The Threat of Cyber-Terrorism & Security in Intelligent Transportation Systems Architecture

Bingyi Han, Biyu Wu, Quan Nguyen, Rodrigo Camargo, Ignacio Arancibia

This research was conducted to satisfy the assessment requirements of the Enterprise Architecture core subject in the Master of Information Systems, The University of Melbourne.

This report acknowledges the mentoring support of Dr Rod Dilnutt, Industry Fellow, School of Information Systems, The University of Melbourne.

The University of Melbourne, 2019.

Table of Contents

Abstract

With the rise of political tensions around the world and the rapid advances in technology along with increased digitization of all sectors, cyber-terrorism has become a prominent threat. Societies increasingly evolving into smart cities become especially vulnerable to this threat. Intelligent Transportation Systems (ITS), due to their large-scale architectures and pervasiveness in smart cities become especially vulnerable to the threat of cyber-terrorism due to the high impact a disruption could cause in society. Cases of cyber-terrorism in ITS suggest that even though security threats have been traditionally addressed in a layered manner following the ITS architecture, current remaining challenges in security awareness, data exchange and the physical-digital divide continue to pose vertical stress across all layers. In order to tackle this issue, a transversal cyber-resilience model is proposed over the existing ITS architecture composed of layers in technical good practices, policies and standards, and organization and people.

Keywords: *Intelligent Transportation Systems, Cyber-Terrorism, Cyber-Security, Enterprise Architecture, Cyber-Resilience.*

Introduction

The threat of terrorism has been ever present, though have traditionally taken place in the physical domain (Ahmad, Yunos, and Sahib, 2012). However, with the exponential advancement of technology and as a result, the digitization of our society, this has given a new domain in which terrorism can exploit: the cyber domain, and hence the evolution of cyber-terrorism.

From the research of Brenner (2006), we understand that terrorism is aimed at creating chaos and demoralization of an entire civilian population at a grand scale, and thus the target of cyber-terrorism tends to be large-scale national infrastructure systems, of which, in the present day, exists in both the physical and cyber domains. Within the realm of national infrastructure systems; transportation infrastructure has particular importance in terms of promoting overall economic growth and prosperity of a nation or region (Démurger, 2001). As a result, national bodies around the world are taking strides towards deploying Intelligent Transportation Systems (ITS) into their national transportation infrastructures in hopes of increasing the safety, mobility, efficiency and sustainability of their transport systems (Lin, Wang & Ma, 2017).

Due to the nature and technology of ITS, it requires the migration of many processes and control systems within the transportation infrastructure to move into the cyber domain (Lin et al, 2017). As a result, ITS would be a major target for cyber-terrorism.

This paper aims to tackle this issue by figuring out: *How does the emergence of cyber-terrorism shape security measures in Intelligent Transportation Systems (ITS) architecture?*

Intelligent Transportation Systems Architecture

Intelligent Transportation Systems (ITS) are enterprise applications that aim to improve the efficiency and safety of transport systems. ITS is an umbrella term for many kinds of systems; it can do anything from warning drivers of traffic congestions to letting commuters know how many seats are left available in a train. In order for the ITS to have the maximum impact, its implementation must span across all areas of a transportation system. A comprehensive system architecture must be developed with the ITS is in order to successfully create value across the different parts of the system and successfully integrate all its parts. The four most prevalent and widely used types of ITS systems are: (1) Advanced Traveler Information System (ATIS) (2) Advanced Traffic Management System (ATMS) (3) Advanced Public Transportation System (APTS), and (4) Emergency Management System (EMS)" (Singh, 2015).

With the proliferation of affordable connected devices, ITS systems have grown to encompass more and more agents, which can, (1)perceive their environment, (2) have some control over their actions and (3) interact with other agents (Lin, 2017). Each new connected device that the ITS must interact must do so without providing a new vulnerability that can be targeted by malicious actors.

Most ITS have a 3-tier architecture as shown in figure 1 (Horan & Schooley 2005), and the institution layer is presented as a combination of the operations and service layer mentioned by Lin, Wang & Ma (2017):

1. **Transportation layer**: Data is collected and translated into information and knowledge. Agents are able to react to changes in the environment from the field devices.
2. **Communication layer**: It provides timely and accurate communication between the different parts of the ITS and enables the exchange and utilization of data.
3. **Institutional layer**: It provides a structure for organizations to implement, operate and maintain ITS efficiently, and it outlines the socio-economic infrastructure for various organizations.

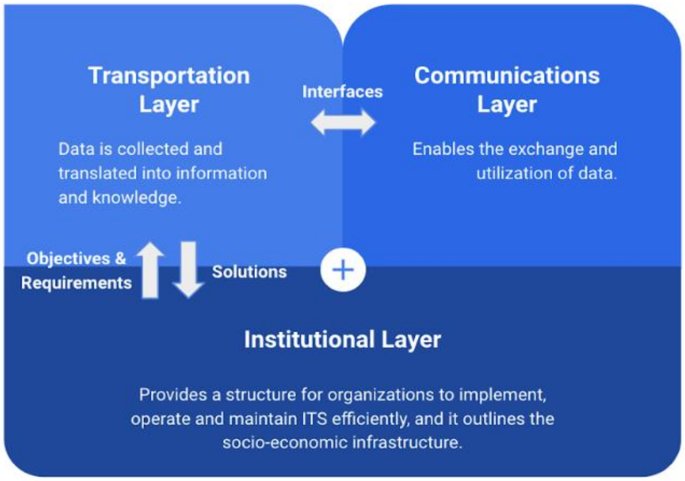

Transportation Layer
Data is collected and translated into information and knowledge.
Interfaces
Communications Layer
Enables the exchange and utilization of data.
Objectives & Requirements
Solutions
Institutional Layer
Provides a structure for organizations to implement, operate and maintain ITS efficiently, and it outlines the socio-economic infrastructure.

Figure 1: Current ITS Architecture (Horan & Schooley 2005)

Transportation Layer

The transportation layer is the physical ITS infrastructure where data can be collected. It defines the key players of ITS and identifies the transportation solutions in terms of subsystems, interfaces, fundamental functionality and data definitions, which are essentially required for each transportation service (Jamal, 2017a). This layer is regarded as the core of ITS architecture as it establishes a common terminology for ITS.

Multiple field devices will be required for traffic surveillance and motorist information dissemination, and some of the common pieces of equipment are inductive loop detectors, magnetic detectors, infrared and microwave, acoustic detectors, and video imaging (Jamal, 2017b).

Communications Layer

The communication layer enables the fast and precise exchange of information among different technical elements from the transportation layer for valid transportation solutions on the agents' side. The communication layer represents the types of information and means of communication, including wireless and wired communications, to support various ITS services (Jamal 2017b). It also sets up standards for data sharing and utilization by various physical entities or subsystems (Horan & Schooley 2005).

Institutional Layer

The institutional layer outlines the socio-economic infrastructure for various organizations including governmental-level agencies, public and private entities. The social roles of these organizations are also determined under this layer reflecting jurisdictional boundaries (Horan & Schooley 2005). The institutional layer includes elements that are required for effective implementation, operation as well as the maintenance of ITS. This layer is mandatory for an effective ITS program because the elements such as institutions, policies, funding mechanisms, and processes are crucial for providing solid institutional support and effective decisions (Jamal 2017a).

Cyber-Terrorism

Within the legal space, there are many terms being thrown around that may blur the lines of what exactly constitutes cyber-terrorism. What is the difference between a crime and an act of terrorism? What makes a cyber-crime different from a "regular" crime? First, one must break down these legal terms into classifiable components known as a taxonomy, as only then will a precise understanding of cyber-terrorism be defined (Brenner, 2006).

Based on the research of Ahmad et al (2012), several key factors have been selected to precisely identify and differentiate cyber-terrorism from other terms in the legal taxonomy. First and foremost is the question of "Motivation": acts of cyber-terrorism have an underlying political or ideological motive as opposed to personal motives that would constitute a cyber-crime (Cavelty, 2007). Secondly, comes the question of "Target": critical national infrastructures and industrial control systems such as electricity grids and air-traffic control systems are the key targets of cyber-terrorists as only attacks to such large-scale systems would bring about the desired "Impact": that is, a threat to national security and public safety that terrorists desire (Brunst, 2007). Fourth, is the "Tools of attack": being computer technology such as worms and bots to gain unauthorized access to a computer network (McGuire & Dowling, 2013). Finally, is the "Domain" through which an attack is deployed: in this case, the "cyberspace", which includes any "interdependent networks of information technology infrastructures" such as the internet, telecommunications networks and embedded industrial control systems (United States of America, 2009).

The Emergence of Cyber-Terrorism

Back in 1965, based on empirical observation, Gordon Moore proposed for the first time the concept of "Moore's Law", suggesting that every two years, computing power would double, implying an exponential growth curve in the capabilities and functions of computers over time (Schaller, 1997). This concept of exponential growth coupled with the concept of "Accelerating Returns": the idea that computers would be more powerful while simultaneously becoming much more affordable and accessible to people (Kurzweil, 2006), would indicate that it is not only the capabilities and functions of the computer that are increasing but also its influence and control over human life.

Lee (2013) has provided evidence that computers and information technology have substantially changed the way the world functions at an economic and social level. However, it has also subtly taken its control at a governmental and political level. The majority of nations in the world have their critical national infrastructures and industrial control systems such as electricity grids, water supply systems, air traffic control, financial service systems almost completely dependent on information technology. This means that they are all intertwined, interdependent and connected to a computer network, vulnerable to be exploited not just in the physical domain, but also the cyber domain (Murray, Johnstone & Valli, 2017).

The concerning issue is that there is a general lack of awareness and urgency in terms of trying to protect these infrastructures and control systems within the cyber domain (Estevez-Tapiador, 2004).

Within the global sphere, tensions are clearly on the rise and the risk of political interstate conflict is ever more present. The United Kingdom has already distanced itself from Europe and many major European powers are also following suit. The United States is losing its grasp as the "powerhouse" of the world and China and Russia are battling it out for power (Global Trends, 2018). Of late, the world has also experienced devastating terror attacks with harsh ideological and political motives such the recent bombings in Sri Lanka, the mosque attacks in New Zealand and the Paris bus attacks just to name a few (McKirdy, E., McKenzie, S., Hu, C., Said-Moorhouse, L., Kaur, H., Yeung, J. & Wagner, M., 2019).

When critical national infrastructures (of which Intelligent Transportation Systems are a part) are in such a vulnerable state in the cyber domain, coupled with rising political tensions, that we believe cyber-terrorism is now a major area of concern, and safeguards need to be put in place for this.

Case Analysis

Cases in Cyber-Terrorism and Intelligent Transportation Systems

As cyber-terrorism has emerged with the rise of digitization and interconnectivity, intelligent transport systems of different kinds have also become vulnerable to it. In 2016, a prominent case was reported in the San Francisco Municipal Transport System, where hackers aided by ransomware took over more than 2000 computers that operated the public transport system of the municipal agency (Gibbs, 2016; Newcomb, 2016). While the computers were left completely inoperable and showing a ransom message, the agency was forced to open all fare gates in order to minimise the impact on the public and the city itself (Gibbs, 2016). While the attack did not impact customers physically, or their data, the event has the potential to disrupt an entire functioning city (Newcomb, 2016).

A similar situation happened in 2017 when the notoriously famous ransomware 'WannaCry' affected several stations in Germany's Rail network. The train company Deutsche Bahn had their computers infected with the virus, leading to the ransomware message appearing on screens at train stations. Deutsche Bahn released a press statement revealing that due to the Trojan attack, the train network experimented system failures in various areas (Graham, 2017).

Civil aviation is not exempt from the risk of cyber-terrorism, as it heavily relies on "vehicle-to-vehicle" and "vehicle-to-infrastructure" communication technologies, along with complex system controls. In 2013, the commercial pilot and computer security expert Hugo Teso found that much of the flight plan and cruising altitude information of a plane, amongst other key metrics, were neither secure nor encrypted. Gathering and manipulating information of networks and radars linked to flight plans, he was able to come up with an android application called 'PlaneSploit' to gain control of an aircraft remotely, that he presented in the 'Hack in the box' security conference in Amsterdam that year. By doing this, he proved the possibility of cyber-hijacking an aircraft by manipulating in a remote fashion, flight variables such as speed, altitude, direction, and even cabin lights. All these factors, he believed, can be used to terrorize crew and passengers during a flight. Other experts have repeatedly backed similar experiments, being able to even hack into the identification and flight plan of high-profile aircrafts such as Air Force One (Heitner, 2014).

The rise of the cyber-terrorism risk does not only affect organizational or civilian data, it has the potential to threaten their safety and security. In 2019, the European Union Agency for Network and Information Security (ENISA) raised concerns about the EU legal framework for cyber-security in regard to the transport sector. By acknowledging the global and interconnected nature of today's transport systems, the ENISA called for the exchange of information and best practices, by including cyber-security as a regular agenda item for discussion in the meetings of the Aviation Security (AVSEC) and Maritime Security (MARSEC) Committees, Stakeholder Advisory Groups on Maritime Security (SAGMAS) and Aviation Security (SAGAS) as well as Land Transport Security Expert Group (LANDSEC) (Markovčić Kostelac, 2019).

This is not the first time that international bodies, as well as governments, have recognized the risks of cyber-terrorism for intelligent transport systems. By including different types of ITS, and even going ahead of time and taking into consideration autonomous vehicles (not limited to trains and metro systems, but also several types of driverless transport), countries such as USA, China and Australia strengthening laws and regulatory frameworks not only in regard to cyber-security, but also in relation to data and privacy protection on what is considered to be these public IoT devices (Lim & Taeihagh, 2018).

Cyber-Terrorism and Security Implications in Intelligent Transportation Systems Architecture

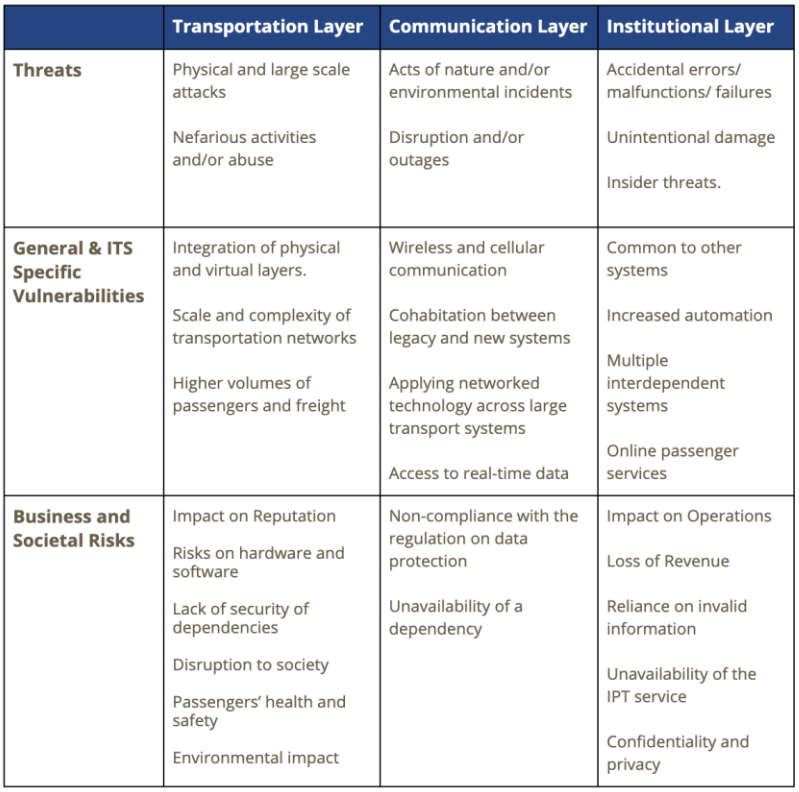
The complex multi-tier architecture across many different agents makes ITS especially vulnerable to cyber-terrorist attacks. The failure of an ITS system can not only disrupt the operations of a whole city, and put passengers at risk, but also put the financial information of the organization and the passengers at risk. As an organization's ITS continues to grow, they must assess the different Threats, Vulnerabilities and Risks (Levy-Bencheton and Darra, 2015, p21) that their system faces across all level of their system architecture; The European Union Agency for Network and Information Security (ENISA) provides organizations with a wide array of possible Threats, Vulnerabilities and Risks that their system may face.

Threats are potential causes of an incident that may result in harm to an ITS. ENISA has identified 7 main categories into which individual security threats fall into: (1) Physical and large scale attacks (2) Acts of nature and/or environmental incidents (3) Accidental errors/malfunctions/failures (4) Disruption and/or outages (5) Nefarious activities and/or abuse (6) Unintentional damage (7) Insider threats (Levy-Bencheton and Darra, 2015).

As ITS continue to grow, so does the need for integration amongst different types of system. Connections amongst systems and the exchange of information are especially vulnerable to acts of cyber terrorism. There are 5 general vulnerabilities that ITS share with most other enterprise systems: (1) Common to other systems (2) Wireless and cellular communication (3) Integration of physical and virtual layers. (4) Cohabitation between legacy and new systems (5) Increased automation. The 6 specific vulnerabilities are: (1) Scale and complexity of transportation networks (2) Applying networked technology across large transport systems: (3) Multiple interdependent systems (4) Access to real-time data (5) Higher volumes of passengers and freight (6) Online passenger services (Levy-Bencheton and Darra, 2015).

Risk is the impact to the organization that a threat successfully exploiting a vulnerability would cause. Risks are divided into business risks, which impact financial assets and normal operations, and societal risks, which affect the usage of the transportation system by the passengers. Business risks include: (1) Impact on Operations, (2) Loss of Revenue (3) Impact on Reputation (4) Non-compliance with the regulation on data protection (5) Risks on hardware and software (6) Reliance on invalid information (7) Lack of security of dependencies (8) Unavailability of a dependency. Societal risks include (1) Unavailability of the IPT service (2) Disruption to the society (3) Passengers' health and safety (4) Environmental impact (5) Confidentiality and privacy (Levy-Bencheton and Darra, 2015).

An organization looking to assess how these dangers can affect its systems across their multi-tier architecture can use the mapping we provide of the 3 layers stated by Horan & Schooley (2005) against the elements presented by ENISA.



	Transportation Layer	Communication Layer	Institutional Layer
Threats	Physical and large scale attacks Nefarious activities and/or abuse	Acts of nature and/or environmental incidents Disruption and/or outages	Accidental errors/ malfunctions/ failures Unintentional damage Insider threats.
General & ITS Specific Vulnerabilities	Integration of physical and virtual layers. Scale and complexity of transportation networks Higher volumes of passengers and freight	Wireless and cellular communication Cohabitation between legacy and new systems Applying networked technology across large transport systems Access to real-time data	Common to other systems Increased automation Multiple interdependent systems Online passenger services
Business and Societal Risks	Impact on Reputation Risks on hardware and software Lack of security of dependencies Disruption to society Passengers' health and safety Environmental impact	Non-compliance with the regulation on data protection Unavailability of a dependency	Impact on Operations Loss of Revenue Reliance on invalid information Unavailability of the IPT service Confidentiality and privacy

Table 1. Cyber-Terrorism effects on ITS Architecture

Discussion

Remaining Challenges

According to the risks and vulnerabilities defined from the previous section, three main challenges are identified through assessing each layer of the ITS architecture: Poor security awareness, Inefficient collaboration & data exchange, and Cyber-physical hybrid ITS assets & unclear security responsibilities. It is found that all those challenges have direct or indirect impacts on all three layers of the architecture at the same time:

Challenge 1: Inadequate Security Awareness

As mentioned in the previous section, low security awareness was found in all three layers of the ITS architecture. The high variety of cyber threats as well as the unclear security boundaries of intelligent public transportation systems are challenging to be fully managed by organizations within the transportation sector (US Department of Homeland Security, 2015). As a result, the interconnected components of ITS become even more complex as intelligent transportation develops.

Meanwhile, cyber-security isn't seen as a significant component in ITS and is paid minimal attention by various organizations including governmental-level agencies, public and private entities. Safety and security are still treated entirely separately in different categories due to the lack of security awareness. Often, intelligent public transportation operators would only take safety into consideration and would regard safety a higher level of importance than security due to a poor understanding of the significance of cyber-security (Levy-Bencheton and Darra, 2015, p31, p33).

This challenge directly brings weakness to the institutional layer, that results in the inefficient implementation of the security process at both the transportation layer and communication layer.

Challenge 2: Inefficient Collaboration & Uneven Data Exchange

The challenges of inefficient collaboration and inadequate data exchange in terms of cyber-security analytics can be found in two parties: transport organizations and ITS operators. These challenges are reflected in both the communication layer and the institutional layer of the existing ITS architecture.

Although the communication layer guarantees timely and accurate communication within ITS, the exchange of cyber-security related information is restricted among transport organizations due to both competitive pressure and incompatible systems for information exchange. The low levels of awareness of security information sharing, and the lack of necessary communication systems, pose a significant challenge for efficient utilization of data and effective avoidance of cyber-crimes within the sector (Levy-Bencheton and Darra, 2015, p32-33).

While the operators encourage collaborations and information sharing activities, the data exchange between ITS and operators (e.g. railways, local government etc.) is inadequate, inefficient and uncoordinated. This is potentially caused by incohesive security countermeasures deployed by different operators and their inadequate checking of the efficiency (Arshfold, 2011). An uneven data exchange will expose the operation of ITS and other smart cities systems to potential security threats since security issues aren't communicated (Levy-Bencheton and Darra, 2015, p32-33).

Challenge 3: Cyber-physical Hybrid ITS Assets & Unclear Security Responsibilities

As the ITS combines multiple societal function related assets into one with real-time intelligence under either wireless or wired communications, ITS assets are now exposed to a wider range of physical and security threats compared to the traditional silo-based transportation system. There are no clear boundaries between cyber and physical components since all assets are a cyber-physical hybrid under ITS (Levy-Bencheton and Darra, 2015, p19).

The operators and stakeholders are required to treat both cyber-security and physical safety as interdependent concerns since cyber-security networks will be affected if the physical operation of ITS assets is under attack. Both, the transportation and communication layers of the ITS architecture need to take the nature of cyber-physical hybrid ITS assets into consideration in order to prevent physical and security threats at the same time.

Since ITS is integrated into other smart city systems through data exchange and system collaborations, the boundary of ITS operator's network and security responsibilities needs to be better defined at the institutional level for more effective network risk assessments facing the broader range of cyber and physical attacks.

A Framework for Architectural Security and Cyber-Resilience in ITS

The group of challenges identified from the analysis of cases presented in this paper affect in a vertical fashion the ITS layered-architecture model. In consequence, and contrary to how traditional layered-security models for ITS have previously presented (Javed, Hamida, and Znaidi, 2016; Malygin, Komashinskiy, and Korolev, 2018; Chen, Sowan, and Xu, 2018), it also becomes necessary to address said challenges in a cross-layered way. The analysis of the evidence suggests that in order to build architectural cyber-resilience in Intelligent Transport Systems, the Cyber-Terrorism issue must be tackled by putting in place transversal measures across the entire architecture, as Figure 2 shows.

In order to correctly and comprehensively tackle the challenges presented, the Vertical cyber-resilience structure should be built on to the IT architecture from three main components aligned with what has been suggested by the European Union Agency for Network and Information Security (ENISA) (Lévy-Bencheton and Darra, 2015): (1) Technical Good Practices, (2) Policies & Standards and (3) organizational, people & processes.

Technical Good Practices

When creating solutions and integrating device development, organizations must set strict technology requirements and best practices for all of the systems they have control with, and all the communication channels within the systems.

Organizations that set and follow clear and concise best practices for all of their applications will minimize the risk of a technical vulnerability being breached in any of the systems, thus greatly reducing the likelihood that the whole system could be breached because one of its agents has technical vulnerabilities that could have been prevented (Yeh & Chang, 2007). Some of the policies organizations must create ensure implementation of secure digital access controls to networks and data through VPNs, encryption of all sensitive information, and using intrusion detection systems (Lévy-Bencheton and Darra, 2015).

Policies and Standards

With ITS becoming more intertwined with IoT, mobile devices, and virtual networks their number of connections and exchange of information multiplies exponentially. Organizations must strive to develop a clear and cohesive ITS architecture in order to set cross platform policies and standards for the way information is exchanged. Developers would have to ensure that applications follow the institutional rules and policies (Hone, & Eloff, 2002).

Each system and device would need to adhere to hardware and software policies that enable it to communicate securely with the rest of the enterprise; most importantly since all of the interactions across the communication layer are standardized, it can be monitored and secured in a scalable way.

Organizations can set clear policies and standards such as: building solutions with security in mind, adopt Disaster Recovery plans and backups, a clear separation of critical systems and non-critical systems, amongst other policies (Knapp, Franklin Morris, Marshall, & Byrd, 2009). These policies will help reduce the likelihood of an incident as well as ensure that the organization is prepared when an incident occurs (Lévy-Bencheton and Darra, 2015).

Organizational, People and Processes

The organizational, people and processes component will contribute to building cyber-resilience in ITS insofar as it brings together all main components/actors involved in the implementation of the ITS architecture. As the European Union Agency for Network and Information Security (ENISA) (Lévy-Bencheton and Darra, 2015) recommends, it becomes necessary that cyber-awareness is raised and built at all levels of the architecture, engaging all staff and management into training on the matter (Stewart & Lacey, 2012; Ki-Aries & Faily, 2017; da Veiga, & Martins, 2017). Said training should include all security guidelines and procedures in order to embed cyber-resilience as an asset into the culture (da Veiga, & Martins, 2017). Alongside this, organizational processes such as procurement should be guided by security requirements at the same level of importance as the functionality requirement. Lastly, monitoring should be done at both physical and digital level aiming to achieve a cohesive security management of ITS.

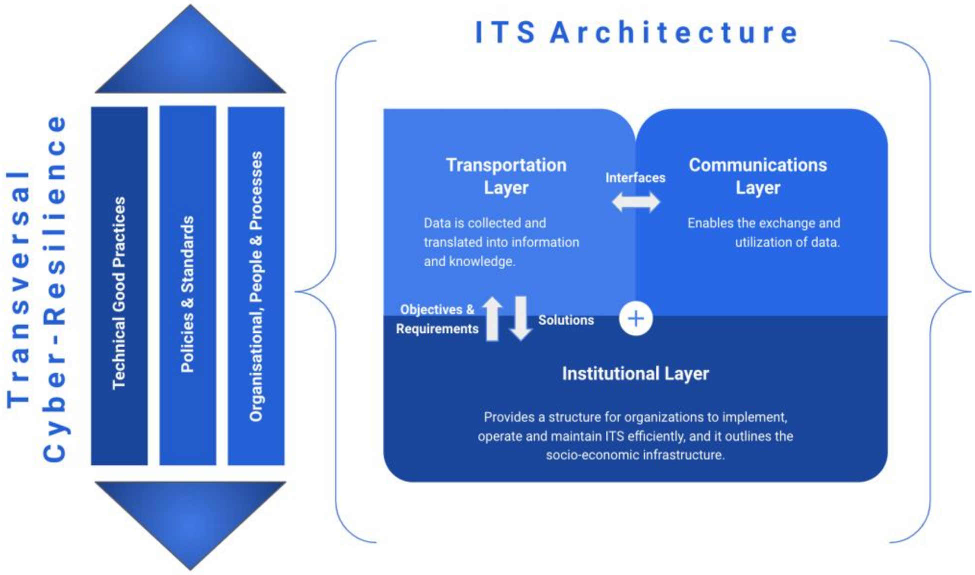

ITS Architecture
Transversal Cyber-Resilience
Technical Good Practices
Policies & Standards
Organisational, People & Processes
Transportation Layer
Data is collected and translated into information and knowledge.
Interfaces
Communications Layer
Enables the exchange and utilization of data.
Objectives & Requirements
Solutions
Institutional Layer
Provides a structure for organizations to implement, operate and maintain ITS efficiently, and it outlines the socio-economic infrastructure.

Figure 2. Proposed Framework for ITS Architecture with Vertical Cyber-Resilience Structure

Conclusion

As digitization and interconnectivity become more prominent in our cities' infrastructure, the rise of cyber-terrorism poses threats to intelligent transport systems of different kinds. The existing traditional multi-layer ITS architecture can no longer cope with the needs for cyber-security. Three major challenges are identified under the threat of cyber-terrorism: poor security awareness, inefficient security collaboration & data exchange, and cyber-physical hybrid ITS Assets & unclear security responsibilities. In order to comprehensively tackle the vertical challenges presented, ITS should adopt a transversal cyber-resilience model based on the current traditional three-layer architecture. The three main components proposed in the vertical cyber-resilience architecture will enable ITS to tackle cross-layered issues and deal with other potential risks, vulnerabilities and security threats.

References

Ahmad, R., Yunos, Z. and Sahib, S. (2012). Understanding cyber terrorism: The grounded theory method applied. In: *2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*.

Arshfold, W. (2011). *Security Think Tank: How can businesses measure the effectiveness of their IT security teams?*. [online] ComputerWeekly.com. Available at: https://www.computerweekly.com/feature/Security-Think-Tank-How-can-businesses-measure-the-effectiveness-of-their-IT-security-teams [Accessed 8 May 2019].

Brenner, S. W. (2006) 'Cybercrime, Cyberterrorism and Cyberwarfare', *REVUE INTERNATIONALE DE DROIT PENAL*, p. 453. Available at: https://search-ebscohost-com.ezp.lib.unimelb.edu.au/login.aspx?direct=true&db=edsbl&AN=RN216509560&site=eds-live&scope=site (Accessed: 3 May 2019).

Brunst, P. W. (2010) “Terrorism and the Internet: New Threats Posed by Counterterrorism and Terrorist Use of the Internet,” pp. 51-79.

Cavelty, M. D. (2007) “Critical Information Infrastructure: Vulnerabilities, Threats and Responses,” ICTs and International Security, pp. 15-22.

Chen, Q., Sowan, A. and Xu, S. (2018). A Safety and Security Architecture for Reducing Accidents in Intelligent Transportation Systems. In: *2018 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. [online] San Diego: ACM. Available at: https://eds-a-ebscohost-com.ezp.lib.unimelb.edu.au/eds/detail/detail?vid=0&sid=fbc03d81-c0ec-4642-b1b9-132ab89620fa%40sdc-v-sessmgr01&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=edseee.8587735&db=edseee [Accessed 1 May 2019].

da Veiga, A. and Martins, N. (2017) ‘Defining and identifying dominant information security cultures and subcultures’, *Computers & Security*, 70, pp. 72–94. doi: 10.1016/j.cose.2017.05.002.

Demurger, S. (2001) ‘Infrastructure development and economic growth: an explanation for regional disparities in China?’, *Journal of Comparative Economics* , 29(1), pp. 95–117. Available at: https://search-ebscohost-com.ezp.lib.unimelb.edu.au/login.aspx?direct=true&db=bas&AN=BAS185589&site=eds-live&scope=site (Accessed: 5 May 2019).

Estevez-Tapiador, J. M. (2004). ‘The Emergence of Cyber-Terrorism’ *IEEE Distributed Systems Online, Distributed Systems Online, IEEE, IEEE Distrib. Syst. Online*, (10), p. 4. doi: 10.1109/MDSO.2004.29.

Gibbs, S. (2016). Ransomware attack on San Francisco public transit gives everyone a free ride. The Guardian. [online] Available at: https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware [Accessed 28 Apr. 2019].

Global Trends (2019) ‘THE NEAR FUTURE: TENSIONS ARE RISING’. [ONLINE] Available at: https://www.dni.gov/index.php/global-trends/near-future. [Accessed 8 May 2019].

Graham, C. (2017). Cyber attack hits German train stations as hackers target Deutsche Bahn. The Telegraph. [online] Available at: https://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-target-deutsche/ [Accessed 28 Apr. 2019].

Heitner, K. (2014). Cyber Threats within Civil Aviation. Master Thesis. Utica College.

Hone, K, & Eloff, J 2002, 'What Makes an Effective Information Security Policy?', *NETWORK SECURITY*, 6, p. 14, British Library Document Supply Centre Inside Serials & Conference Proceedings, EBSCOhost.

Horan, T, & Schooley, B 2005, Inter-organizational Emergency Medical Services: Case Study of Rural Wireless Deployment and Management, Information Systems Frontiers, Vol. 7, Issue 2, p. 11.

Jamal, H 2017a, ITS Architecture / Hierarchy / Layers, viewed 29th April 2019, <https://www.aboutcivil.org/ITS-architecture-layers.html>.

Jamal, H 2017b, Physical Components and Devices in ITS, viewed 29th April 2019, <https://www.aboutcivil.org/ITS-physical-components-devices.html>.

Javed, M. A., Hamida, E. B. and Znaidi, W. (2016) ‘Security in Intelligent Transport Systems for Smart Cities: From Theory to Practice’, *Sensors (14248220)*, 16(6), p. 879. doi: 10.3390/s16060879.

Ki-Aries, D. and Faily, S. (2017) ‘Persona-centred information security awareness’, *Computers & Security*, 70, pp. 663–674. doi: 10.1016/j.cose.2017.08.001.

Knapp, K, Franklin Morris, J, Marshall, T, & Byrd, T 2009, 'Information security policy: An organizational-level process model', *Computers & Security*, 28, pp. 493-508, ScienceDirect, EBSCOhost.

Kurzweil, R. (2006). Sander Olson Interviews Ray Kurzweil. [Online]. Available at: https://www.kurzweilai.net/sander-olson-interviews-ray-kurzweil [Accessed: 2 May 2019].

Lee, K. (2013). Impacts of Information Technology on Society in the new Century. Lausanne. [Online]. Available at: https://www.zurich.ibm.com/pdf/news/Konsbruck.pdf. [Accessed 5 May 2019].

Lévy-Bencheton, C. and Darra, E. (2015). *Cyber security and resilience of intelligent public transport*. Heraklion: ENISA.

Lim, H. S. M. and Taeihagh, A. (2018) 'Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications'. doi: 10.3390/en11051062.

Lin, Y., Wang, P. and Ma, M. (2017) 'Intelligent Transportation System(ITS): Concept, Challenge and Opportunity' *2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids), Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2017 IEEE 3rd International Conference on, BIGDATASECURITY-HPSC-IDS*, p. 167. doi: 10.1109/BigDataSecurity.2017.50.

Malygin, I., Komashinskiy, V. and Korolev, O. (2018) 'Cognitive technologies for providing road traffic safety in intelligent transport systems', *Transportation Research Procedia*, 36, pp. 487–492. doi: 10.1016/j.trpro.2018.12.134.

Markovčić Kostelac, M. (2019). EU raises cyber-security awareness in transportation. Safety4Sea. [online] Available at: https://safety4sea.com/eu-raises-cyber-security-awareness-in-transportation/ [Accessed 28 Apr. 2019].

McGuire, M. and Dowling, S. (2013). *Chapter 1: Cyber-dependent crimes*. Cyber crime: A review of the evidence. UK Home Office.

McKirdy, E., McKenzie, S., Hu, C., Said-Moorhouse, L., Kaur, H., Yeung, J. & Wagner, M. (2019) 'Sri Lanka attack death toll rises to 290'. *CNN* [ONLINE] Available at: https://edition.cnn.com/asia/live-news/sri-lanka-easter-sunday-explosions-dle-intl/index.html. [Accessed 8 May 2019].

Murray, G., Johnstone, M.N., & Valli, C. (2017). The convergence of IT and OT in critical infrastructure. The Proceedings of 15th Australian Information Security Management Conference, 5-6 December, 2017, Edith Cowan University, Perth, Western Australia. (pp.149-155).

Newcomb, A. (2016). Who's Next, After San Francisco's Public Transit System Got Hacked?. NBCNews. [online] Available at: https://www.nbcnews.com/storyline/hacking-in-america/who-s-next-after-san-francisco-s-public-transit-system-n689216 [Accessed 28 Apr. 2019].

Schaller, R. R. (1997) 'Moore's law: past, present and future' *IEEE Spectrum, Spectrum, IEEE, IEEE Spectr*, (6), p. 52. doi: 10.1109/6.591665.

Singh, B. and Gupta, A. (2015) 'Recent trends in intelligent transportation systems: a review', Journal of Transport Literature, (2), p. 30. doi: 10.1590/2238-1031.jtl.v9n2a6.

Stewart, G. and Lacey, D. (2012) 'Death by a thousand facts: Criticising the technocratic approach to information security awareness', *INFORMATION MANAGEMENT AND COMPUTER SECURITY*, p. 29. Available at: https://search-ebscohost-com.ezp.lib.unimelb.edu.au/login.aspx?direct=true&db=edsbl&AN=RN309292502&site=eds-live&scope=site (Accessed: 2 May 2019).

United States Department of Homeland Security (2015) 'The future of smart cities: Cyber-physical infrastructure risk', p.10. Available at: https://ics-cert.us-cert.gov/Future-Smart-Cities-Cyber-Physical-Infrastructure-Risk

United States of America (2009) "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure" [Online]. Available: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. [Accessed: 2 May 2019]

Yeh, Q, & Chang, A 2007, 'Threats and countermeasures for information system security: A cross-industry study', *Information & Management*, 44, pp. 480-491, ScienceDirect, EBSCOhost.