of 3rd party*.

Table 5 shows the frequency and full descriptive statistics of the likelihood ratings. From the responses, the top three risks that are rated most likely to occur are:

- *Unavailability of IoT/IIoT devices and/or networks* with a mean of 3.49;
- *Damage to reputation* with a mean of 3.4; and
- *Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information* with a mean of 3.31.

These are all slightly above *Medium* likelihoods.

The three risks that are rated least likely to occur are:

- *Extortion demands to cease a cyber attack* with a mean of 3.02;
- *Data corruption or loss of data integrity* with a mean of 3.06; and
- *Loss or deletion of data* with a mean of 3.15

Again, these are all *Medium* likelihoods.

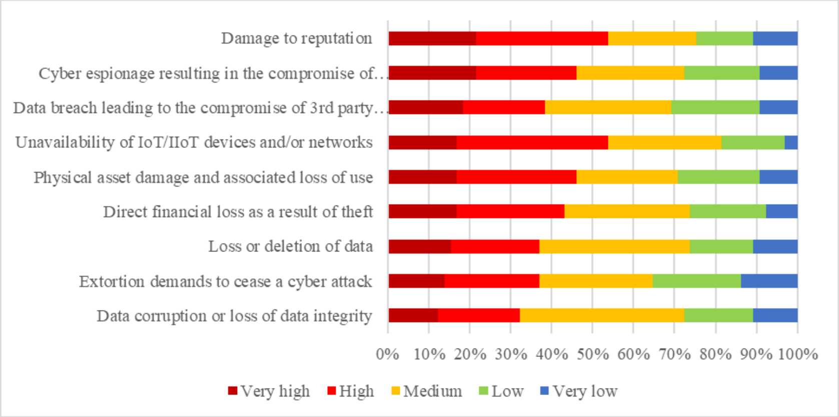


Figure 10: Risk (likelihood) related to IoT and IIoT

Table 5: Frequency and descriptive statistics of risks (likelihood)

	Physical asset damage and associated loss of use	**Unavailability of IoT/IIoT devices and/or networks**	**Loss or deletion of data**	**Data corruption or loss of data integrity**	**Data breach leading to the compromise of 3rd party confidential information, including personal information**	**Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information**	**Extortion demands to cease a cyber attack**	**Direct financial loss as a result of theft**	**Damage to reputation**
Very low	6	2	7	7	6	6	9	5	7
Low	13	10	10	11	14	12	14	12	9
Medium	16	18	24	26	20	17	18	20	14
High	19	24	14	13	13	16	15	17	21
Very high	11	11	10	8	12	14	9	11	14
Mean	3.25	3.49	3.15	3.06	3.17	3.31	3.02	3.26	3.40
Std. deviation	1.2	1.0	1.2	1.1	1.2	1.3	1.3	1.2	1.3
Variance	1.5	1.1	1.4	1.3	1.5	1.6	1.6	1.4	1.6

The risk for each of the categories is listed in Table 6 and illustrated in Figure 11, taking into account both the mean impact ratings and the mean likelihood ratings. For Table 6, *Risk* is calculated as the product of the mean for *Impact* and *Likelihood*, and has a range of 1 to 25. The highest risk is shown in the top right corner, and the lowest risk is reflected in the bottom left corner.

The top three risks are

- *Unavailability of IoT/IIoT devices and/or networks*;
- *Damage to reputation*; and
- *Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information*.

The three categories presenting the lowest risks for IoT/IIoT are:

- *Extortion demands to cease a cyber attack*;
- *Data corruption or loss of data integrity*; and
- *Physical asset damage and associated loss of use*.

It is also evident from Figure 11 that the risks are clustered together because the mean of the **Impact** and **Likelihood** ratings were all between 3 and 4. There is therefore no distinct category risk posed by IoT and IIoT, but there is a clear risk present.

Table 6: Calculated risk for IoT and IIoT

	Physical asset damage and associated loss of use	**Unavailability of IoT/IIoT devices and/or networks**	**Loss or deletion of data**	**Data corruption or loss of data integrity**	**Data breach leading to the compromise of 3rd party confidential information, including personal information**	**Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information**	**Extortion demands to cease a cyber attack**	**Direct financial loss as a result of theft**	**Damage to reputation**
Very low	6	2	7	7	6	6	9	5	7
Low	13	10	10	11	14	12	14	12	9
Medium	16	18	24	26	20	17	18	20	14

High	19	24	14	13	13	16	15	17	21
Very high	11	11	10	8	12	14	9	11	14
Mean	3.25	3.49	3.15	3.06	3.17	3.31	3.02	3.26	3.40
Std. deviation	1.2	1.0	1.2	1.1	1.2	1.3	1.3	1.2	1.3
Variance	1.5	1.1	1.4	1.3	1.5	1.6	1.6	1.4	1.6

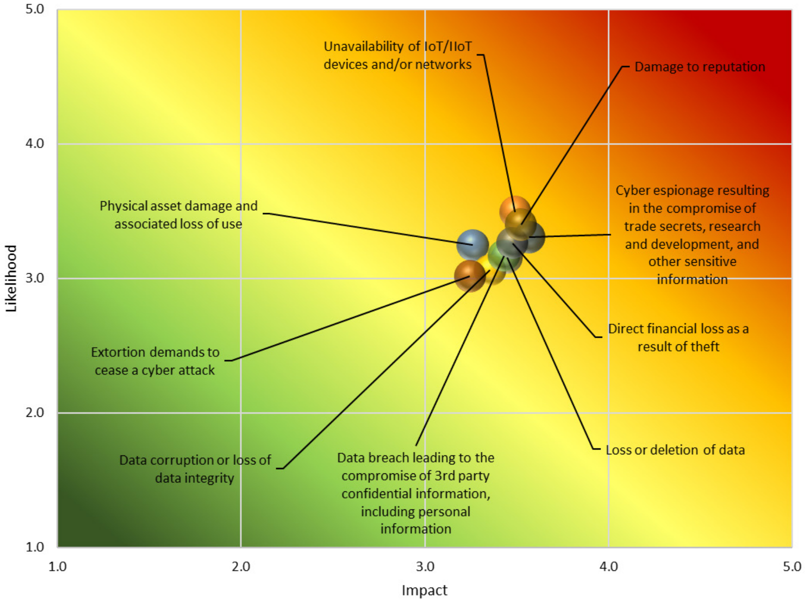


Figure 11: Risk (impact vs likelihood)

Discussion and recommendations

Within the transport sector, there is a prevalence of IoT in terms of smart TVs for boardrooms and CCTV systems, with lower penetration of IIoT. The smart TVs and CCTV systems are of particular note, particularly due to concerns of eavesdropping via the smart TVs, and the use of CCTV systems in the notorious Mirai botnet used to conduct DdoS attacks. Two of the top three perceived risks are therefore aligned to these specific IoT devices: cyber espionage relating to the TVs, and IoT and IIoT and network unavailability relating to the possibility of DdoS due to compromised IoT devices.

Similarly, the top three threats where IoT and IIoT are perceived to introduce new threats are *Remote access*, *Cyber espionage*, and *Signal jamming attacks*. The cyber espionage as described above, and the signal jamming attacks have been reported as discussed in the Literature review above. Remote access is also aligned to incidents that have occurred regarding the IoT that is reported to be prevalent in the sector. When considering the top three threats by the mean of the responses, *Ransomware* replaces *Signal jamming*. An increase in ransomware has been seen, and has negatively affected maritime organisations such as Maersk and Transnet.

When considering the top three threats in general related to IoT and IIoT (compared to being increased by IoT and IIoT), *Malware* was first, followed jointly by *Insider and privilege misuse* and *DdoS*, then *Cyber espionage*. *Cyber espionage* is evidently a recurring theme of concern to the sector. *Malware* has become a common threat related to IoT and IIoT, and *Insider threats* refer to the possibility of insecure rogue devices breaching security. In addition, insider threats were listed as one of the major categories of cyber incidents in 2019 (McKee, 2019). A key recommendation for IoT and IIoT is network segmentation and to include the IoT and IIoT networks in security monitoring in order to detect any abnormalities on the network which could signify the presence of malware, misuse, DdoS, or cyber espionage. Traditional perimeter monitoring security should be updated to ensure the IoT and IIoT environment are catered for.

The perceived vulnerabilities include *No or delay in Patching / firmware updates* and *Insecure mobile interface*, both in the top three based on the number of *Very high* responses as well as the mean of responses. *No or Weak Password* was in the top three based on *Very high* responses, and *Insecure Default Settings* was in the top three based on the mean. All of these perceived vulnerabilities related to the concept of 'insecure by design', where products are provided without sufficient security testing or unacknowledged bugs (Solomon, 2022). These vulnerabilities could allow malicious users the ability to compromise IoT and IIoT devices easily to gain a foothold in a network, and has been demonstrated by a number of incidents. The latter two vulnerabilities can be seen as a 'low-hanging fruit' in that they should be fairly simple to correct by immediately changing the default settings and passwords to secure the devices. A procurement requirement for IoT and IIoT devices that could be included is that the devices must not have hard-coded (i.e. impossible to change) passwords. During project design stage of IoT and IIoT, it is important to consider the patching and the security of such devices, and to conduct adequate security testing well before deploying them to allow for time to make the necessary security adjustments in the interfaces and patching methods if required.

IoT and IIoT present a clear general risk, rated as *Moderate* but leaning towards *High*. While there is no clear risk category that is higher than any other, the top three (*Unavailability of IoT/IIoT devices and/or networks*, *Damage to reputation*, and *Cyber espionage*) signify availability and data theft concerns (which could in turn could have privacy implications). These two categories explain the third, *Damage to reputation*, as an outage of the networks affecting delivery of products or services, or a data breach being discovered, that would lead to reputational damage of the organisation. In terms of service disruption, the NotPetya incident affecting Maersk and the ransomware at Transnet are prime examples. Overall, the responses align to actual incidents that have been experienced.

As is evidenced from the demographics, IoT and IIoT are still relatively new within the SA transport sector, with 38% of respondents having two years or less of experience, and another 29% having two to five years of experience. It is therefore important to continue similar research, as the environment becomes increasingly established, to assess any changes in the threat landscape (or perceptions thereof). Future research could include an investigation into prevalent industry IoT and IIoT security frameworks in order to propose a dedicated IoT and IIoT security framework for the SA maritime and freight transport sectors.

Conclusion

The IoT and IIoT present benefits to the maritime and related transport sectors; however, IoT and IIoT may introduce vulnerabilities and broaden the attack surface. A number of cybersecurity incidents have been perpetuated through the use of insecure IoT devices. The transport sector, and the maritime sector in particular, have seen increasing cybersecurity incidents; for example, the ransomware incidents that disrupted operations at Maersk and Transnet. It is therefore important to research the potential effect of introducing IoT and IIoT into the environment.

This study investigated the threats, vulnerabilities and risks associated with IoT and IIoT in the SA transport sector. Questionnaires were distributed using convenience and snowball sampling. Remote access, cyber espionage and signal jamming were top threats considered to be introduced along with IoT and IIoT, while malware, insider or privilege misuse, DDoS and cyber espionage were the top threats associated with IoT and IIoT in general. Key vulnerabilities include issues with patching and firmware updates, weak authentication, insecure default settings, and insecure interfaces. While there were no clear leaders of risk, the top three risks based on the perceived severity and likelihood are unavailability of IoT and IIoT devices and/or networks, damage to reputation, and cyber espionage. In general, the responses align to cybersecurity incidents that have already occurred. Recommendations are to ensure that the IoT and IoT devices in existing security controls are considered, that they are on segregated networks, and that security is a key design and procurement consideration for IoT and IIoT devices.

About the Authors

Barend Pretorius holds a Master's degree in Information Systems and a Bachelor of Science (Honours) in Mathematical Statistics. He is studying towards a PhD focusing on the Cyber Security of Industrial Internet of Things and is a Certified Information Security Manager (CISM). He joined Transnet Group in 2014 as a Senior Information Security Analyst and was transferred in 2017 as the Information Security Officer at one of its divisions, Transnet Port Terminals (TPT). He was promoted in 2020 to Senior Manager for ICT Support Service at TPT, responsible for Cyber Security, Networks, Infrastructure, Cloud and End user computing. In 2022 he was promoted and transferred to Transnet Group where he is currently in the role of Senior Specialist: Information Security & Governance responsible for establishing and maintaining an enterprise-wide information security program, enterprise-wide information security strategy, including an Information Security Management System, ICT Governance, Risk, and Compliance.

Prof Brett van Niekerk (PhD) is an associate professor in the Department of Information Technology at the Durban University of Technology, a non-resident fellow at the Security Institute for Governance and Leadership in Africa (Stellenbosch University), chairs the International Federation of Information Processing Working Group on ICT in Peace and War, and is Editor-in-Chief of the International Journal of Cyber Warfare and Terrorism. He has cybersecurity experience across industry, academia and civil society. He has actively participated in international cybersecurity forums (Global Commission on the Stability of Cyberspace, Paris Call working groups, Carnegie Endowment for International Peace's project on countering influence operations). He is CISM certified, with over 50 academic publications and 20 presentations at industry events.

References

Akpan, F., Bendiab, G., Shiaeles, S. & Karamperidis, S. 2022. Cybersecurity challenges in the maritime sector. *Network*, 2, 123–138.

Australian Government. 2018. *Security of Critical Infrastructure Act 2018*. Available at: <https://www.legislation.gov.au/Details/C2018A00029/Download> [Accessed 25 May 2022].

Awan, J.H., Memon, S., Shah, A.A. & Pathan, K.J. 2020. Proposed framework of smart transportation in Pakistan: Issues, challenges, vulnerabilities, and solutions. *International Journal of Cyber Warfare and Terrorism*, 10(4), 48–63.

Ayyagari, M. 2018. *Five smart ways how IoT is transforming the railways*. CYIENT. Available at: <https://www.cyient.com/blog/rail-transportation/five-smart-ways-how-iot-is-transforming-the-railways> [Accessed 24 June 2022].

Bowne, M. 2015. *IOT vs. IIOT*. Profinet. Available at <http://us.profinet.com/iot-vs-iiot/> [Accessed 14 October 2019].

Bronk, C. & Tikk-Ringas, E. 2013. The cyber attack on Saudi Aramco. *Survival*, 55(2), 81–96.

Burkhalter, M. 2022. IoT at sea: *How the internet of things powers the maritime industry*. Perle. Available at: <https://www.perle.com/articles/iot-at-sea-how-the-internet-of-things-powers-the-maritime-industry-40193572.shtml> [Accessed 24 June 2022].

Chan, B. 2017. *Industrial IoT versus IoT: Do you know the difference?* Strategy of Things. Available at: <https://strategyofthings.io/industrial-iot> [Accessed 14 October 2019].

Chen, P. 2016. *Why security in the Internet of Things is different from cybersecurity*. EDN-Europe. Available at: <http://www.edn-europe.com/blog/why-security-internet-things-different-cybersecurity> [Accessed 12 July 2016].

Cimpanu, C. 2017. *University DDoSed by its own IoT devices*. BleepingComputer. Available at: <https://www.bleepingcomputer.com/news/security/university-ddosed-by-its-own-iot-devices/> [Accessed 20 February 2017].

Cimpanu, C. 2018. *Maersk reinstalled 45,000 PCs and 4,000 servers to recover from NotPetya attack.* BleepingComputer. Available at: <https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack> [Accessed 7 September 2018].

Clayton, M. 2013. *Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage*. The Christian Science Monitor. Available at: <https://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage> [Accessed 3 June 2022].

CyberKeel. 2014. *Maritime cyber-risks: Virtual pirates at large on the cyber seas*. Available at: <http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf> [Accessed 24 June 2022].

Cybersecurity and Infrastructure Security Agency. 2020. *Transportation systems sector*. Available at: https://www.cisa.gov/transportation-systems-sector [Accessed 24 May 2022].

Darktrace. 2016. *Darktrace discoveries: Global threat case studies 2016*. Available at: <http://www.informationweek.com/whitepaper/cybersecurity/security/darktrace-discoveries-global-threat-case-studies-2016/383043> [Accessed 14 June 2017].

Dooley, R. 2017. Cyber security at the heart of the Fourth Industrial Revolution, I. *UK Construction Online*, 15 June. Available at: <https://www.ukconstructionmedia.co.uk/features/cyber-security-industrial-revolution/> [Accessed 24 June 2022].

Dunn, J.E. 2013. Hackers planted remote devices to smuggle drugs through Antwerp port, Europol reveals. *Techworld*, 16 October. Available at: <http://news.techworld.com/security/3474018/hackers-planted-remote-devices-to-smuggledrugs-through-antwerp-port-europol-reveals/> [Accessed 22 June 2022].

Fletcher, D. & Bye, P. 2022. *Cybersecurity in transit systems*. The National Academies Press. Available at: <https://nap.nationalacademies.org/catalog/26475/cybersecurity-in-transit-systems> [Accessed 27 May 2022].

Forrest, C. 2016. How the Mirai botnet almost took down an entire country, and what your business can learn. *Tech Republic*, 3 November. Available at: <https://www.techrepublic.com/article/how-the-mirai-botnet-almost-took-down-an-entire-country-and-what-your-business-can-learn/> [Accessed 24 June 2022].

Gallagher, R. & Burkhardt, P. 2021. 'Death Kitty' ransomware linked to South African port attack. *Bloomberg*, 29 July. Available at: <https://www.bloomberg.com/news/articles/2021-07-29/-death-kitty-ransomware-linked-to-attack-on-south-african-ports> [Accessed 3 January 2022].

Gartner. 2022. *Internet of Things (IoT)*. Gartner Glossary. Available at: <https://www.gartner.com/en/information-technology/glossary/internet-of-things/> [Accessed 24 June 2022].

Goward, D. 2019. GPS jamming and spoofing reported at port of Shanghai. *The Maritime Executive*, 13 August. Available at: <https://www.maritime-executive.com/editorials/gps-jamming-and-spoofing-at-port-of-shanghai> [Accessed 27 May 2022].

Henning, C. 2017. *7 steps to IIoT*. Profinet. Available at: <http://us.profinet.com/7-steps-iiot/> [Accessed 7 September 2019].

Ismail, S., Sitnikova, E. & Slay, J. 2015. SCADA systems cyber security for critical infrastructures: Case studies in the transport sector. In *Proceedings of the 10th International Conference on Cyber Warfare and Security (ICCWS 2015)*, 425–433.

Johnson, J. 2017. Securing industrial IoT: There is no simple answer. *IIoT World*, 15 June. Available at: <https://www.iiot-world.com/ics-security/cybersecurity/securing-industrial-iot-there-are-no-simple-solutions/> [Accessed 24 June 2022].

Kan, M. 2016. DDoS attack on Dyn came from 100,000 infected devices. *Computer World*, 26 October. Available at: <http://www.computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html> [Accessed 31 October 2016].

Kapkaeva, N., Gurzhiy, A., Maydanova, S. & Levina, A. 2021. Digital platform for maritime port ecosystem: Port of Hamburg case. *Transportation Research Procedia*, 54, 909–917.

Kerner, S.M. 2022. Colonial pipeline hack explained: Everything you need to know. *TechTarget*, 26 April. Available at: <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know> [Accessed 6 July 2022].

Knox, J. 2015. *Coast guard commandant on cyber in the maritime domain*. US Coast Guard. Available at: <https://mariners.coastguard.blog/2015/06/15/6152015-coast-guard-commandant-on-cyber-in-the-maritime-domain/> [Accessed 27 May 2022].

Kovacs, E. 2014. Default password exposes digital highway signs to hacker attacks. *Security Week*, 6 June. Available at: <http://www.securityweek.com/default-password-exposes-digital-highway-signs-hacker-attacks> [Accessed 24 July 2020].

Kravets, D. 2009. Feds: Hacker disabled offshore oil platforms' leak detection system. *Wired*, 18 March. Available at: <https://www.wired.com/2009/03/feds-hacker-dis/> [Accessed 27 May 2022].

Ku, R. & Weiss, J. 2017. *Integrating security into the IoT strategy in the new converged environment*. Trend Micro.

KVH Watch. 2021. How using dedicated maritime IoT connectivity produces cost savings. *The Maritime Executive*, 27 September. Available at: <https://www.maritime-executive.com/features/how-using-dedicated-maritime-iot-connectivity-produces-cost-savings> [Accessed 24 June 2022].

Lomas, N. 2015. Samsung edits Orwellian clause out of TV privacy policy. *Tech Crunch*, 10 February. Available at: <https://techcrunch.com/2015/02/10/smarttv-privacy/> [Accessed 12 June 2017].

Marchant, N. 2021. *What is the Internet of Things?* World Economic Forum. Available at: <https://www.weforum.org/agenda/2021/03/what-is-the-internet-of-things/> [Accessed 24 June 2022].

McCue, A. 2003. 'Revenge' hack downed US port systems. *ZDNet*, 7 October. Available at: http://www.zdnet.com/article/revenge-hack-downed-us-port-systems/> [Accessed 27 May 2022].

McKee, M. 2019. Insider threats: Manufacturing's silent scourge. *Industry Week*, 25 April. Available at: <https://www.industryweek.com/technology-and-iiot/article/22027503/insider-threats-manufacturings-silent-scourge> [Accessed 24 June 2022].

Miller, B. & Rowe, D.C. 2012. A survey of SCADA and critical infrastructure incidents. Paper presented at the ACM Special Interest Group on Information Technology Education (SIGITE) Research in IT Conference, 11–13 October.

Min, H. 2022. Developing a smart port architecture and essential elements in the era of Industry 4.0. *Maritime Economics & Logistics*, 24, 189–207.

Molavi, A., Lim, G. & Race, B. 2019. A framework for building a smart port and smart port index. *International Journal of Sustainable Transportation*, 14(9) 686–700.

Pretorius, B.H. & Van Niekerk, B. 2020. Industrial Internet of Things security for the transportation infrastructure. *Journal of Information Warfare*, 19(3), 50–67.

Ragan, S. 2012. Railway network disrupted after cyber attack, report says. *Security Week*, 25 January. Available at: <http://www.securityweek.com/railway-network-disruptedafter-cyber-attack-report-says> [Accessed 24 June 2022].

Schiffer, A. 2017. How a fish tank helped hack a casino. *The Washington Post*, 21 July. Available at: <https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/> [Accessed 24 June 2022].

Solomon, H. 2022. Many OT products are 'insecure by design,' say researchers. *IT World Canada*, 22 June. Available at: <https://www.itworldcanada.com/article/many-ot-products-are-insecure-by-design-say-researchers/489735> [Accessed 24 June 2022].

Starr, M. 2014. Fridge caught sending spam emails in botnet attack. *CNET*, 19 January. Available at: <http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/> [Accessed 10 March 2015].

Sullivan, P. 2020. Critical IIoT security risks cloud IoT's expansion into industry. *Tech Target*, September. Available at: <https://www.techtarget.com/searchsecurity/tip/Critical-IIoT-security-risks-cloud-IoTs-expansion-into-industry> [Accessed 24 June 2022].

Swanbeck, S. 2015. *Coast guard commandant addresses cybersecurity vulnerabilities on offshore oil rigs.* Center for Strategic and International Studies. Available at: <https://www.csis.org/blogs/strategic-technologies-blog/coast-guard-commandant-addresses-cybersecurity-vulnerabilities> [Accessed 27 May 2022].

Theoharidou, M., Kandias, M. & Gritzalis, D. 2011. Securing transportation-critical infrastructures: Trends and perspectives. In C.K. Georgiadis, H. Jahankhani, E. Pimenidis, R. Bashroush & A. Al-Nemrat (eds.). *Global security, safety and sustainability & e-democracy.* Lecture notes of the Institute for Computer Sciences, Social Informatics and

Telecommunications Engineering, Volume 99. Berlin: Springer, 171-178.

Townsend, K. 2019. Industry is not prepared for the IIoT attacks that have already begun. *Security Week*, 30 May. Available at: <https://www.securityweek.com/industry-not-prepared-iiot-attacks-have-already-begun> [Accessed 24 June 2022].

Van Niekerk, B. 2017. Analysis of cyber-attacks against the transportation sector. In M.E. Korstanje (ed.). *Threat mitigation and detection of cyber warfare and terrorism activities.* Hershey, PA: IGI-Global, 68–91.

Vaughan-Nichols, S. 2019. FBI warns about snoopy smart TVs spying on you. *ZDNET*, 3 December. Available at: <https://www.zdnet.com/article/fbi-warns-about-snoopy-smart-tvs-spying-on-you/> [Accessed 24 June 2022].

Wagstaff, J. 2014. All at sea: Global shipping fleet exposed to hacking threat. *Reuters*, 24 April. Available at: <https://www.reuters.com/article/us-cybersecurity-shipping-idUSBREA3M20820140424> [Accessed 27 May 2022].

Warrick, J. & Nakashima, E. 2020. Officials: Israel linked to a disruptive cyberattack on Iranian port facility. *The Washington Post*, 18 May. Available at: <https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html> [Accessed 27 May 2022].

Woolf, N. 2016. DDoS attack that disrupted internet was largest of its kind in history, experts say. *The Guardian*, 26 October. Available at: <https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet> [Accessed 9 June 2016].

Zimmerman, G. 2017. Target settles HVAC data breach for $18.5 million. *FacilitiesNet*, 25 May. Available at: <https://www.facilitiesnet.com/hvac/tip/Target-Settles-HVAC-Data-Breach-for-185-Million--39237> [Accessed 24 June 2022].