INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research

International Journal of Critical Infrastructures

ISSN online: 1741-8038 - ISSN print: 1475-3219
https://www.inderscience.com/ijcis

Managing technological security of smart environment monitoring systems: study of a coastal province in Vietnam

Anh Tuan Hoang, Xuan Ky Nguyen

DOI: 10.1504/IJCIS.2023.10056422

Article History:

Received:	23 December 2022
Last revised:	13 March 2023
Accepted:	13 March 2023
Published online:	13 July 2023

Managing technological security of smart environment monitoring systems: study of a coastal province in Vietnam

Anh Tuan Hoang* and Xuan Ky Nguyen

Hanoi School of Business and Management,
Vietnam National University, Hanoi,
144 Xuan Thuy, Cau Giay,
Hanoi, Vietnam
Email: tuanha@hsb.edu.vn
Email: kynx@hsb.edu.vn
*Corresponding author

Abstract: With the machinery and systemic interconnections of the current 'Industry 4.0' world that we live in today, water critical infrastructures (CI) are crucial, interconnected with major urban entities such as medical and natural ecosystems. Environment monitoring technology (EMT), bounded to water CIs, providing the necessary real-time information for control and operation of urban water facilities, can become potential targets for physical or online attacks, disruption or destruction, imposing discomforts, outages and damages to affected water CI systems and related stakeholders, affecting the nontraditional security of affected region/cities. This is increasingly crucial as many cities in Vietnam are planning to implement digital transformation to become smart cities, creating multitudes of digital, internet connections, and numerous technological risks. In summary, this article attempts to analyse and draw conclusions about various aspects of technological security of environment monitoring systems (EMSs) of Quang Ninh, Vietnam and propose solutions that the city can apply to mitigate such nontraditional threats and prevent probable future incidents that can cause serious disruptions to such critical structures.

Keywords: critical infrastructure; technological security; monitoring systems; nontraditional security; smart city; Vietnam.

Reference to this paper should be made as follows: Hoang, A.T. and Nguyen, X.K. (2023) 'Managing technological security of smart environment monitoring systems: study of a coastal province in Vietnam', *Int. J. Critical Infrastructures*, Vol. 19, No. 4, pp.383–403.

Biographical notes: Anh Tuan Hoang is currently a researcher at Hanoi School of Business and Management – Vietnam National University, Hanoi. He has background in automation, environment monitoring. His research interests are technology management, technological security and technology aspects of sustainable development. He has co-authored books in technology and innovation management. He holds a Bachelor's in Electrical, Electronic and IT and Master's in Management of Nontraditional Security.

Xuan Ky Nguyen is a government official and currently working in Quang Ninh, Vietnam. He is currently pursuing his PhD at Hanoi School of Business and Management where his research is focused on sustainable development for environment and tourism. He holds a Bachelor's in Environment Engineering and Master's in Management of Nontraditional Security.

1 Introduction

Bradley and Bartram (2013) stated in their paper the importance of the act of monitoring domestic water qualities and monitoring results, standards are used for many purposes, including policy development, planning, system and program evaluation, benefit estimation and enforcement of regulatory compliance. Bradley implied that environment monitoring technologies (EMTs) have their uses but not without conflicting intentions due to the multitudes of applied scenarios and context such as different industries requirement, both regulatory and managerial.

Birkett (2017) in his paper mentioned the importance of water monitoring systems without which would cause considerable damage to water critical infrastructure (CI) if pathogens, viruses, poison are deliberately inputted into water CI systems. The paper also stated the needs for more advanced monitoring to assess wider range of foreign pollutants to water CI.

Current literature on environmental pollution indicates that increased human activities are adversely impacting world's water (Encinas et al., 2017; Dwiyaniti et al., 2020; Danh et al., 2020) and air quality as mentioned by Notardonato et al. (2019) and Corlan et al. (2021). This increased environmental concern as well as the use of advanced technologies such as the use of sensors and wireless electronic data collection systems are bringing new perspectives to the design of alternatives that may be considered for the monitoring technology. The primary purpose of an environment or water quality monitoring system is "to provide a system that would generate sufficient and timely information to enable the managers to make informed management decisions regarding the exposure health risk of the populations who are utilising this resource. The secondary purpose of water quality monitoring may include issues such as monitoring the quality of the environment for the essential needs of the habitat, identification of pollution sources and thus potential polluters, immediate initiation of clean-up operations after an accidental causing environmental damages, concerns on potential terrorism events and the use of the data collected to identify stringent rules and regulations to avert the adverse effects that may be caused by the consequential environmental degradation" (Telci et al., 2009).

EMT systems are parts of environmental/water CI (Shapiro and Maras, 2021; Kloosterman et al., 2022) and thus, inherit similar CI threats, vulnerabilities. Subsequently, the paper will adapt CI principles and concepts in analysing EMT technological issues. In Rehak et al.'s (2020) research concerning railway security, there are several elements of CI are key in selection of adequate security measures. Rehak et al. have identified numerous factors including: technical and process – of which require reliable foundation infrastructure and proper address of external and internal threats. Similarly, when Hedel et al. (2018) analyse EU framework for critical infrastructure protection (CIP), there are multiple threats mentioned, most prominently

cyber threats due to SCADA networks and physical threats pertaining to deliberate physical attacks and natural disasters.

Environment (water) monitoring technology (EMT) can ensure several benefits to the industries that deploy this type of systems, as conveyed by Encinas et al. (2017), including: improved environmental control, reduction of damage caused by potential environment disasters, reduction of environmental management costs.

Due to the overwhelming effect of environment pollution, over-exploitation (Dao, 2019) and climate change in Vietnam, environment monitoring, namely air and water monitoring have been in focus of the local government. Ministry of Natural Resources and Environment (MONRE), with multiple update directive[1] and circulars[2] issued within these past 5 years, has constantly updated new processes and requirements for compulsory air and water monitoring for various industrial and domestic sectors.

Quang Ninh (QN) Department of Natural Resources and Environment (DONRE) annual environment reports, obtained by direct request from the author, described multiple advantages of the province: possessing both natural resources as well as being in a geographical advantaged location, i.e., sharing water and land border with China have created many opportunities but also environment risks and threats to the province itself. With multiple planned nuclear reactors[3] and several highly populated industrial zones near its border, Quang Ninh is exposed to potential environment security threats from nuclear spillage, water discharge failures, etc.

Quang Ninh leadership understands the importance of environment monitoring system (EMS), as shown via the provincial effort in deploying the highest number of installed environmental sensors in the Northern region of Vietnam – 148[4] real-time and automated water and air monitoring stations over an area of 6,200 km^2.

This paper attempts to define the concept of technological security as well as assessment of technological security (TS) level for Quang Ninh – an important province of Vietnam, prone to many nontraditional security threats – in the context of EMSs, managed under Quang Ninh's DONRE.

2 Materials

2.1 Technological security

TS-related issues have been trending both in academia and industry. Recently there have been many technological accidents, i.e., cybersecurity incidents[5], technological disasters[6], etc., causing human and financial losses for reasons related to technology and technology system, i.e., the crash of the Boeing[7] aircraft's automatic control system; Takata[8] Corporation bankrupted due to errors in the production of airbags for many car manufacturers around the world, leading to many fatal accidents for users. US officials[9] have said cyberattacks impose deadly risks for the federal government, after the country's Energy Department was hacked by Russian hackers and nuclear codes may have been stolen.

Given the size and nature of technology-related industries, research on risk management, and technology risk management and subsequently, TS will be of great importance. There are more factors affecting technology and technological companies, involving several seemingly unrelated issues such as climate change, environment pollution, macroeconomic environment, etc. Weir et al. (2020) stated in the authors'

research regarding developers' challenges in this era involve more than the 'traditional security' common practice, involving dialogues with a 'range of counterparties'.

Furthermore with the emphasis and advancement of new 4.0 technologies such as internet of things (IoT), 5G infrastructure, smart city, will bring forth new risks as new and immature technologies are introduced into the current technology ecosystem and society, explained by Valerdi and Kohl (2004). Katina et al. (2017) also mentioned the difficulty of cyber governance with complex CI systems where software intertwines with hardware.

Quang Ninh is also one of pioneering province in implementing 'smart city' projects. Important city such as Ha Long will need to implement smart environment monitoring systems with requirements of complete automation, international standards, early monitoring capabilities and using real-time connection to realise its smart city goals. Parra et al. (2015) has emphasised on importance of accurate monitoring to achieve aims of smart cities.

Latest surveys in 2021 by multiple consulting firms such as EIU[10], AON[11], Protiviti[12] have affirmed the impact of TS threats/risks on business performance, of companies participated in such surveys. Top technology risks have been compiled and tabulated to show there are overlapped risks such as cyber threats; risks related to diseases; interruption due to new technology and environmental threats in Table 1.

Table 1 Current technology-related risks according to three surveys

Protiviti	*AON*	*EIU*
Pandemic-related policies impact business performance	Cyber attacks/data breach	Inter-state cyberwar
Adoption of digital technologies requires new skills	Business interruption	New COVID-19 variants resistant to vaccines
Inability to utilise 'big data' analytics for intelligence	Damage to reputation/brand	Famine-induced severe droughts
Cyber threats	Pandemic risk/health crises	China property crash
Resistance to business changes	Failure to innovate	Worsening US-China ties

Deloitte's[13] risk management survey of 94 financial institutions with total assets of more than $29.1 trillion, showed that only about half of those surveyed are confident in their group risk governance and are concerned about new and rising non-financial risks include: reputation; corporate sustainability; strategy; third party risks; political geography; and data integrity.

Technology has become very complex and sophisticated (Haines and Sharif, 2006) and with new emerging – often immature – technologies creating risks for the overall systems (Valerdi and Kohl, 2004).

The concept of TS is much aptly recent with seldom scholarly researches. The concept of technology-related security focuses on the aspect of ensuring safety (safety), stability/resilience for a particular technology system such as IT, in the studies of Jahankhani and Nkhoma (2009) and Chernyakov and Chernyakova (2018).

The introduction of the concept of a holistic technological security is a new and appropriate research direction, where processes and models of risk management have not yet offered an appropriate framework (Hubbard, 2009). The current Industrial

Revolution 4.0, when technology systems become multi-sectoral and multidisciplinary, demanding monitoring, analysis and management of more than one specific group of technological risks or threats (Oehmen et al., 2020).

As one of the first technology risk research firms, McKinsey[14], published an analysis of technology risk in 2016. This paper focuses on in banks and financial companies, the survey and analysis contents have pointed out the main risk groups, which are still relevant. McKinsey's general comments emphasised the lack of connection between technology risk management (TRM) activities and enterprise risk management (ERM).

An overall risk map developed by Kouns and Minoli (2010) as a continuation of the traditional risk management matrix, depicting specific risks that create hazards for the company and locates in which category those risks fall. There are four main groups of risks: external risks (natural disasters, terrorism, etc.), financial risks, business risks and operational risks.

Letete and Wallis (2014) in his research mentioned types of risks related to electricity distribution, which would also apply to environment monitoring systems due to the same complexity of components and control systems. That including some common risks, i.e., structural risk; growth risks; risks due to impacts from external sources; reputational risk – customer loss, failure to meet legal standards and regulations; technical/technological risks; degraded and damaged infrastructure; rapid changes in technology; changes in policies related to occupational health, safety and environment.

Carpignano et al. (2011) focuses on risk assessment of human safety (people safety) and environmental risk in his research. For human safety risks, the vulnerability factor is the person itself and the damage is the loss of life. For environmental risks, vulnerability factors are environmental components such as, rivers, lakes, groundwater, sea, air, and damage are expressed in resources that will have to be expended to restore components. above after being contaminated.

Specific papers that contained the term 'technological security' (TS) are summarised and tabulated. Most papers treat TS as safety of businesses or humans that interacted with the technology systems in Table 2.

Table 2 Definitions and/or descriptions of technology security by various papers and books

Ribeiro et al. (2019)	"The level of uncertainty that the business needs to understand and effectively manage to achieve its goals and create value".
Akhmetov et al. (2020)	Safety of environment, human health, prevention of threats.
Zhavoronkova et al. (2019)	"to protect research, production, technological and innovation activities from external and internal hazards and to ensure the economic stability".
Shabanov et al. (2019)	Safety and prevention of equipment failures.
Sun et al. (2020)	"the science and technology system … can maintain a safe and effective operation under the action of its own operation or under the external environment".
Geis and Melzer (2021)	"(TS) addresses deliberate threats from terrorists and naturally occurring … threats".

2.2 Security threats of EMTs

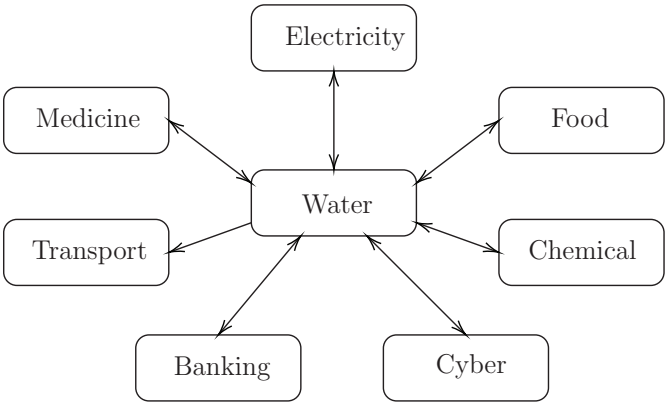
EMTs reside under water critical infrastructure (CI) that affect everyday lives as water is a crucial (Falkenmark, 2020) and non-negotiable essentials of human and society. Falkenmark highlighted several challenges pertaining to water in the next half of century, with multiple core functions: "regulatory, involving all the functions of soil moisture, evaporation and transpiration flows to regulate the Earth's energy balance and climate system through for instance carbon sequestration and water's ability as a greenhouse gas; productive, such as evaporation and transpiration to sustain food, biomass and bioenergy production; and moisture feedback, regulating the water cycle over land by evaporation. Water also has five different functions: water for societal supply, available to be withdrawn; water as a carrier of nutrients and pollution, and for transport; water as state, involving the function of water masses and storage; the productive function, for irrigation to produce food, and water to sustain aquatic growth; and the control function, regulating the Earth's energy balance, sea levels and geological processes, such as subsidence." Birkett (2017) coined the concept water critical infrastructure security (WCIS) and emphasised water CI as the most important CI which encapsulates global and human impacts, prone to terrorist attacks and exposed to multiple threats. Encinas et al. (2017) have mentioned the linkage and dependence of the quality of water (CI) with EMTs and thus it's sufficient to assume that EMTs issues would be directly related to water CIs. Furthermore, according to Birkett (2017), water CI are interconnected with other crucial CIs, depicted in Figure 1 such as electricity, medicine, etc. Scenarios such as inadequate water supply for cooling of nuclear reactors or thermal electric plants or no water input for filtration of clean water at the hospitals, would critically damage societies and humans that live within those societies.

Alcaraz and Zeadally (2015) mentioned crucial factors of CI such as stability, performance, safety as top priorities for countries around the world. Notably, the article mentions about the concept of security management in various categories of water including water distribution and generation, control of water quantity and quality – continues to be mentioned at the top of the list of components of CI. Alcaraz also points out that CI includes systems and assets, and the properties of this CI system or property can be physical or virtual. Affected CI could result in disruptions to groups of services that affect national security, the health of the economy, the health of society, or any combination thereof. Alcaraz also described technical, administrative and organisational security standards related to CI control systems. Similar risks, threats are mentioned by Popescu et al. (2021) in IOT systems, which bear much resemblance with EMS as there are more IOT technology being integrated in EMT systems to align with governmental requirements, e.g., in Vietnam require real-time, untouched datalogger signals of EMT monitoring stations to transmit to relevant local DONRE every minute the correct data of exhaust or wastewater of the installed facility.

Ivanenko (2020) proposed on important issues in protecting Ukraine's essential infrastructure, among which there are a number of important goals: companies of strategic importance, affecting the economy and national security; important subjects of the power sector system; state assets; terrorist attack, etc.

The ultimate goal is to prevent the emergence of new and reduce known risks of catastrophes by undertaking integrated and inclusive economic, structural, legal, social, health, cultural, educational, environmental, technological, political.

Figure 1 Water CI connection



Henrie (2013) described the problem of systems using the SCADA protocol related to the network security of the control system, critical to EMTs due to the fact that almost all modern monitoring systems employ SCADA as the communication and control protocol for corresponding series of environment sensors.

In general, EMT is similar to other developing technologies, which are exposed to multiple threats both from the technology itself and other external threats such as human errors, climate change where storms, floods could damage existing EMSs or cause delays to the sensors.

2.3 Concept of nontraditional security

The field of nontraditional security management (MNS) has emerged as a better comprehensive approach due to its interdisciplinary and human-focused nature. TS management will require a more specific and comprehensive management method, tools and philosophy. At the same time, the nontraditional security management landscape is changing as businesses and organisations shift their focus to more non-financial company performance indicators (Al-Nimer et al., 2021) such as sustainability, environmental protection, reputation, loyalty, employee satisfaction, safety, reliability, etc.

First introduced in terms of definition and concept in 2006 by Dosch (2006), the paper proposed a new security concept, with UNDP's recognition of the term simultaneously. The new definition of security focuses on institutions, governments, and people. "Security represents protection against the threats of disease, famine, unemployment, crime, social conflict and environmental disasters".

With Floyd and Croft (2011) MNS was soon applied in the European context, but now this definition is broader and clearly differentiated from traditional security management practices. The author has pointed out that today's (nontraditional) security needs to include environmental, social, political and economic security issues.

Srikanth (2014) in his assessment study, MNS presented six nontraditional security issues, including major issues such as environmental pollution, climate change, population distribution change, war, terrorism and conflict, network attack – involving many technologies. However, Srikanth's research paper still focuses on the topic of the

impact of these issues on the government, with the participation of the people, with the goal of ensuring national security.

Singh and Nunes (2016) interpreted the Copenhagen academic school of thought in a relatively interesting light, in which issues such as human rights violations, environmental degradation can become threats to national security once they require attention. government concerns and responses as well as solutions.

The concept of nontraditional security depicted by Hoang et al. (2022) is aligned with definition of general security proposed by Blokland and Reniers (2020) whereas: "security is the set of circumstances where the likelihood of intentional negative effects on objectives is low".

Thus, the concept of technological security can be adapted from Hoang, Blokland and Reniers, to be defined as "the set of conditions where likelihood of intentional negative effects on the safety, stability and sustainable development of the in-question technological system is low".

The concept of MNS is compatible with TS as the main goals of TS – according to the compilation of Table 2, at least would focus on safety of the environment, human health, of which are very aligned with researches from Hoang et al. (2022) and Phi et al. (2019). The concept of TS mentioned in this article also draws inspiration from the classical theory of technology determinism and socio-technology theory (Nograšek and Vintar, 2011) whereas technology is either the main factor or most important factor affecting the four main pillars of Leavitt's diamond model of: human, structure, process and organisational culture.

2.4 Research gap

There is a lack of a general concept and framework for technological security assessment and management as explained above. Global scholars have dwelled into the technology-related 'security' field with numerous researches – over 40,000 entries[15] in 'cyber security' in 13,000 entries in 'water security', approx. 15,000 entries in 'health security' the last 10 years. However, there still lacks research entries on technological security – six entries with the exact keyword, as shown in Table 2.

Locally, Vietnamese academia has started researches about TS-related issues such as cybersecurity in banking sector (Phuong and Dien, 2021), technological risks in finance industry (Nguyen and Pham, 2019). However, researches of TS or the more general – nontraditional security issue such as cybersecurity or finance security is still limited to the banking sector, IT industries. Without a holistic concept and framework for TS, there will be difficulties in integrating risks and security threats in multidisciplinary topics or issues that have wider spread across multiple industries.

2.5 Analysis method and conceptual model

This study attempt to validate the four factors (system, perception, risk management practices, human) using exploratory and confirmatory factor and SEM analyses. Items that did not fit were reassigned or omitted. Data collected is analysed with SPSS 20.0 and AMOS 20.0.

This study measured and investigated opinions numericalised by Likert scale of employees from Quang Ninh's DONRE and other provincial agency from 1 February

to 30 August 2022. The study considered personnel in multiple positions at those agencies to enhance the accuracy of answers. The direct effects of technological security factors (independent variables) on organisational financial and non-financial performance (dependent variable) were verified using the conceptual model shown in Figure 1.

2.6 Hypotheses and concept model

Phi et al. (2019) and Hoang et al. (2022) proposed a new research framework for management of nontraditional security (MNS), whereas the degree of nontraditional security of a subject, is expressed by a group of factors:

1 safety (S1)

2 stability (S2)

3 sustainability (S3)

4 (cost of) risk management (C1)

5 (cost of) crisis management (C2)

6 (cost of) crisis recovery (C3).

The overall effect is calculated as the sum of effect by S1, S2, S3 and deduction of the often negative effects of C1, C2, C3.

When describing TS, it is important to dissect aspects of technology and The Technology Atlas Team (1987) clearly identified four different aspects of technology, relevant in today context, that includes: technoware; humanware; infoware; orgaware. The authors have decided to integrate technoware and S1, S2 as one factor of Hoang et al. (2022) as safety and stability/reliability in TS is directly related to the technological systems themselves.

Perception of a new concept is very important in order to establish awareness of a new definition of threats such as TS threats. In order for policy makers to issue relevant and effective directives, circulars, perception of both public and governmental stakeholders is crucial, as depicted by Renn and Benighaus (2013) and Pidgeon (2021).

Kearns et al. (2005), in their study regarding technology management, describe six facets to technology that are referenced in this paper when creating the questionnaire. The study highlighted several principles and factors that were considered concurrently in this paper, which includes: technology experience; human factors; contingency plans; communication; evaluation; training and corporate support.

The application of MNS principles is carried out extensively in Quang Ninh, as mentioned in its provincial regulation memo. Therefore, it is appropriate to apply MNS constructs to assess how technological risks are affecting the organisation performance of Quang Ninh's Department of Environment (DONRE).

All constructs, including system factors, perception factors, risk management and human factors, organisational financial performance (OFP), organisational non-financial performance (ONFP), were measured by five-point Likert scales.

According to contemporary researches by Medina et al. (2009), Chatzoglou and Diamantidis (2009), Mackita et al. (2019) and Kouns and Minoli (2010) as well as reports by world leading corporations such as McKinsey, Marsh, all types of technology

security risks lead to losses/impacts on financial and non-financial organisational performance (OFP&ONFP): reputation; trust of customers; damage to property; damage to life/health; legal harm due to administrative fines or lawsuits. Loss of human lives is also one important factor to care for, mentioned by Yin et al. (2019). These properties are adapted for the OFP and ONFP variables in the analysis.

For the null hypothesis H0, it is assumed that TS has no effect on OFP and ONFP:

H0 TS affect neither OFP nor ONFP.

Naidoo and Hoque (2018) and Chatzoglou and Diamantidis (2009) have investigated the impacts of IT risks on firm performance where the technological (IT) systems have several factors that may potentially impact firm performance including: technology outsourcing; investment in new technology (machinery, method of production), etc. Yin et al. (2019) also mentioned other technical risks such as: lack of innovation; lack of advanced equipment; lack of talents in technical fields. Yin also mentioned about operational risks related to technology including technology operational errors, information security error. Therefore, the authors have decided to integrate all of these arguments into the system factors (S) that will affect OFP and ONFP:

H1a System factors affect OFP.

H1b System factors affect ONFP.

Renn and Benighaus (2013) and Yin et al. (2019) have pointed out the importance of having proper perception of technical risks in order for top management and relevant stakeholders to perform decision-making activities. Yin et al.'s (2019) study shows significant statistical significance between risk perception and performance. Peter and Robert (2016) also investigated the management perception on technological uncertainty – which is a factor belonging to the nontraditional security definition of Hoang et al. (2022) – and stated this is one important factors to manage. This leads to the second hypothesis:

H2a Perception factors affect OFP.

H2b Perception factors affect ONFP.

Yin et al. (2019), in their paper, have mentioned the impact of technical risks and (technical) risk perception on firm performance and emphasised the needs to have proper management framework such as COSO as the first step. As the focus of nontraditional security management is to minimise risks and have the best cost-benefit solution for implementing risk mitigation, it is necessary to consider risk management effect on OFP and ONFP in the nontraditional context of preventing losses:

H3a Risk management factors affect OFP.

H3b Risk management factors affect ONFP.

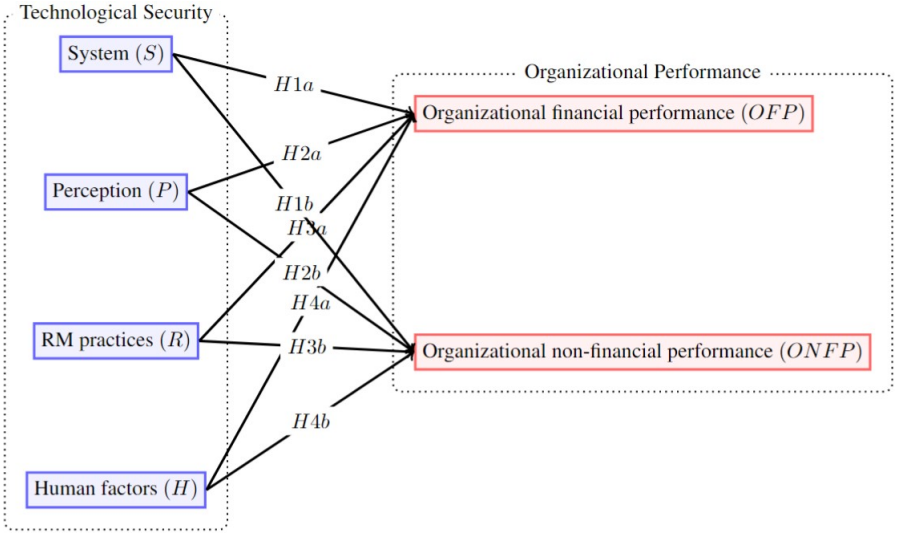
As the focus of nontraditional security is on human (Hoang et al., 2022) and human factor also contributes to impact on firm performance (Yin et al., 2019) such as lack of talent, safety risks for personnel which can be interpreted as the potential to have injury, loss of lives:

H4a Human factors affect OFP.

H4b Human factors affect ONFP.

The authors have compiled all hypotheses' arguments in a pictorial format as shown in Figure 2.

Figure 2 Theoretical model proposed (see online version for colours)



3 Methods

3.1 Design of questionnaire

As the participants are local DONRE and provincial personnel, all questions are translated and printed in physical copies and later scanned, cleaned and reorganised data for processing.

Table 3 Questionaire constructs

Construct	*Measurements*	*Sources*
Technological security		
System factors	44	Letete and Wallis (2014), Henrie (2013), Medina et al. (2009), Chatzoglou and Diamantidis (2009) and Yin et al. (2019)
Perception factors		
Risk management factors		
Human factors		
Financial performance	2	Kouns and Minoli (2010)
Non-financial performance	4	Mackita et al. (2019)

Independent and dependent variables are explained in Table 3, divided into four sections focusing on perception, risk management, system and human factors

of technological security that can affect organisation financial performance and non-financial performance.

All questions are opinion-based on Likert scale, with 1 being the least agreeable and 5 being fully agreed to the question. Participants will circle the most likely answer according to them.

4 Results

4.1 Descriptive

The survey as shown in Table 4 comprises of opinion questions and has returned several interesting results in their answers summary as most of the participants give very high answer above 4 (highly agreeable):

- most of the technology systems are from G7 manufacturers
- software's synchronicity is high and excellent compatibility with current hardware
- internet connectivity are high for systems under DONRE management
- frequent backups of data of systems
- failure of technology systems would cause damages in finance to the organisation.
- human errors are most concerning
- risks of policy changes are most concerning
- cybersecurity risks are most concerning
- good management of technological security is important in ensuring stability and safety of technology systems.

These opinions showing important technological risk factors affecting OFP and ONFP also coincide with researches' results from Kearns et al. (2005), Letete and Wallis (2014) and Alcaraz and Zeadally (2015).

Table 4 Questionaire results

Subjects	*Format*	*Collected*	*Responses*	*Ratio*
Quang Ninh DONRE and relevant agencies	Direct survey	200	150	75%
	Online survey	100	50	50%
	Total	300	200	63%

4.2 Reliability and validity

Exploratory factor analysis and confirmatory factor analysis (CFA) was conducted using SPSS 20.0 and AMOS 20.0 as well as Cronbach's alpha for each construct was calculated to be satisfactory, i.e., above 0.7. EFA factor loadings of all constructs are above 0.6 suggesting high correlation and reliability. The results affirm consistency and reliability of the constructs, as shown in Table 5. Other tests also returned positive results with Cronbach's alpha = 0.921 and KMO measure = 0.799.

Table 5 EFA and descriptive analysis of all factors

Constructs and descriptions	*Item*	*Mean*	*Std. dev.*	*EFA factor*
Human				
Professional personnel leaving the organisation	H1	3.28	1.05	0.649
Human risks are most concerning	H2	4.61	0.81	0.792
Perception				
Hardware risks are most concerning.	P1	3.97	1.05	0.721
Cybersecurity risks are most concerning	P2	4.54	0.67	0.792
Management of technological security is important to ensure stability, safety of systems	P3	4.18	1.12	0.786
Risk management				
Training corresponding response for different loss of technological security scenarios	RM1	1.79	0.84	0.658
Awareness of the concept of technological risks management	RM2	3.53	0.75	0.814
Presence of training and studying to enhance knowledge of technological risks management	RM3	3.22	0.75	0.656
Application degree of ISO 31000 in risk management	RM4	2.01	0.90	0.717
System				
Usage of G7 origin technology systems or equivalent	S1	4.08	0.82	–0.645
High localisation degree of the hardware	S2	2.56	1.11	0.825
High frequency of technology transfer project from vendors of G7 countries	S3	3.17	1.07	0.627
High frequency of technology transfer project from vendors of India/China/ASEAN countries	S4	2.39	1.11	0.680
Financial performance				
Losses related to technological equipment	FP1	1.24	0.78	0.779
Losses related to human lives/injuries	FP2	1.33	0.87	0.774
Non-financial performance				
Losses related to impacts on environment	NFP1	1.79	1.03	0.917
Losses related to reputation	NFP2	2.68	1.56	0.898
Losses related to professional staff leaving	NFP3	1.74	0.92	0.868
Losses related to legal issues	NFP4	2.07	1.15	0.806

4.3 SEM analysis

The SEM model results (Figure 3) show good model fit with the collected data, with Cmin/Df < 3, CFI > 0.9 and RMSEA $= 0.05$ with a significant Pclose $= 0.475 >$ 0. H1a, H2a, H2b, H3a have significant inferential p (<0.05) and therefore can be admitted.

The expert group are personnel working in the QN DONRE, with the nature of being public servants, are potentially less inclined to share information about the losses in hardware and human life. Therefore, the SEM analysis only found significant P values for H1a, H2a, H2b, H3a, i.e., different aspects affecting the non-financial performance

of the provincial DONRE overall. H2a is the most prominent hypothesis with the highest regression weighting, followed by H1a and H3a.

Table 6 CFI results

Model	*NFI Delta1*	*RFI rho1*	*IFI Delta2*	*TLI rho2*	*CFI*
Default model	0.759	0.687	0.928	0.900	0.923

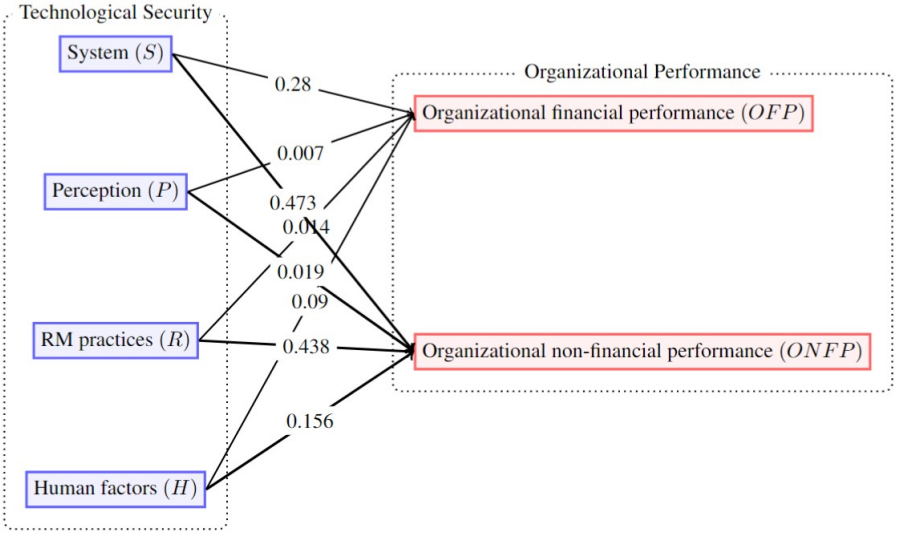
Table 7 RMSEA results

Model	*RMSEA*	*LO 90*	*HI 90*	*PCLOSE*
Default model	0.050	0.014	0.076	0.475

Table 8 Hypotheses SEM test results

Hypotheses			*Estimate*	*S.E.*	*C.R.*	*P*
OFP	←	System factors (H1a)	1.119	0.508	2.203	0.028
OFP	←	Perception factors (H2a)	–1.374	0.511	–2.689	0.007
OFP	←	Risk management factors (H3a)	0.882	0.358	2.462	0.014
OFP	←	Human factors (H4a)	–0.861	0.509	–1.693	0.091
ONFP	←	System factors (H1b)	–0.187	0.261	–0.717	0.473
ONFP	←	Perception factors (H2b)	–0.800	0.341	–2.349	0.019
ONFP	←	Risk management factors (H3b)	–0.148	0.190	–0.776	0.438
ONFP	←	Human factors (H4b)	–0.529	0.372	–1.420	0.156

Figure 3 SEM results of theoretical model (see online version for colours)



Based on the results obtained, it can be seen that H1a (system) and H2a (perception) has the most impact on OFP. From this result, we can also deduce that risk management

factors, often involving financial costs will have higher impacts on OFP – H3a, confirmed with results from Chairani and Siregar (2021).

It can be seen from the analysis results that in order to ensure technological security using nontraditional security methodology, an organisation needs to monitor and control aspects of technology system safety and stability (S1, S2) and effectively manage technological risks (C1), as well as enhancing the overall perceptions of involved stakeholders. This observation is aligned with Hoang et al. (2022) whereas the same factors are important for sustainable development.

5 Discussion

Our research contributes to the risk management literature in several aspects. First of all, management of nontraditional security is a new research area and is especially focused in Vietnam. As Vietnam and Quang Ninh in particular is preparing intensively for implementing smart city initiative, industry 4.0, technology security is an important aspect that need more in-depth researches. After SEM analysis with highly appropriate results, H1a, H2a, H2b and H3a are confirmed to have significant p value, i.e., $p < 0.05$. We can conclude from the results that TS mainly affect OFP and partially affect ONFP.

5.1 System factors of technological security

H1a implies that managers and leader of organisations need to control operations of technology systems efficiently, comprising of factors such as: maintenance partner, localisation degree of hardware/software, having equipment, systems transferred from countries of the G7 groups, have impacts on financial performance, i.e., reducing possible losses in equipment damage, losses involving human lives/injury. As a result, organisations especially in countries with similar traits as Vietnam in terms of economics, technology status should invest in better equipment, systems because for technologically advanced system such as EMSs, the most important aspect should be the durability and accuracy. Once these two factors are ensured, organisations can focus on effective management with the knowledge that data input from monitoring system is always dependable.

The author would also make the argument for H1b that system factors can affect non-financial firm performance as explained earlier about the nature of the participants answer can possibly be prone to skewness. It is very logical to assume that low quality equipment and low compatibility of interconnected systems (Stoel and Muhanna, 2009) can open organisations to possible failures causing reputation, customer losses when technology incidents happened affecting the public or the natural habitat. For the case study – Quang Ninh DONRE, being an governmental organisation, technological systems – EMSs' failure will cause damages to the provincial competitive index – PCI, affecting overall image and tourism potentials of the region.

5.2 Perception of technological security

H2a, H2b suggests that perception factors, namely the awareness which risks are concerning to the organisation in this case Quang Ninh's DONRE stakeholders are

aware of cybersecurity risks, hardware risks. Raising awareness of the importance of TS should be embedded in training plans of organisations as for when the degree of awareness of TS increases, top managers and subsequent department staffs will find it urgent to establish contingency plans, investment, recruitment, etc. H2a and H2b having inverse relationships (negative regression estimate) with OFP and ONFP suggests that as perception of technological security increases, financial and non-financial losses will decrease.

5.3 Risk management factors of technological security

H3a indicates that technological risk (C1) is important in preventing losses affecting OFP, which includes the tendency to organise training for technological risk events; understanding of management of TS; presence of training to improve knowledge on technology security; the degree of application of ISO 31000. These factors also coincide with researches by Chernyakov and Chernyakova (2018) and Oehmen et al. (2020). At the same time, in order to enhance risk management, organisation should invest in insurance as there are numerous insurance products in the market that can help protect the multi-million technology system that, e.g., Quang Ninh DONRE is managing. This can help with contingency events where systems failures happen and with the insurance compensation, new systems or components can be purchased immediately.

5.4 Human factors of technological security

Although both H4a and H4b is rejected ($p > 0.05$), the author would like to argue that with data sharing pattern from governmental agency, it is not fully possible for sensitive information such as personnel leaving, losses due to human errors to be fully expressed by the survey participants, as shared by Zhou et al. (2021), detailing in interviews about government agency willingness in sharing data. However, with H4a = 0.09 which is not far from 0.05, it can be partially concluded that human factors, in particular human risks and important technology personnel leaving the organisation can have impact on financial losses of an organisation such as Quang Ninh DONRE, e.g., lack of technology personnel can lead to system failure or late/incomplete maintenance of system components, software.

5.5 Managerial implications

The results of our study also provide some managerial insights involving technological security threats/risks. First, this study suggests that organisations and firms should involve efforts in creating better processes to raise awareness and training for better perception of involved stakeholders with technological security, which are the very prominent in organisations with multitudes of high-tech systems, is crucial (Ahmed et al., 2102). Managers with low awareness of the increasing complexity and uncertainty may take technological security management lightly, or they are not willing to invest in TS practices due to the up-front costs.

System overall factors involving safety and stability should be the utmost concerns of technology-intensive organisations as confirmed by H1a having highest impacts on OFP. There should be investments on quality systems from reputable firms from

G7 countries, who are already known for their engineering prowess and quality. Additionally, organisations should utilise technology transfer with partnered countries to improve overall quality of system. Modern and updated smart water management, as mentioned by Saiteja and Ponnapalli (2023), can in addition be applied for more proficient governance.

Confirmation of H3a suggests that organisation should spend time on training for different risks scenarios and have higher involvement from top management. At the same time there are factors that appear significant both descriptively and inferentially such as cybersecurity risks, human errors as well as using components from reputable G7 countries are very important in reducing non-financial losses, which are also not measurable by normal financial means – should be top concerns.

6 Conclusions

This study attempts to establish a relationship between technological security factors, particularly with the environment monitoring systems and performance of a governmental agency specialised in environment protection and management. Our results suggest that TRM contributes and have significant impact on non-financial performance of QN DONRE and provincial focus on better technological risks management is needed to prevent further consequences. The findings clarify the system, perception and risk management effects, of technology security all have considerable impacts on OFP and ONFP of QN DONRE.

The research conducted has also provided evidences that nontraditional security framework proposed by Hoang et al. (2022) can be utilised to analyse complex security problems. Additionally, the research has discovered with statistical association ($p \sim 0.05$) that human factors in nontraditional security, H4a and H4b, can affect organisational performance, especially where technology is involved extensively such as Quang Ninh DONRE. As nontraditional security focus is on human, this factor would be better monitored with deeper scrutiny in future researches.

There are limitations to the study as there are other systems besides monitoring systems that a DONRE is responsible of implementing and managing. At the same time, Quang Ninh does not represent all coastal areas of Vietnam, economically and environmentally, due to its high competitiveness provincial index – CPI[16] compared to other provinces, i.e., having better resources and higher provincial GDP. The human factors aspect still open spaces for further investigation as other scholars have studied the effects of human factors' impact on firm performance and this case should prove similar.

Further researches can investigate different coastal provinces and private companies specialising in this area for a wider confirmation of the effects of technological security of environment monitoring systems would have on performance of other provincial DONREs. Future researches for other technology – intensive industries would also confirm the validity and application degree of TS as well as TS management.

Acknowledgements

This research was funded by the research project QG.20.71 of Vietnam National University, Hanoi.

References

Ahmed, M., Sharif, L., Kabir, M. and Al-Maimani, M. (2102) 'Human errors in information security', *International Journal of Advanced Trends in Computer Science and Engineering*, Vol. 1, No. 3, pp.82–87.

Akhmetov, B.Z., Ustavich, G.A. and Dubrovskiy, V.A. (2020) 'Land and informational approach to the technological security of nuclear testing site economic use', *IOP Conference Series: Earth and Environmental Science*, Vol. 459, No. 4.

Al-Nimer, M., Abbadi, S.S., Al-Omush, A. and Ahmad, H. (2021) 'Risk management practices and firm performance with a mediating role of business model innovation. Observations from Jordan', *Journal of Risk and Financial Management*, Vol. 14, No. 3, p.113.

Alcaraz, C. and Zeadally, S. (2015) 'Critical infrastructure protection: requirements and challenges for the 21st century', *International Journal of Critical Infrastructure Protection*, Vol. 8, pp.53–66.

Birkett, D.M. (2017) 'Water critical infrastructure security and its dependencies', *Journal of Terrorism Research*, Vol. 8, No. 2, p.1.

Blokland, P.J. and Reniers, G.L. (2020) *The Concepts of Risk, Safety, and Security: A Fundamental Exploration and Understanding of Similarities and Differences*, Springer International Publishing.

Bradley, D.J. and Bartram, J.K. (2013) 'Domestic water and sanitation as water security: monitoring, concepts and strategy', *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, Vol. 371.

Carpignano, A., Nironi, C. and Ganci, F. (2011) 'Technological risk: a criterion for the optimisation of future eu energy supply scenarios', *International Journal of Energy Sector Management*, Vol. 5, No. 1, pp.81–100.

Chairani, C. and Siregar, S.V. (2021) 'The effect of enterprise risk management on financial performance and firm value: the role of environmental, social and governance performance', *Meditari Accountancy Research*.

Chatzoglou, P.D. and Diamantidis, A.D. (2009) 'IT/IS implementation risks and their impact on firm performance', *International Journal of Information Management*, Vol. 29, No. 2, pp.119–128.

Chernyakov, M. and Chernyakova, M. (2018) 'Technological risks of the digital economy', *Journal of Corporate Finance Research*, Vol. 12, No. 4, pp.99–109.

Corlan, R., Balogh, R.M., Ionel, I. and Kilyeny, S. (2021) 'The importance of indoor air quality (IAC) monitoring', *Journal of Physics: Conference Series*, Vol. 1781.

Danh, L.V.Q., Dung, D.V.M., Danh, T.H. and Ngôn, N.C. (2020) 'Design and deployment of an IoT-based water quality monitoring system for aquaculture in Mekong Delta'.

Dao, H.A. (2019) 'Attracting foreign direct investment in Vietnam – opportunites and threats', *Journal of Investment and Management*, Vol. 8, No. 2, p.53.

Dosch, J. (2006) 'The concept and management of non-traditional security in Southeast Asia', *Sicherheit & Frieden*, Vol. 24, No. 4, pp.179–184.

Dwiyaniti, M., Novita, W.R. and Tohazen (2020) 'Development of water quality monitoring systems in super intensive aquaculture system using ESP32 and Blynk', *ASAIS 2019*, pp.90–95.

Encinas, C., Ruiz, E., Cortez, J. and Espinoza, A. (2017) 'Design and implementation of a distributed iot system for the monitoring of water quality in aquaculture', *Wireless Telecommunications Symposium*.

Falkenmark, M. (2020) 'Water resilience and human life support – global outlook for the next half century', *International Journal of Water Resources Development*, Vol. 36, pp.377–396.

Floyd, R. and Croft, S. (2011) 'European non-traditional security theory: from theory to practice', *Geopolitics, History, and International Relations*, Vol. 3, No. 2, pp.152–179.

Geis, R. and Melzer, N. (2021) *The Oxford Handbook of The International Law of Global Security*, Oxford University Press.

Haines, J.D. and Sharif, N.M. (2006) 'A framework for managing the sophistication of the components of technology for global competition', *Competitiveness Review: An International Business Journal*, Vol. 16, No. 2, pp.106–121.

Hedel, R., Boustras, G., Gkotsis, I., Vasiliadou, I.A. and Rathke, P. (2018) 'Assessment of the european programme for critical infrastructure protection in the surface transport sector', *Int. J. Crit. Infrastructures*, Vol. 14, pp.311–335.

Henrie, M. (2013) 'Cyber security risk management in the SCADA critical infrastructure environment', *EMJ – Engineering Management Journal*, Vol. 25, No. 2, pp.38–45.

Hoang, P.D., Nguyen, H.Q., Nguyen, K.X. and Hoang, A.T. (2022) 'Management of nontraditional security for Vietnam's sustainable development: an integrated approach', *Sustainability: Science, Practice and Policy*, Vol. 18, No. 1, pp.696–709.

Hubbard, D. (2009) *Failure of Risk Management: Why It's Broken and How to Fix It*.

Ivanenko, O. (2020) 'Implementation of risk assessment for critical infrastructure protection with the use of risk matrix', *ScienceRise*, Vol. 2, No. 2, pp.26–38.

Jahankhani, H. and Nkhoma, M. (2009) 'Information systems security and its affiliation to information technology risk management', *Communications in Computer and Information Science*, Vol. 45, pp.195–204.

Katina, P.F., Keating, C.B., Gheorghe, A.V. and Masera, M. (2017) 'Complex system governance for critical cyber-physical systems', *Int. J. Crit. Infrastructures*, Vol. 13, pp.168–183.

Kearns, M.B., Taylor, J.B. and Hull, C.E. (2005) 'The six facets model: technology management in the effective implementation of change', *International Journal of Innovation and Technology Management*, Vol. 2, No. 1, pp.77–100.

Kloosterman, R.A., Herder, P.M. and van der Hoek, J.P. (2022) 'Enhancing the resilience of drinking water infrastructures', *Int. J. Crit. Infrastructures*, Vol. 18, pp.336–365.

Kouns, J. and Minoli, D. (2010) *Information Technology Risk Management in Enterprise Environments*.

Letete, M.M. and Wallis, M. (2014) 'Enterprise risk management in the generation and distribution of electricity: the case of Lesotho introduction', *Journal of Research and Development*, Vol. 1, No. 10, pp.1–33.

Mackita, M., Shin, S.Y. and Choe, T.Y. (2019) 'Ermoctave: a risk management framework for it systems which adopt cloud computing', *Future Internet*, Vol. 11, No. 9, pp.1–20.

Medina, H., Arnaldos, J. and Casal, J. (2009) 'Process design optimization and risk analysis', *Journal of Loss Prevention in the Process Industries*, Vol. 22, No. 5, pp.566–573.

Naidoo, I.P. and Hoque, M. (2018) 'Impact of information technology on innovation in determining firm performance', *African Journal of Science, Technology, Innovation and Development*, Vol. 10, No. 6, pp.643–653.

Nguyen, T.H. and Pham, T.H. (2019) 'Applying fintech in banking business in Vietnam – the inevitable trend of 4.0 era', *Journal of Trade Science*, Vol. 130.

Nograšek, J. and Vintar, M. (2011) 'Technology as the key driver of organizational transformation in the eGovernment period: towards a new formal framework', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Vol. 6846 LNCS, pp.453–464.

Notardonato, I., Manigrasso, M., Pierno, L., Settimo, G., Protano, C., Vitali, M., Mattei, V., Martellucci, S., di, F., Boccia, P. and Avino, P. (2019) 'The importance of measuring ultrafine particles in urban air quality monitoring in small cities', *Geographica Pannonica*.

Oehmen, J., Guenther, A., Herrmann, J.W., Schulte, J. and Willumsen, P. (2020) 'Risk management in product development: risk identification, assessment, and mitigation – a literature review', *Proceedings of the Design Society: DESIGN Conference*, Vol. 1, No. 3, pp.657–666.

Parra, L., Sendra, S., Lloret, J. and Bosch, I. (2015) 'Development of a conductivity sensor for monitoring groundwater resources to optimize water management in smart city environments', *Sensors (Switzerland)*, Vol. 15, No. 9, pp.20990–21015.

Peter, A. and Robert, E. (2016) 'Managing human resources and technology innovation: The impact of process and outcome uncertainties', *International Journal of Innovation Science*, Vol. 7, No. 2, pp.91–106.

Phi, H.D., Huong, V.N., Tuan, H.A. and Huynh, N.X. (2019) 'Management of nontraditional security: a new approach', *International Journal of Engineering, Applied and Management Sciences Paradigms*, Vol. 54, No. 1, pp.253–262.

Phuong, N.V. and Dien, T.V. (2021) 'Risks and challenges for cybersecurity in the banking sector in Vietnam', *HCMCOUJS*, Vol. 16, No. 2, pp.30–44.

Pidgeon, N. (2021) 'Engaging publics about environmental and technology risks: frames, values and deliberation', *Journal of Risk Research*, Vol. 24, No. 1, pp.28–46.

Popescu, T.M., Popescu, A.M. and Prostean, G. (2021) 'IoT security risk management strategy reference model (IoTSRM2)', *Future Internet*, Vol. 13, p.148.

Rehak, D., Slivkova, S., Pittner, R. and Dvořák, Z. (2020) 'Integral approach to assessing the criticality of railway infrastructure elements', *Int. J. Crit. Infrastructures*, Vol. 16, pp.107–129.

Renn, O. and Benighaus, C. (2013) 'Perception of technological risk: insights from research and lessons for risk communication and management', *Journal of Risk Research*, Vol. 16, Nos. 3–4, pp.293–313.

Ribeiro, J., Alves, V., Vicente, H. and Neves, J. (2019) 'Planning, managing and monitoring technological security infrastructures', *Lecture Notes in Electrical Engineering*, Vol. 505, pp.10–16.

Saiteja, S. and Ponnapalli, V.A.S. (2023) 'A review on smart water management in various domestic areas: an approach for water consumption and leakage perspectives', *Int. J. Crit. Infrastructures*, Vol. 19, pp.1–16.

Shabanov, B., Sotnikov, A., Palyukh, B., Vetrov, A. and Alexandrova, D. (2019) 'Expert system for managing policy of technological security in uncertainty conditions: architectural, algorithmic, and computing aspects', *Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2019*, pp.1716–1721.

Shapiro, L.R. and Maras, M-H. (2021) *Encyclopedia of Security and Emergency Management*.

Singh, N.K. and Nunes, W. (2016) 'Nontraditional security: redefining state-centric outlook', *Jadavpur Journal of International Relations*, Vol. 20, No. 1, pp.102–124.

Srikanth, D. (2014) 'Non-traditional security threats in the 21st century: a review', *International Journal of Development and Conflict*, Vol. 4, pp.60–68.

Stoel, M.D. and Muhanna, W.A. (2009) 'It internal control weaknesses and firm performance: an organizational liability lens', *Accounting Technology & Information Systems eJournal*.

Sun, D., Lu, S. and Sun, Y. (2020) 'Research on countermeasures for science and technology security problems in national defense science and technology industry', *ICEEMR*, Vol. 385, pp.39–42.

Telci, I.T., Nam, K., Guan, J. and Aral, M.M. (2009) 'Optimal water quality monitoring network design for river systems', *Journal of Environmental Management*, Vol. 90, No. 10, pp.2987–2998.

The Technology Atlas Team (1987) 'Components of technology for resources transformation', *Technological Forecasting and Social Change*, Vol. 32, No. 1, pp.19–35.

Valerdi, R. and Kohl, R.J. (2004) 'An approach to technology risk management', *Engineering Systems Division Symposium*, January, pp.1–8.

Weir, C., Rashid, A. and Noble, J. (2020) 'Challenging software developers: dialectic as a foundation for security assurance techniques', *J. Cybersecur.*, Vol. 6.

Yin, H., Chen, Z. and Xiao, Y. (2019) 'Risk perception affecting the performance of shipping companies: the moderating effect of China and Korea', *Maritime Policy and Management*, Vol. 46, No. 3, pp.295–308.

Zhavoronkova, G., Zhavoronkov, V. and Klymenko, V. (2019) 'Mechanisms for ensuring the region's technological security of law', Vol. 127, No. 4, pp.123–127.

Zhou, L., Chen, L. and Han, Y. (2021)) "Data stickiness' in interagency government data sharing: a case study', *Journal of Documentation*.

Notes

1 https://thuvienphapluat.vn/van-ban/Tai-nguyen-Moi-truong/Nghi-dinh-40-2019-ND-CP-huong-danthi-hanh-Luat-bao-ve-moi-truong-413905.aspx.

2 https://luatvietnam.vn/tai-nguyen/thong-tu-10-2021-tt-btnmt-bo-tai-nguyen-va-moi-truong-205541-d1.html.

3 https://tuoitre.vn/ung-pho-3-nha-may-dien-hat-nhan-trung-quoc-sat-bien-gioi-1185490.htm.

4 https://baotainguyenmoitruong.vn/quang-ninh-bao-ve-moi-truong-van-hanh-hieu-qua-148-tram-quantrac-347953.html.

5 https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020.

6 https://www.preventionweb.net/quick/70187.

7 https://www.nytimes.com/interactive/2019/business/boeing-737-crashes.html.

8 https://www.reuters.com/article/us-takata-bankruptcy-japan-idUSKBN19G0ZG.

9 https://www.nytimes.com/2020/12/17/us/politics/russia-cyber-hack-trump.html.

10 https://www.eiu.com/n/10-risk-scenarios-that-could-impact-global-growth-and-inflation-in-2022/.

11 https://www.aon.com/2021-global-risk-management-survey.

12 https://www.protiviti.com/us-en/survey/2022-and-2031-executive-perspectives-top-risks.

13 Deloitte's Global Risk Management Survey 12th Edition.

14 https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-ghost-in-the-machinemanaging-technology-risk.

15 semanticscholar.org.

16 https://pcivietnam.vn/ho-so-tinh/quang-ninh.