Cyber-threat Landscape of Border Control Infrastructures

Petros Chatzis (corresponding author), Eliana Stavrou
{petros.chatzis@hotmail.com, estavrou@uclan.ac.uk}
Applied Cyber Security Research Laboratory
University of Central Lancashire Cyprus
12 -14 University Avenue, Pyla
7080 Larnaca, Cyprus

Abstract

Various events in recent decades, such as the 9/11 tragedy and the European migration crisis, have highlighted the critical nature of robust borders and the impact of associated attacks on their integrity. However, it is unclear as to the extent to which cyber-attacks can threaten border operations. Interestingly, no extensive research has been conducted into this topic, possibly due to the complexity and diversity of border controls. This paper specifies the cyber-threat landscape of border control infrastructures to assist professionals in assessing the relevant cybersecurity risks. Border control infrastructures are complex environments and relevant risks might not be easily identified. To investigate the cyber-threat landscape of these infrastructures, a mixed research method, combining qualitative and quantitative results, and using border-related expert interviews and risk analysis investigation was chosen. Key contributions of this work include the classification of a widespread set of border assets, the description of the profiles of threat actors and their potential synergies, the specification of a threat taxonomy applicable to all border types, and the identification of potential areas of vulnerability. Moreover, through the risk analysis investigations, exemplary input is developed to guide professionals while applying a risk assessment methodology in the context of border control infrastructures. The paper concludes with future directions addressed to policy makers and border professionals.

Keywords: Threat profiling, threat modelling, cyber security, threat landscape, border control, critical infrastructure.

1. Introduction

In an era of globalization and growing displacement and movement of people, nations increasingly rely upon well-controlled borders. Protection against border attacks is of utmost priority and a key challenge for all nations, considering the recent border limitations imposed due to COVID-19 [1] and a series of events of the last decades, such as:

- **11th September attacks (USA, 2001):** Islamic terrorists entered the US by crossing the border illegally [2]. The events of 9/11 paved the way significantly towards hi-tech border controls [3].
- **Paris terrorist attacks (2015):** One of the terrorists had entered France illegally via Greece [4]. Strengthened border control measures were the primary European response to foreign fighters [5].
- **The EU migration crisis (2015):** Approximately one million irregular migrants arrived in the EU via the Eastern Mediterranean route. As a direct result strengthened management of the external border was implemented [6]. Expansion of the biometrics in border control was a main part of the proposed measures [7].
- In February 2020, Turkey announced it was **'opening the borders' to Europe** causing thousands of migrants to head (mainly) towards the Greek-Turkish land border. The European Union reiterated the importance of external border protection [8].

Despite the multiple dimensions of the examples presented, from geopolitical factors to terrorism threats, a common characteristic is that the reinforcement of the border controls using advanced technological systems was the immediate response of the countries; in fact, a "simple" border event, such as an illegal crossing, can have a severe impact on national security. So far, the existing literature and research on cyber-threat landscape evolves around relevant infrastructures to the border control, such as ports, airports or defense systems. A coherent overview of the cyber-threat landscape specifically addressing the border control infrastructures is a dimension which needs to be further explored.

There are various definitions for a 'border', but most describe it as the geographical boundary dividing one country from another. Some may be open or unguarded (e.g., intra-Schengen borders) and others may be fully controlled. In the latter case any border crossing other than through official land, air or maritime crossing points is prohibited, and consequently border surveillance (ground, air or maritime) is conducted by the authorities [9] as depicted in Figure 1.

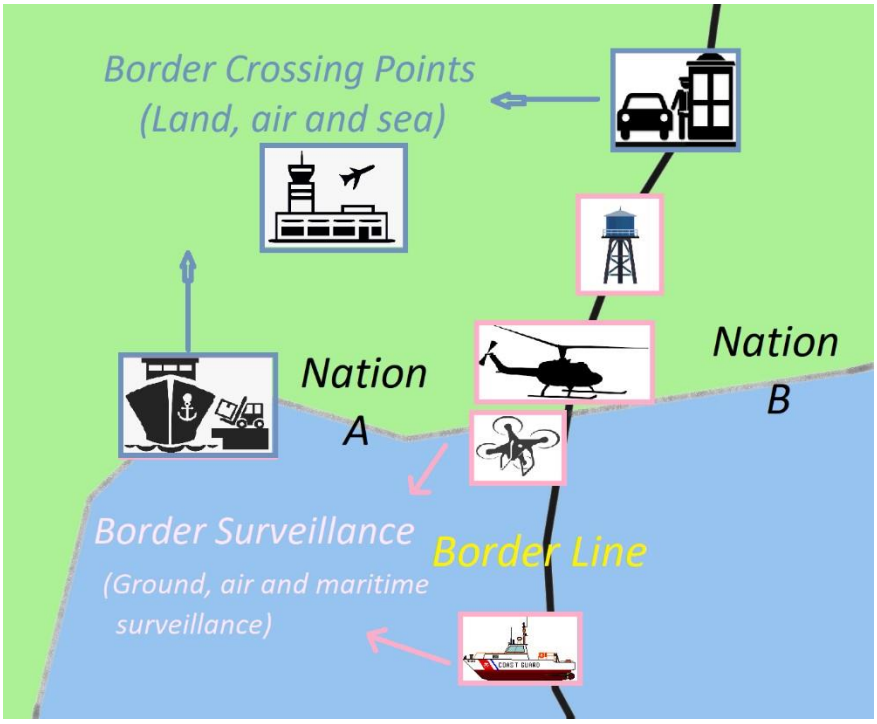

Figure 1: A high level representation of the border control landscape

Border control is most often a government responsibility, balancing the need to promote and expedite lawful trade and travel, while preventing the illegal movement of persons or goods, for instance terrorists, weapons, or drugs. Border management is increasingly turning to digital technology and ICT projects [10] [11] , whilst passenger data and biometrics are integrated into networks in multiple locations [3]. The interconnectivity of systems, people and processes, from travelers to advanced technological projects, showcase the strong link between the cyber and physical threat landscape relevant to the border control. The domino effect caused by such interdependencies [12], requires the integration of three elements throughout the analysis, in particular the physical, cyber and human [13]. Despite their criticality, border control infrastructures are not included as such in any of the lists of critical infrastructure sectors, e.g., the ones identified by the Cybersecurity & Infrastructure Security Agency (CISA) [14] or by the European Union [15].

Among the key controls that can be applied as part of a cybersecurity governance is risk management, identifying the threats, vulnerabilities, likelihoods and impacts on an organization's operations and assets. All these factors are utilized to determine the risks relevant to a specific infrastructure. As in the case of border control management, authorities need to have a solid understanding of the cybersecurity risks relevant to the borders' operations and assets to be able to select and apply the necessary controls to minimize, even eliminate, identified risks. So far, risk assessments are extensively applied in the context of critical infrastructures such as in healthcare, transportation, telecommunication, banking, etc. Furthermore, published work on assessing risks in a border control infrastructure context is limited. A wide understanding of border control management and its relevant infrastructure and threat landscape

is required, to be able to contact a comprehensive risk assessment, identifying relevant risks and responses.

This paper specifies the threat landscape of border control infrastructures to assist professionals in assessing the relevant cybersecurity risks. Border control infrastructures are complex environments and relevant risks might not be easily identified. Through this research work, a coherent overview of the borders' cyber-threat landscape is provided, revealing how widespread the attack surface at the borders is and the significance to protect them. To disject the complexity of border control infrastructures, identify key border control related components and specify the relevant cyber-threat landscape, extensive research, expert interviews, and a risk analysis-based investigation were utilized. Through the risk analysis-based investigations, exemplary input is developed to guide professionals while applying a risk assessment methodology in the context of border control infrastructures. Key contributions of this work include the classification of a widespread set of border assets, the description of the profiles of threat actors and their potential synergies, the specification of a threat taxonomy applicable to all border types, and the identification of potential areas of vulnerability. The paper concludes with future directions addressed to border professionals and policy makers.

Section 2 presents related work and section 3 discusses the research methodology. Section 4 briefly discusses relevant cyber-attacks against the borders, identifying trends related to the threat actors, their motivation, and synergies. The investigations are supported through interviews conducted with border experts and the relevant findings are also briefly presented. Section 5 applies a risk analysis approach to examine the cyber-threat landscape at border control infrastructures and to produce exemplary inputs to risk assessment methodologies when considered in a border control context. Section 6 presents the validation process with the experts and discusses future directions. Section 7 constitutes conclusions.

2. Related work

Several research works address the different border related aspects: Al-dhudhani et al. [11], Alkhammash and Alkhaldi [16] presented the emerging technology at the borders such as the Internet of Things, Artificial Intelligence and Cloud Computing; Wright et al. [17] assessed the developments in "smart" surveillance technologies in relation to privacy aspects, concluding that improvements are required; Papastergiou et al. [18], Yvon [19], Chiappetta and Cuozzo [20], Ahokas et al. [21] examine the ports and airports as critical infrastructures, underlining their susceptibility to cyber-threats. In parallel, there is vast literature on risk assessment methodologies for critical infrastructures and cyber-physical systems (CPS), such as the ones presented by Genge et al. [22], Paté-Cornell et al. [23], Tantawy et al. [24], whilst Yaacoub et al. [25] survey the main aspects of CPS. Unfortunately, risk assessment investigations are

limited in the context of border control infrastructures. Existing taxonomies and risk management approaches for critical infrastructures do not provide a sufficient basis to gain a solid understanding of all the components entailed in these infrastructures to be able to effectively apply a risk assessment methodology. For example, the Frontex risk methodology focuses on the migratory pressure [26], not considering in-depth the various physical and cyber threats, while ENISA threat taxonomy [27] is not addressing key border threats already identified in this work such as the travelers' unauthorized entry / exit or the concealment of goods.

Due to the complexity of border control infrastructures, applying a risk assessment methodology is not an easy task to perform, especially if the assets, processes, and threat landscape are not well specified. Through the analysis provided in this paper, the complexity of border control infrastructures is disjected, making evident all assets, and specifying the relevant threat landscape.

3. Methodology

The research methodology applied in this work consisted of four phases, in particular:

Phase 1 - Scope definition: To examine the cyber-threat landscape at the borders, a mixed research method, combining qualitative and quantitative results, and using expert interviews and risk analysis-based investigation was chosen. This approach was necessary to disject the complexity of border control infrastructures and identify all relevant elements. Authors would like to highlight that the cyber-threats on the borders cannot be assessed in isolation to the physical threats as they are interlinked and, therefore, various elements of the physical assets, threats and actors are incorporated for the needs of the paper.

Phase 2 - Data collection: Initially, an extensive web research and literature review was conducted to gain an overview of the borders' cyber-threat landscape. A range of research databases was used for identifying suitable papers, mainly ACM Digital Library, Springer Digital Library, IEEE Explore, Elsevier ScienceDirect, and searching Google Scholar, using general keywords (e.g., "critical infrastructures", "cyber-threats", "cyber-attacks", "border control infrastructures", "borders", "border surveillance", "border checks") and more focused ones with necessary combinations (e.g., "Border cyber security", "border security incidents", "border hacker attacks", "border vessel attacks", "border threats", "biometrics", "airports", "ports"). The research was complemented by a google search using similar keywords and structure, focusing mainly on publications and studies, with special attention to the ones of relevant US and European Agencies and bodies, such as the US Department of Homeland Security, Customs and Borders Protection, EU Commission, Frontex and ENISA. Only refereed papers at conference

and journal publications were chosen, along with publications by well-known bodies or companies, focusing on the timeframe between 2010 and 2020, with variations when required e.g., recent papers in the last 5 years for the cyber-threat landscape. In several occasions, the research was extended to citations or authors.

A challenge faced was the limited number of sources matching the scope of the research. For example, there is a range of papers examining different border dimensions, from fundamental rights to geopolitical dimensions, but none was identified examining the borders as a critical infrastructure, which could further be used as an input. Therefore, to a great extent the research incorporates different elements from different papers, reports and studies; approx. 120 sources were chosen for further review after reading the title and the abstract and 75 out of them were close to the scope, ruling out the rest. Based on this challenge and in order to gain a more concrete input, a search on known cyber-attacks at the borders was conducted, reviewing the CSIS list of major cyber-attacks [28] and utilizing Google Scholar and normal Google search. The outcome of the research provided initial insights on the border control infrastructure threat landscape and was used as an input for interviewing the experts, in particular choosing the proper profiles and drafting the questionnaires for each interview.

Research insights were further enhanced through the input provided by six experts with proven experience in their field, with each expert representing a different dimension of the border control infrastructure (as depicted in Figure 1). Specifically, the experts' group consisted of three border guards who carry out checks at an international airport, a seaport, and a land border crossing-point respectively, and three experts who conduct border surveillance tasks (Green Border Surveillance Officer, Coast Guard Officer and UAV expert). A tailor-made questionnaire per expert's profile was drafted as the basis for the interview, which aimed at identifying the organization's mission and objectives, main technologies in place and data-flow, technological and other assets and the existing threats and threat actors. An essential aspect of the interviews was to keep basic principles in order to avoid bias, preserve confidentiality and ensure the maximum insight for the research needs. Each expert was interviewed separately, and in total six interviews were conducted, with a duration of two hours each on average. The interviews were based on open ended questions (e.g., "can you describe the main threats and threat actors in your unit?"), allowing the interviewees to give their insights or illustrate examples and they were adjusted to the profile of each one of them e.g., the Coast Guard officer was interviewed on all topics related to the maritime affairs.

Summarizing, the data collection phase consisted of a) extensive research on papers, studies and reports for a general overview and b) identification of cyber-attacks to understand the trends in the context of border control infrastructures. Both were used as a basis for interviewing experts in the field.

Phase 3 - Risk assessment investigations and synthesis of threat landscape: The outcome of the extensive research and the outcome of the interviews were utilized in a risk assessment methodology that was applied to analyze the threat landscape at the border control infrastructures and provide exemplar input to professionals to assist in carrying out a comprehensive risk assessment. The risk assessment investigations consisted of the key steps in NIST SP 800-30 [29] (Figure 10), in particular:

a) Description of the organizational context, functions and asset identification. An asset register is specified as this is the first step before assessing the threats and relevant vulnerabilities.

b) Threat assessment: threat actors, their profiles and potential synergies are identified. Moreover, an elaborated taxonomy of relevant border control infrastructure threats is presented to gain a clear view of the threat landscape.

c) Vulnerability and impact assessment: description of factors and areas of vulnerabilities and description of potential impact are briefly analyzed. The aim here is to provide a basis and guide professionals to identify and elaborate details on specific vulnerabilities that are relevant for a specific type of border control infrastructure.

Phase 4 - Validation: A second round of separate interviews for validation was performed with the same experts (ref. Phase 2). All principles followed in phase 2 were applied and each interview consisted of a brief presentation of the findings delivered to each expert (identified assets, vulnerabilities, impact), followed by a bespoke discussion based on their area of expertise and their initial input. The duration of each interview was two hours and a tailor-made questionnaire with open ended questions was used to facilitate the oral discussion and validate the findings.

4. Existing attacks to the borders

This section briefly discusses recent cyber-attacks against the borders and provides valuable observations as to the trends that are observed related to borders' threat landscape. The aim was not to produce an exhaustive list of all border related attacks but to gain an initial overview, which served as an input for the risk analysis investigations, along with the interviews conducted with the experts.

4.1 Cyber-Attacks against borders

Research was conducted on border-related cyber incidents during the years 2015-2020 (Table 1), using the CSIS Major Attacks list [28] and extensive web search to identify trends and other useful information related to borders' cyber-threats. Qualitative assessment by the authors was required for characterizing the attacks as border control related ones, due to the limited number of cases identified, possibly due to

the discretionary nature surrounding the topic. In addition, several incidents were ruled out for a range of reasons: not directly related to the borders, e.g., espionage on law enforcement staff, limited info available or repeated cases, such as attacks to ports and airports. The cyber incidents were selected based on key border characteristics, such as the movement of specific traveler groups, ICT infrastructure, e.g., biometric systems, surveillance and communications equipment and means, e.g., vessels, UAVs, etc.

Table 1: Cyber-attack case studies

CASE ID	Date, Area	Incident	Description
N.1	2020 Oct., UK	Cyber-attack on International Maritime Organization (IMO) [30]	IMO reported that its website and networks had been disrupted by a sophisticated cyberattack against the IT systems, despite the robust security measures. Threat actors, motive and techniques used remain unknown.
N.2	2020 May, Iran	Major port in Iran disrupted [31]	Israeli hackers disrupted operations at a major Iranian port by attacking the computer systems, causing traffic jams and delays. The attack is possibly a retaliation for a failed Iranian cyberattack on an Israeli water facility.
N.3	2020 May, UK	Chinese hackers attacked Easyjet airline [32]	Chinese hackers accessed the travel records of nine million customers of Easyjet using highly sophisticated tools. It is believed that the same group of hackers had previously targeted travel data to track the movement of specific individuals.
N.4	2019 Sep., Asia	China hacked Asian telecoms to spy on Uighur travelers [33]	According to Reuters, China launched an espionage campaign tracking the movements of Uighurs, a minority perceived as a security threat. Chinese hackers compromised telecom operators in various countries.
N.5	2019 Aug., South Korea	Breach in biometric system used by banks, police and defence firms [34]	Security researchers found that Biostar 2's database of Suprema, a top security manufacturer, was unencrypted allowing access to millions of personal records and data, e.g., fingerprints, passwords and facial recognition details.
N.6	2019 Jul., USA	A US Coast Guard vessel was infected by malware [35] and [36]	Specialists found that malware had degraded the functionality of a vessel. The US Coast Guard issued a safety alert, implying that external media had caused the incident.
N.7	2019 Jun., USA	US Customs travelers' photos were exposed [37]	Perseptics, a company cooperating with U.S. Customs and Border Protection, experienced a cyber extortion attack. When no ransom payment was paid, the perpetrator started encrypting the company's network. Traveler's photos and license plate information were uploaded to the dark web.
N.8	2018 Jun., USA	A hacker downloaded US drone secrets [38]	MQ-9 Reaper drone is used for unmanned surveillance missions, including border control. A hacker accessed its sensitive files, exploiting router vulnerabilities used by military staff, and attempted to sell them.
N.9	2017 Dec., Taiwan	China accessed data on Taiwan's e-Gate system [39]	Since 2011, Taiwan has used biometric e-Gates allowing fast-track passport control at three main airports. Liberty Times newspaper was informed that the border security system, manufactured by a Chinese company, might have been compromised, allowing the Chinese Government to use a pre-installed 'backdoor'.
N.10	2015, USA	US Border Patrol drones hacked by drug cartels [40]	An Officer of the US Department of Homeland Security confirmed that drug traffickers invest in spoofing and jamming GPS systems, used by the border drone technology.

4.2 Borders' cyber-threat landscape trends

The analysis of the border related cyber incidents revealed interesting trends related to threat sources, their capabilities, motivation, and impact. The findings are summarised and presented following NIST definitions and categorisation [29]. Moreover, the insights gained from the cyber incidents' analysis were utilized as input to the interviews performed with the border-related experts to draw more conclusions and develop a solid understanding of the borders' cyber-threat landscape.

Most case studies had adversarial threat sources, mainly Nation States, cyber-criminals or criminal groups (Table 2). As to be expected, the capability of Nation States is substantial, with a high level of expertise and resource, and the possibility to carry out multiple and coordinated attacks.

Table 2: Threat actors

Type of Threat Source / Actor	CASE ID (ref. Table 1)	Capability
Accidental		
User	N.6	Low
Adversarial		
Established Group	N.10	Moderate
Individual / Outsider	N.7, N.8	Low
Nation State	N.2, N.3, N.4, N.9	High
Structural		
Software	N.5	Low

Motivations include espionage, economic or technological advantage, profit, or disruption, possibly caused through negligence. Travel industries and control systems can be targeted by mass digital surveillance campaigns (CASE ID N.3, N.4, N.9).

Third-party service provider vulnerabilities (CASE ID N.5, N.7), or those of various secondary assets (CASE ID N.8) might be exploited. Some cases involved accidental leakage (CASE ID N.5) and social engineering (CASE ID N.6). In most of the cases, operations or assets were harmed (damage to image, inability to perform business functions, or damage/loss of information assets and intellectual property). Further impacts included harm to national security or individuals, mainly due to theft of personal information (Table 3).

Table 3: Impact caused by the cyber-attacks

Impact	CASE ID (ref. Table 1)
Harm to assets	
Damage to information assets	N.1, N.3, N.7
Loss of intellectual property	N.8
Harm to individuals	
Identify theft, loss of personally identifiable information	N.3, N.4, N.7, N.9
Harm to Nations	
National security or loss of government continuity of operations	N1, N.2, N.8, N.9
Harm to operations	
Damage or loss of information assets / intellectual property	N.1, N.3, N.7, N.8
Damage to image / reputation / trust relationships	N.1, N2., N.3, N.5, N.7, N.8
Inability to perform current business functions	N.1, N.2, N.6, N.7, N.10

4.3 Consolidated results of interviews with Experts

As discussed in section 3 Methodology, 6 experts were engaged in the context of this research work and provided their input in phase 2 – Data collection and phase 4 - Validation. The interviews conducted as part of phase 2 provided useful insights in relation to the border control infrastructures, starting from understanding the organizational context, along with their complexity:

- Multiple organizational assets are in place, and the number of technological means used is constantly growing; two decades ago, patrol vehicles, dogs and even station's databases were used, whereas today international databases, air surveillance, advanced communication systems and biometrics are part of the daily routine.
- The variety of stakeholders is a special characteristic of the borders; custom authorities, armed forces, border guards and coast guard officers, airport or port staff and companies, are only indicative categories of the stakeholders involved. The complexity increases even further by the range of the various threat actors, mainly criminals and criminal groups, who constantly try to exploit different border vulnerabilities to achieve their target such as illegal drug and weapons trafficking. Synergies of the different threat actors is a common pattern, e.g., smugglers offering their services to irregular migrants. Threats vary per border unit or even per season e.g., criminals prefer seasons with high traffic to decrease the possibility of detection. Threats are not only caused intentionally but different events can have a severe impact on the daily tasks; a false database's alert can allow a terrorist to enter undetected or create a fuss to an innocent person. Or an extraordinary number of travelers, possibly caused after a strike or during the touristic seasons, can reduce the control's efficiency.

- Border experts are required to respond to a range of different tasks within a challenging environment, from cooperating with the multiple stakeholders to efficiently handling different databases and tools. In parallel, they must preserve different societal assets; national security and public order, travelers' fundamental rights or even the health and safety, for example performing search and rescue operations for missing persons in the sea.

The interview findings, alongside the trends identified in section 4.2, provided a basis to guide the risk analysis investigations as presented in section 5.

5. Risk analysis investigations

Investigations were carried out using a risk analysis approach to solicit conclusions on the cyber-threat landscape affecting border control infrastructure, and to produce exemplary inputs to risk assessment methodologies that can be applied to assess the risks in border control infrastructures. Investigations were facilitated by semi-structured interviews with border control experts.

5.1 Organizational context & assets identification

It is essential to have a clear insight into border-related definitions, processes, and functions. In fact, even the perception of what a 'border' is has changed over recent years [41]. Definitions relevant to the current research include the following:

- **Border Crossing Points (BCPs)** are the official control points where 'border checks' are carried out to ensure the entry or exit of persons, their transport, or their effects are properly authorized. Key functions include the verification of documents and permissions for crossing the border, checks on vehicles and property, and the detection and prevention of potential threats [42].
- **Border Surveillance,** carried out by border guards, is the surveillance of the areas between BCPs to prevent the entry or exit of those seeking to circumvent border checks. In this context the EU defines three objectives [43]: a) combatting cross-border crime, b) preventing undetected entry of irregular migrants, and c) reducing migrant fatalities at sea.
- **Border Control** includes both border checks and border surveillance activities (Figure 2). For the EU, *"The aim of border control is to help combat illegal immigration and trafficking in human beings and to prevent any threat to the Member States' internal security, public policy, public health and international relations*" [9] .

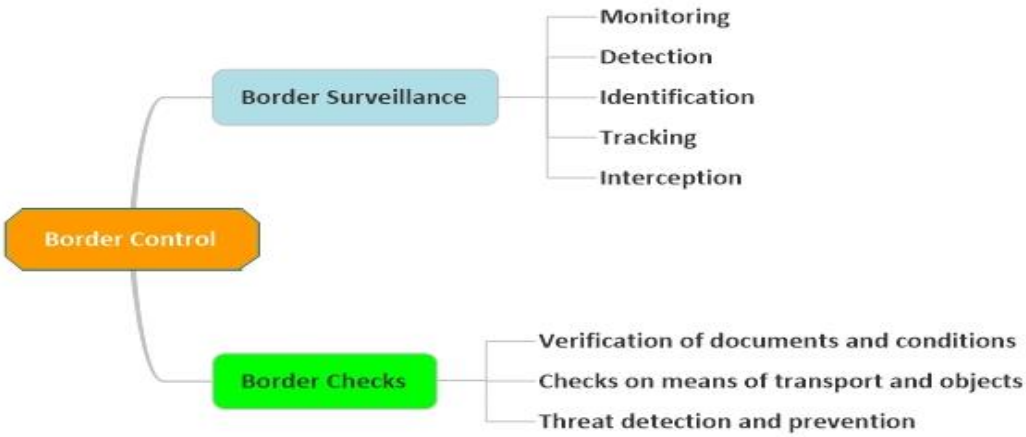

Figure 2: Key border control functions

Control of the cross-border flow of persons and goods, along with surveillance and protection duties, are the core elements of external border management. The visualization of border control functions at Figure 3 aims to enhance the readers' understanding of border checks and surveillance infrastructure. "Big-data" refers to the abundance of data in all border functions, from biometrics used for the checks (fingerprints, databases, photos etc) to other kinds of data in surveillance, such as communications, videos and sensors.

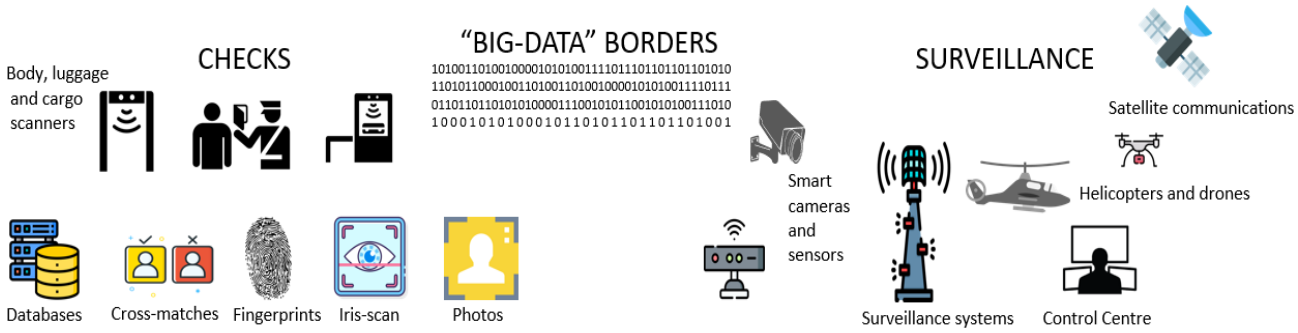

Figure 3: Representative big data components of the border control

Experts stressed out the magnitude of impact that can be caused from any form of assault against borders, especially legal costs. It is imperative to develop a solid understanding of all assets that take part in a border control infrastructure to be able to protect them from compromisation. As mentioned before, the complexity of border control infrastructures can hinder the development of an effective security governance. For example, border control systems are based on a range of databases which are operated by different services to serve a range of purposes, such as verifying that a person is not a threat to the internal security, public health, or international relations [44], etc. If this aspect is not identified during risk assessments, then appropriate security controls might not be selected to protect relevant operations. To disject the complexity of border control infrastructures, the next section provides a

thorough classification of assets that will be utilized to specify in detail the threat landscape relevant to borders control infrastructures.

5.2 Border control assets

A novel contribution of this work is the description of an asset's taxonomy relative to the border control infrastructure. A broad definition of the term 'asset' is defined [45] as "*a useful or valuable quality, skill, or person*" or "*something having value…that is owned by a person, business, or organization*". Minor assets or emerging technology related assets were skipped, as they fell beyond the scope of the current research.

This section presents the asset's classification, grouping all relevant assets under two main categories: a) organizational assets, and b) societal assets, providing a complete overview of the border control infrastructure. Figure 4 presents a high-level classification of the assets, whereas Figure 5 and Figure6 present a more detailed categorization.

Figure 4: High-level representation of border control infrastructure key assets

5.2.1 Societal Assets

'Societal assets', in relation to border control, are the assets which have an impact on society. Figure 5 presents the three categories of societal assets:

- Fundamental rights: data protection, human dignity, confidentiality and privacy, and non-discrimination principles are all vital to maintain. Privacy and the integrity of personal data are prevailing border control priorities, which are protected by various EU Regulations and international conventions, e.g., the General Data Protection Regulation (GDPR) and the UN Charter of Fundamental Rights. The Schengen Handbook states that "*rights … must be guaranteed to any person seeking to cross borders*". Discriminatory profiling is another aspect related to personal data processing [46].

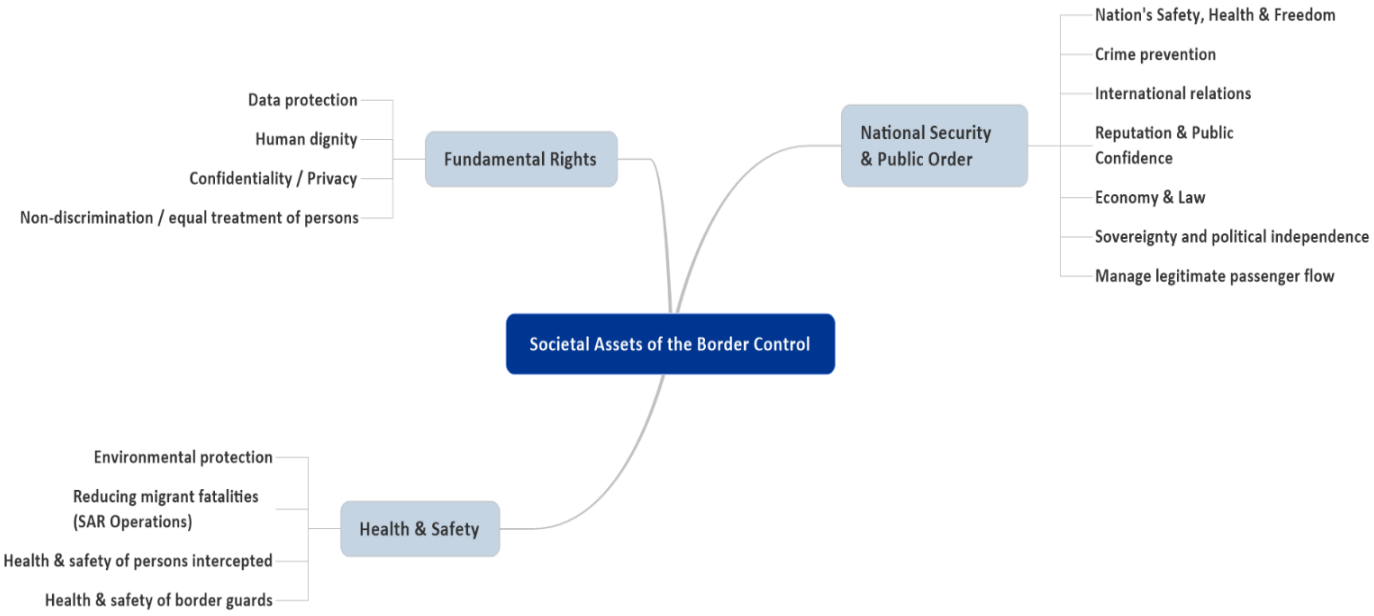

Figure 5: Societal assets taxonomy of the border control infrastructure

- The health and safety of persons apprehended, and of border guards. Search and Rescue (SAR) operations fall under this category. Search and Rescue for people in distress at sea is a legal obligation, as defined by various international conventions, e.g., Art. 98 of the UN Convention on the Law of the Sea. Additionally, the health and safety of both Border Guards and apprehended persons can be put at risk during border operations [47]. Interviewed experts also added environmental protection, e.g., vessels used for illegal activities that are abandoned and sunk causing pollution hazards.
- National security & public order: National safety, health and freedom should be highlighted as the key values for successful border control. The world-wide closure of borders following the outbreak

of COVID-19 was a response to the need to preserve the health of individual populations, but closed borders can also directly affect the (legitimate) freedom of movement of citizens. National safety derives from the need to have well-protected borders to avoid incoming threats, but several interviewed experts serving at BCPs also highlighted the necessity to facilitate and safeguard the lawful movement of people and goods. Crime prevention is another key border control aspect. Sovereignty and political independence are logical and traditional border characteristics. Similarly, international relations are another dimension of the borders, since events that take place there might affect the relationship between two (or more) countries. Reputation and public confidence are important aspects of any governmental (or even private body) functionality and societies trust that governments will carry out effective border checks. The 9/11 tragedy in the USA and 2015 migration crisis in Europe are indicative examples of the serious economic and legal repercussions that follow border-related events.

5.2.2 Organizational Assets

The following important parameters were considered to identify organizational assets: a) the Schengen Catalogue [48], b) the Technical Study on Smart Borders [44], c) interviews with experts, and d) extensive web research and literature review. Defining the organizational assets is the basis for exploring further the threat landscape.

Organizational assets are categorized under seven groups as indicated in Figure 6:

- Border check processes and equipment related to verification of documents and checks on means of transport and objects
- Infrastructure, related to technical infrastructures and facilities e.g., forensic laboratory
- Networking and communication equipment to support the provided services
- Staff and stakeholders such as passengers and third-party service providers
- Databases and lists to support border control functions
- Information such as sensitive documents
- Border surveillance processes and equipment

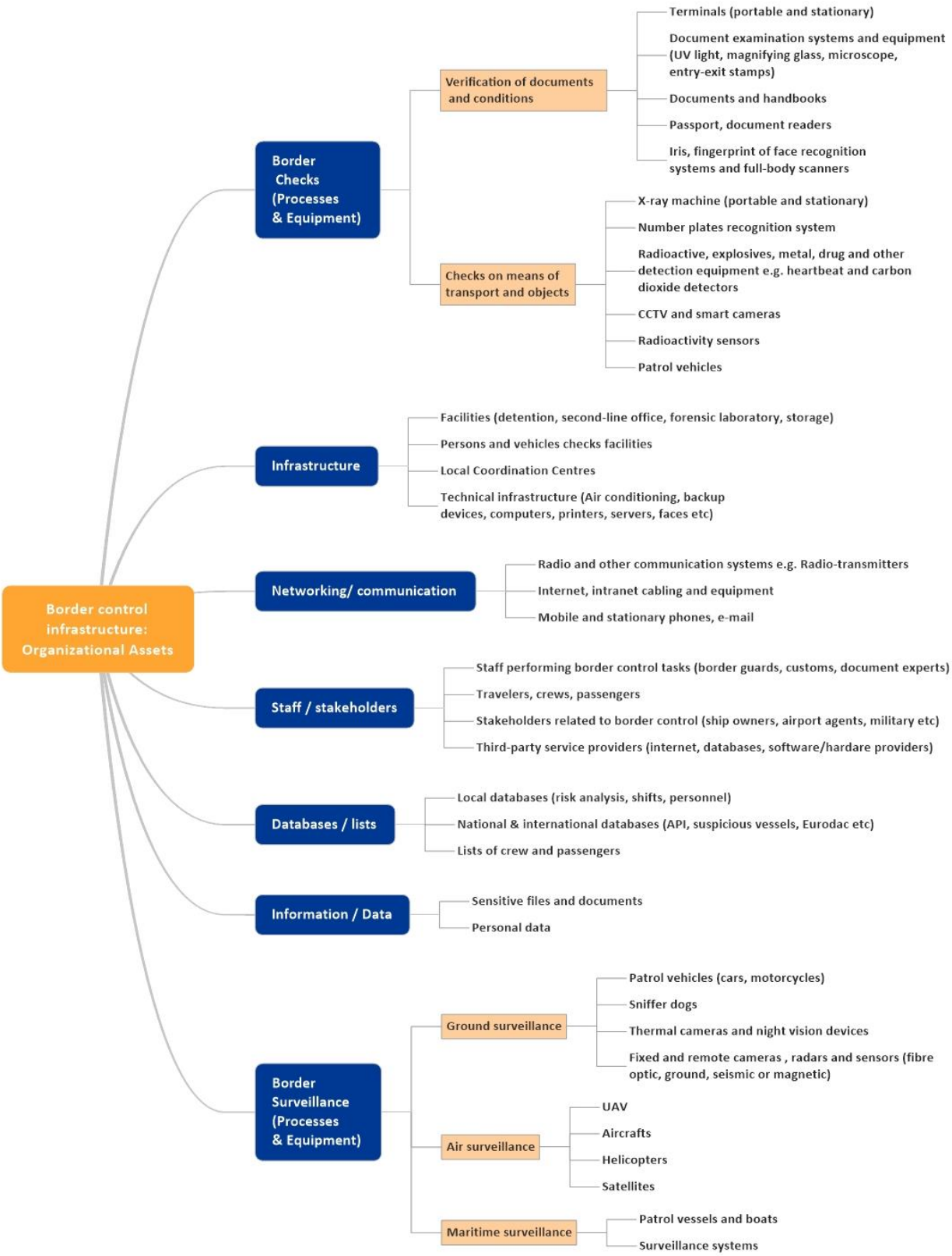

Figure 6: Organizational assets taxonomy of the border control infrastructure

5.3 Threat assessment

Threats to critical infrastructures and operations are evolving and growing. A practical border-based threat classification, applicable to all border assets, has been developed based on the findings from interviews, analysis of previous attacks, and extensive web research and literature review such as the ENISA Threat Landscape Report [49], ENISA Threat Taxonomy [27], and Frontex Integrated Risk Analysis Model [50].

5.3.1 Threat actors & motives

Identifying the threat actors, their objectives and targets, gives a valuable insight into identifying potential threat events that organisations should be focusing on [29]. In considering several criteria, for instance motivation, intent and capability, the threat actors can be classified into seven categories (Figure 7). In particular:

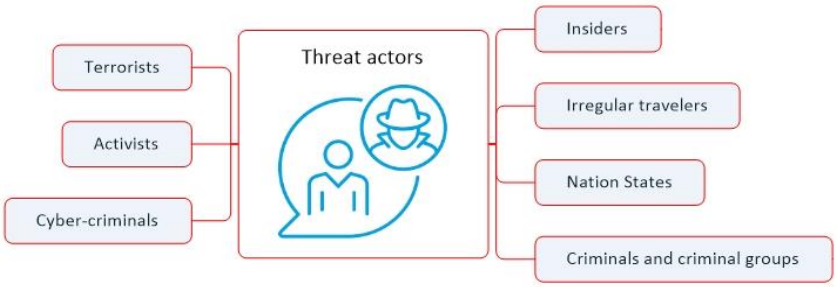

Figure 7: Categorizing the threat actors for the border control infrastructure

- **Insiders**: Border agencies are vulnerable to corruption [51]. Of course, insider threats can be also be due to human error.
- **Irregular travelers:** 'Traveler' is a term used to describe a person "moving … from one place to another" [52]. In this context it refers to those persons who try to enter or exit borders without fulfilling (or avoiding) legal requirements. The strong connection between travelers and criminals is highlighted, e.g., irregular migrants mostly use smuggling services [53].
- **Nation States:** Nation States have adequate resources to mount sophisticated attacks, using advanced technology and methodologies.
- **Criminals and criminal groups:** Migrant smugglers and drug or weapon traffickers are typical cases of criminals who exploit various border vulnerabilities. Some even specialize exclusively in identifying ways to circumvent border controls.
- **Cyber-criminals:** This category comprises those malicious actors who use cyber techniques to compromise a border's control infrastructure, and who may also offer their services to criminal groups to facilitate their illegal cross-border activities.

- **Terrorists:** Terrorist groups may cross borders to illegally traffic small arms, weapons and explosives [54], and illegal border crossings may form part of a plan for a terrorist attack. Terrorist groups can also benefit from cyber-attacks, which are conducted anonymously, remotely and cost-effectively, compared to physical attacks [55].
- **Activists:** Borders are often at the center of political and social debates. The activities of such movements, groups or individuals can vary from peaceful protest to violent action.

Combining all the elements above, along with the findings in Section 4.2 and the expert interviews (input and validation), Table 4 presents the key features of the identified threat actors.

Table 4: Threat actors' profiles

Threat actors	Description	Motivation	Opportunity	Technique
Insiders	Staff assigned to border control tasks and misusing their authority	Profit, revenge, discontent, negligence	Access to classified information and physical access in secure areas	Data theft and manipulation, leaking information, corruption, violating the code of conduct and regulations
Irregular travellers	Persons who want to reach another country, not fulfilling legal requirements	Better financial and living conditions, negligence (when not aware of restrictions)	Limited resources and access to information, mostly relying on criminals.	Document fraud, hiding in means, trespassing illegally the border line, deception / impersonation, bribing
Nation States	Nations attacking Nations, mostly in the frame of covert espionage operations	Geopolitical interests: espionage, financial and technological advantage, damage to other nation	Advanced level of resources in place to perform their activities.	Mass digital surveillance campaigns with advanced tools & techniques e.g., customized malware
Criminals and criminal groups	Migrant and drug smugglers and all individuals performing illegal activities. If organized, they form a criminal group.	Profit	Possibility to move in different geographical areas and perform the attack with the least risk. Different modi operandi, depending on the target.	Use of tools and techniques to skip border checks for themselves or other persons (document fraud, concealments in vehicles, etc) Physical attacks to staff or infrastructure, Bribing
Cyber-criminals	Criminals using cyber techniques to attack the borders, sometimes offering the cyber-crime as a service	Profit, power	No need for physical access to the area, identify a vulnerability and compromise assets. If border control infrastructure is not monitored well, there is low chance of detection	Malware, DoS, Penetration attacks, manipulation of hardware / software / data, social engineering
Terrorists	Non state actors and extremist groups who seek to intimidate or coerce or harm an audience, or force a political change	Ideological: Gain support for and deter opposition to a cause	Easy to hide among migrants	Destroy and disrupt border control functions, acting as irregular traveller to avoid border checks (terrorist action not performed against the borders)
Activists	Mostly groups, seeking to increase awareness against border controls	Ideological	Public feelings and increased media attention can be an opportunity for carrying out an attack.	Vandalism, Assaults, Triggering other stakeholders to cause incidents

Table 5 lists examples of potential synergies that might be established between the threat actors to promote their malicious objectives against the border control infrastructure. It should be noted that even if no direct link has been identified between threat actors, it does not imply that such a link could not exist.

Table 5: Examples of synergies between threat actors

Threat actors	Irregular travellers	Nation state	Criminals/ groups	Cyber criminals	Terrorists	Activists
Insiders	Insiders might be bribed by irregular travellers to avoid checks	The 'negligence' of insiders might be exploited by hostile nations to attack borders, as part of their surveillance campaigns	Corrupted insiders may assist smugglers to avoid border checks on illegal goods or persons	Cyber-criminals could benefit from the negligence or non-compliance with security practices of insiders	A terrorist could benefit from ineffective or slack border checks.	No direct link and synergies. All border staff, (including insiders), could be targeted by activists, e.g., assaulted
Irregular travellers		Cases exist of Nation States using migration to enforce their agenda, e.g., Libya planned to flood Europe with migrants [56].	Irregular travellers might cooperate with, or be coerced by criminals, e.g., assisting in the production of fake documents, or carrying drugs across borders	Criminals providing smuggling services to irregular travellers, may cooperate with cyber criminals (indirect synergy)	A terrorist might avoid border checks, posing as an irregular traveller	Groups of irregular migrants could be incited by activists to unlawful activity e.g., damage to the border control area
Nation States			Nichols (2018) stated that human smugglers in Libya had links to security services	Nation States use cyber-criminals for buying tools or access to infrastructures.	A State sponsored terrorist might seek to avoid border controls	Activist refugee support groups could be infiltrated by hostile State operators.
Criminals / groups				Cyber-criminals offer their services to criminals (cybercrime as a service)	Terrorists could carry out criminal activity, e.g., smuggling, to fund their objectives	Criminals can use activists' info for the border situation and activism as a way to camouflage any illegal activities
Cyber criminals					Cyber-criminals offer their services to terrorists (cybercrime as a service)	No direct link identified
Terrorists						No direct link identified

5.3.2 Threat categories

A threat classification was elaborated, where all threats are grouped under five broader categories (Figure 8):

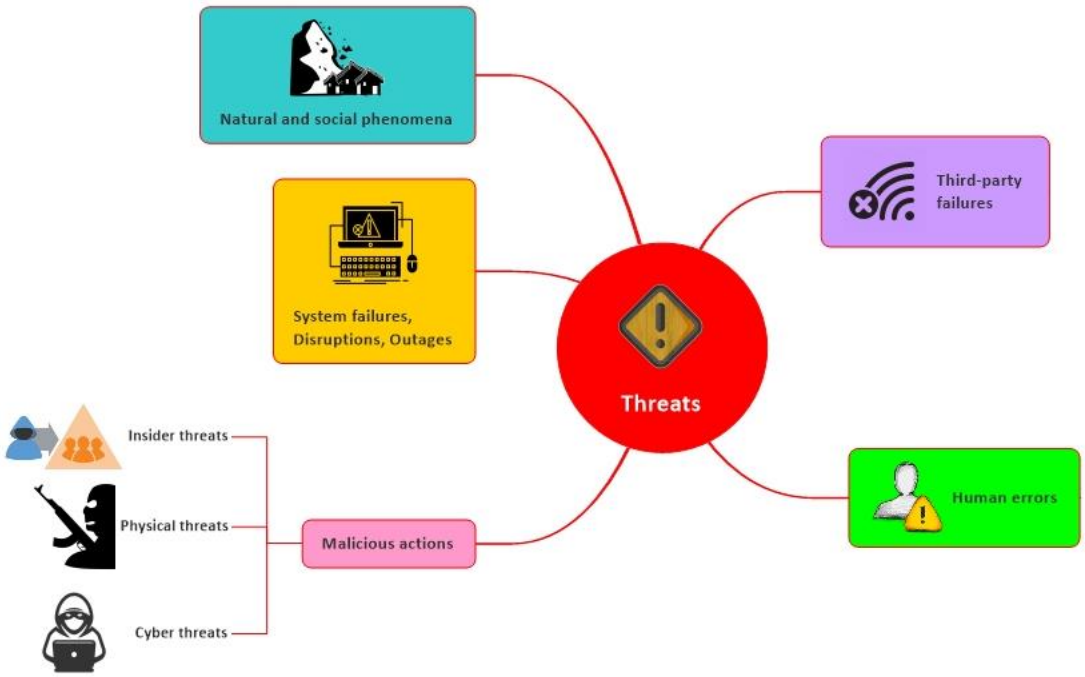

Figure 8: High-level threat categories

- **Natural and social phenomena:** Natural disasters or environmental phenomena, or human activity, that cause serious disruption to the normal functioning of a society. A special sub-category applicable to the borders is the 'push and pull' factors applicable to migration, which are external motivators of a strategic nature, e.g., poverty or war.
- **Third-party failures:** There is a growing number of interdependencies between border control management and third parties, such as vendors and service providers, which increase the potential threat.
- **System disruption / failure and outages:** Hardware and software failures and disruptions of the equipment (e.g., X-rays, cameras) would result in deficient border functions. Outages describe any lack of personnel or assets, e.g., lack of internet connection.
- **Human error:** Includes the full range of unintentional human activity which could harm assets or border control processes.
- **Malicious actions:** These are threats caused intentionally by humans. Three sub-categories are identified, based on the stakeholders involved and the means to perform the attack. In particular:

a) Insider threats: employees with malicious motivation, e.g., corrupted border guards.

b) Physical threats: attacks that take place using traditional 'physical' methods and tools, without reliance on technology, such as vandalism and theft.

c) Cyber-threats: strongly correlated with all other threats. Several subgroups are prevalent:

- **Malware:** Several types of malicious software exist such as trojans, worms, spyware, botnets, and rootkits. Malware was used in 66% of the cyber-attacks in 2019 [57] and is therefore considered a significant threat to the integrity of border controls.
- **Denial of Service attacks:** In DoS attacks, attackers block access from legitimate users, causing delays and disruption. In the border control context, they could be carried out by cybercriminals to disrupt functions (e.g., proper checks and surveillance), possibly requested as a service by criminals.
- **Manipulation of hardware, software, and data:** This type of attack encompasses all infections to systems, having gained access. Considering the complexity of border systems and the variety of existing databases, it is highly likely that such attacks could target the borders.
- **Penetration attacks:** These attacks involve breaking into systems and networks by exploiting known vulnerabilities, e.g., breaking passwords or 'man-in-the-middle attacks'. Borders can be targeted, considering the huge reliance on fixed and wireless networks, e.g., remote cameras or drones.
- **Advanced Persisted Threats (APTs)** are sophisticated and focused network attacks, aiming at high-value information in companies and governments, usually in a long-term campaign, and they are potentially funded by governments [58]. As previously noted, Nation States can be serious threat actors when targeting borders.
- **Social engineering** is the technique of deceiving a person to act against their own interest, or that of their organization. In 2019, 54% of attacks against governments included social engineering, usually combined with malware [57]. Border guards could be deceived, so that malicious actors can gain access to border systems or databases.

Figure 9 illustrates a detailed classification of threats relevant to border control infrastructures.

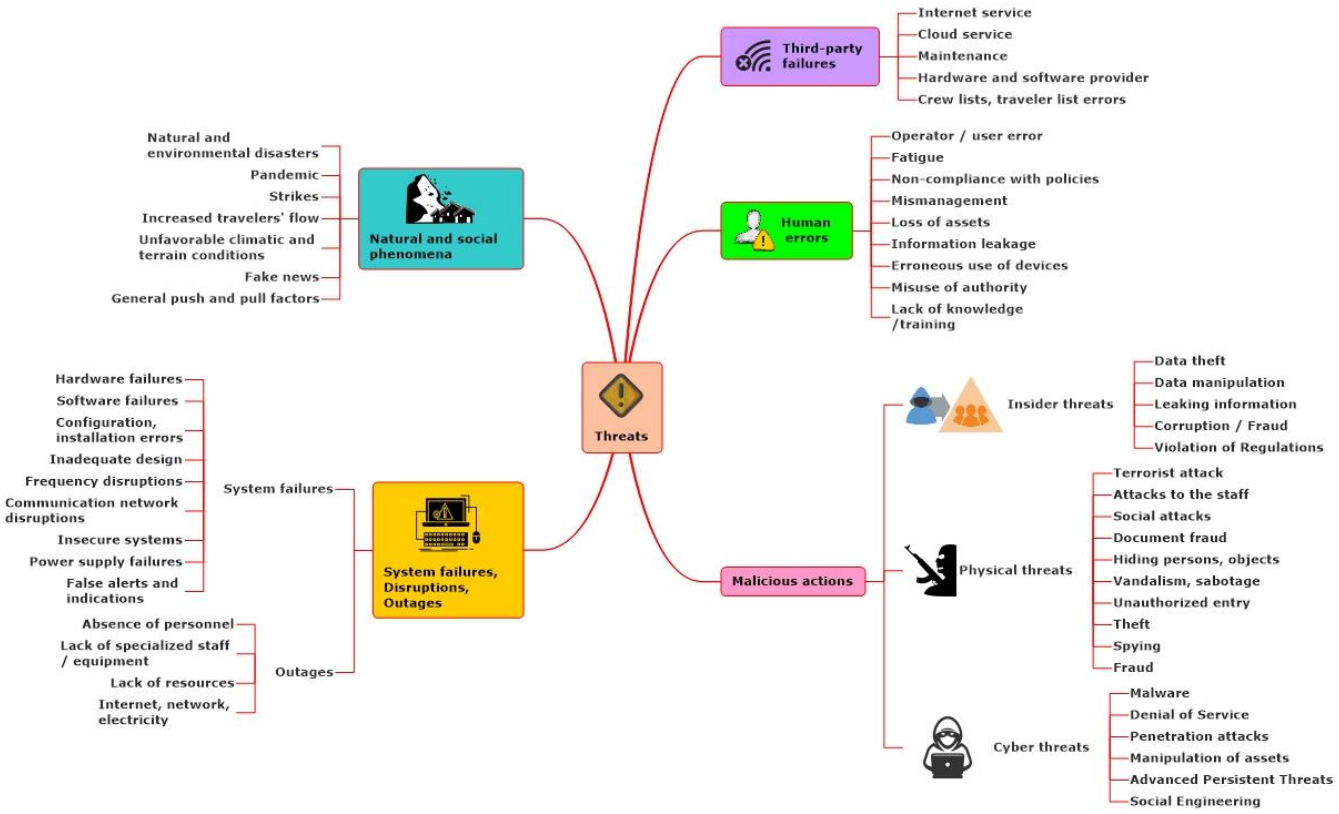

Figure 9: Detailed threat taxonomy

5.4 Vulnerability assessment: Factors and areas of vulnerabilities

Expert input, and the risk-related investigations, led to identifying the main areas of vulnerability, with a focus on those related to cyber-threats relevant to border control infrastructures. These areas can be considered when carrying out risk assessments in specific border control environments. These factors and areas of vulnerability are briefly described below.

- **Increased reliance on technology:** While technology offers solutions by enhancing functionality and capabilities, and reducing human error, it introduces a new threat environment at the same time.
- **Wireless communications:** UAV camera feeds, satellite-based communications, and other systems using wireless connections, are vulnerable to hacking - threatening the effectiveness of surveillance [47].
- **General hardware and software vulnerabilities:** PCs, routers, operating systems, laptops etc. are all assets vulnerable to cyber-attack.
- **Increased number of assets** at the borders increases the potential vulnerabilities that need to be managed in an effective and secure manner.
- **Automation:** Border control relies on databases and algorithms, e.g., smart cameras. Unreliable algorithms, possibly due to design flaws, can impact border control operations. Large information

systems, such as the Schengen Information System, might produce false positives (hits) against innocent persons, while some reports underline the high error rate of body scanners [59].

- **Reliance on third-party service providers:** Sensitive data, like biometrics, are often outsourced to private companies, with limited awareness or audit for data security [60].
- **Restricted databases** containing personal data, documents or files are a primary target for malicious actors, but at the same time the exponential rise in legitimate access to real-time data increases security and maintenance requirements, and costs.
- **Increased connectivity and complexity:** Systems and processes are steadily becoming more sophisticated and complicated, and the vulnerabilities relevant to such a complex environment can be exploited by attackers. Network connectivity is increased to connect different systems together, e.g., databases are accessed via internet and intranet, creating additional access points for malicious actors.
- **Interdependencies:** Failure of an asset could produce a knock-on effect to other assets or functions. For example, a UAV and the vessel controlling it both rely on GPS for navigation. The smooth interface of diverse systems needs to be maintained continuously.
- **Heterogeneity:** A typical example might be a border surveillance system made up of components of a different nature, origin, and manufacture. The more complex a system, the more vulnerable it can become and the less likely that faults can be identified.
- **Insufficient procedures may not identify insider malicious activity:** An insider is fully aware of the organization's capabilities and behaves in a way that does not arouse any suspicion [61].
- **Limited cyber security training:** Law enforcement has limited familiarity with new IT applications [62], which increases the potential for malicious cyber activity.
- **Personal use of social media** and smart devices in the work environment increases vulnerability, e.g., if a border guard accesses the work Wi-Fi with his/her personal mobile phone. Additionally, APT attacks can become more successful when using reconnaissance of social media information [63].
- **Increased traveler flows**: Where there is a sudden increase in traveler flows (e.g., the number of flights from an airport following widespread cancellations), the threat level is increased, including cyber-threats.

5.5 Impact assessment

This section provides useful input when measuring impact during the risk assessment process. Table 6 lists representative examples of potential impacts to both organizational and societal border-control assets identified in section 5.

Table 6: Examples of impact

	Impact on	Impact description
Functions	Operations	- Inability to perform operations (surveillance, checks and maintaining public order) or to perform effectively if any organizational asset is damaged or not operating properly, e.g., CCTV or terminals. - Failure to detect a threat, e.g., a terrorist due to a data false negative.
Organizational Assets	Infrastructure	- Damage to physical facilities, e.g., fire in a server room. - Damage to technical infrastructure, e.g., printers or high-tech fence.
	Networking / communications	- Damage or loss of communication networks, e.g., between border guards or communication with an aerial surveillance asset.
	Databases, lists	- Databases might not be accessible during DoS attacks. - Biometrics might be leaked to malicious parties. - Data could be altered or manipulated.
	Staff / stakeholders	- Safety of staff on board a vessel could be harmed if systems were damaged. - Image and reputation of staff could be harmed, e.g., by neglecting security practices.
	Equipment, assets, and tools	- Damage or loss of assets, e.g., UAV attack. - Inability to use an asset, e.g., a remote terminal.
Societal assets	Health and safety	- Pollution caused by a destroyed vessel or aerial asset. - Smugglers may use dangerous modi operandi to avoid detection, e.g., hiding persons in refrigerated lorries. - Border closures are indicative of how breaching the integrity of a border could impact a nation's health, e.g., an infected person crossing undetected.
	National Security and Public Order	- A terrorist or a smuggler might evade border checks, entering undetected. - Financial and legal costs incurred by an attack, e.g., to replace a destroyed UAV. - Any attack on the border area can affect the sovereignty of a Nation, and any form of espionage can directly impact its political independence. - Harm to international relations since other nations could be involved in an attack (directly or indirectly) on the border area.
	Fundamental Rights	- Technology can mistakenly identify an innocent person as a criminal. - Privacy and confidentiality can be compromised if biometric data is leaked to malicious actors.

5.6 Risk calculation

The calculation of risk uses the formula *Risk = Likelihood x Impact*. The likelihood considers whether the identified threat will exploit a vulnerability which would result in a negative impact [29].

Figure 10 presents ways to use the current research in further risk assessment methodologies at strategic or operational levels, including basic steps such as asset identification and threat or vulnerability assessment.

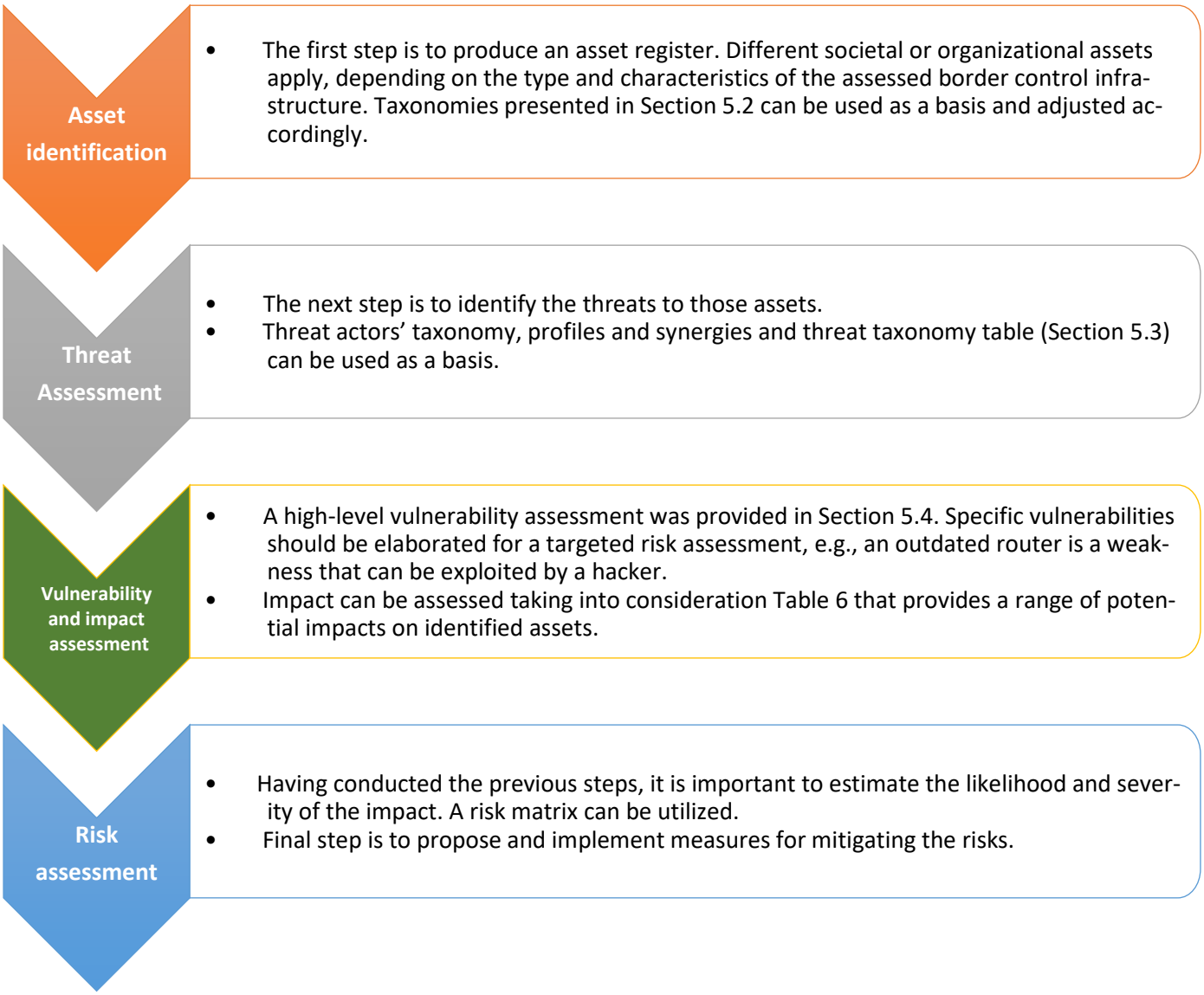

Figure 10: Proposed ways to use the research as input to risk assessment methodologies

Based on the proposed way to use the research for a risk assessment methodology, a simplified example is presented below:

- Asset identification: A drone is used for border surveillance.
- Threats assessment: Threat actors can be a) insiders, using the drone without a specialized training or b) criminals who are interested in damaging the UAV or performing a penetration attack with an aim to avoid detection of illegal drug trafficking, which is the main criminal activity in the area.

- Vulnerability and impact assessment: The drone's firmware is not updated regularly, while the staff never had a specialized training. The drone is stored in a room without 24/7 monitoring.
- The impact could be the damage or theft of the drone, causing the inability to perform air surveillance and detect threats with a risk for the national order (undetected drug trafficking).
- Likelihood and severity of the impact is high, since the drone is the main mean for border surveillance and the border area is constantly targeted by drug trafficking criminal groups, who try constantly to exploit any vulnerability.
- Mitigation measures are a) regular update of the firmware, b) specialized and periodical training for the staff, c) drone's storage in a secure cupboard at the duty officer's room, d) developed relevant security policies to guide adoption of mitigation measures such as firmware updates and physical protection of the asset.

6. Validation and key discussions

An essential part of this research was the validation of the findings by the experts. As explained in section 2 Methodology, each interview consisted of a brief presentation of the findings delivered to each expert (identified assets, vulnerabilities, impact), followed by a bespoke discussion on the accuracy of the findings and a separate discussion elaborating on future directions and scenarios. The duration of each interview was two hours and a tailor-made questionnaire, based on their area of expertise and the initial input, with open ended questions was used to facilitate the oral discussion. For example, questions posed to experts included: "can you describe if the threats presented can occur in your unit?" or "if the UAV used for surveillance purposes is intercepted by malicious actor, what would be the possible damage caused?"

6.1 Key discussions

Once the validation process was concluded, the findings were unanimously accepted, with only minor comments or adjustments required. The input of policy documents, legislation, literature review and case studies further enhanced the analysis, leading to concrete outcomes with no significant knowledge gaps.

Almost all experts acknowledged the value of the research. The maritime BCP expert stated that *"no relevant analysis exists, and the work could be used further for redrafting the risk analysis of the service"*. The border surveillance expert added that *"it is the first time I have seen all the different threats in one place, some of them possible, and I am not even aware of these being included in training or handbooks"* and that *"the findings could be useful at all levels: strategic, tactical and operational"*. All experts agreed that the taxonomies could be easily elaborated and tailored to the needs of individuals border services, as part of the local risk analysis. Lastly, the constantly evolving character and the variety of threats in place was highlighted, reflecting the complexity of the border control infrastructures.

6.2 Future directions and possible scenarios

The key finding of the current research is that cyber-threats to border control infrastructures have not been properly assessed and addressed by Nation States, despite the critical nature of the threat. It is a paradox that countries are investing more and more on securing their borders, but the border control infrastructure is not included in national inventories of "critical infrastructures", although conditions are fully met. There are various possible explanations:

a) Not a good understanding of the complexity level of "the border" [64], due to its multidimensional nature encompassing national sovereignty, fundamental rights and push-pull factors. This complexity is

further compounded by the variety of threats, from traditional actors to Nation States, and the multiple notions of security, e.g., national security, physical security, and personal safety.

b) Border control security is a relatively new science, emerging from the last few decades as a result of increased global mobility and recent migratory events [59] [65].

c) The restricted nature of border controls, based on reputational and national security concerns, does not lend itself to straightforward information exchange.

Actions need to be taken to establish an appropriate security governance for border control infrastructures. The following points summarize important aspects for further consideration by policy makers and border practitioners:

- It is important to develop and implement a comprehensive cyber security strategy specific to critical border control infrastructures. This would include detailed identification of assets, including their processes and functions, threat assessments, vulnerability and impact assessments, and remedial actions to rectify weaknesses and breaches. Wider cyber-threat assessments should form part of this process.
- As a first step, focused cyber security risk assessments and vulnerability assessments could be conducted in respect of critical or priority Border Control or Border Check Units.
- Effective cooperation between private and public sectors is essential. Evaluations of current cooperation mechanisms should be conducted. Security by design would help minimize security vulnerabilities.
- There is a need to integrate fundamental rights considerations into all policies and processes. This would encompass technical specifications to avoid false alerts, algorithms to preserve necessity and proportionality principles, creating complaint mechanisms and choosing less intrusive options, where possible.
- Further action in respect of data and privacy protection should be undertaken. The triad of confidentiality, integrity and availability of information should be a core element of the cyber-defense process. Collection and use of personal information should be both proportionate and appropriate. Data backup must ensure that data will be restored if necessary. A robust data access policy is essential, with multi-factor authentication systems the norm.
- Enhanced information exchange on cyber-related incidents specific to the border control infrastructure. Multiple stakeholders could and should be involved, for instance border guards who carry out border checks and surveillance tasks, airline and maritime companies, or third parties such as private sector researchers involved in cyber security.

- Awareness building and bespoke training are required. Security awareness would allow border guards to recognize cyber security risks and implement best practices in their daily routine.
- Invest in and enhance appropriate technology to protect border infrastructures against cyber-attack. This could include secure network architectures, data encryption, access controls, firewalls, intrusion detection systems, etc.
- Incidents cannot be entirely avoided, and catastrophes should always be anticipated. Mapping possible scenarios requires preparatory work. Business continuity plans, including a disaster recovery plan, are the proactive and reactive sides to disaster recovery [61].
- Develop and ensure the implementation of a security policy, including best practices and operational guidelines for staff and users of relevant equipment.
- Enhanced physical security. Based on their security classification, assets should be adequately protected with access limited to authorized personnel and kept in secured storage, with servers set aside from workspaces.

Moreover, three key attack scenarios have been identified, based on information derived from the experts' opinions and the findings of this research, which could be further developed by border professionals, enhancing the protection of border control infrastructures:

- **Drone interception attack:** A UAV is a significant asset when compared to border patrols or stationery surveillance equipment, with a greater chance of locating illegal border attempts [66]. Malicious persons could compromise drones for several reasons, for instance destroying the equipment (sabotage), stealing sensitive data such as log files, movement records or even real-time pictures, or taking control of the asset. For criminal enterprises, compromising a UAV would mostly be a way to avoid detection.
- **Network attack to camera surveillance system:** Camera surveillance systems are an essential part of border control infrastructure aiming mainly at the detection of unauthorised persons in designated areas. In border surveillance, cameras support the identification, monitoring and tracking of suspicious persons. Hacking into a CCTV system is comparatively easy: firewall misconfigurations, insecure protocols, and weak passwords form part of the threat.
- **Spear fishing attack scenario:** Online presence of people makes it easy for cyber criminals to profile a border employee. The target, a border guard, has published his service e-mail account in social media. The malicious attacker creates a spoof mail which redirects the border guard to a page for renewing the password, where he / she provides all their credentials.

7. Conclusions

Borders are increasingly exposed to cyber-threats as 'traditional' criminals, already operating in border areas, look to use cyberspace in support of their activities. At the same time, enhanced border-related data collection activity and reliance on technology is increasing the potential threat. Threat actors are not limited to individuals or criminal groups; Nation States are another threat actor that uses advanced and sophisticated tools to attack the borders, typically for espionage purposes. Third parties, such as private sector vendors, play a significant role since they could either be targets of a cyber-attack, or their products could lack adequate security features. System and software failures might lead to false alerts and messages, disrupting functions and processes or even breaching the privacy or fundamental rights of citizens. Physical and cyber threats are correlated, for example a physical attack to an asset could form part of a cyber-attack event.

Governments remain largely unprepared for the potential dangers from the cyber world and there is an urgent need to implement robust cyber security policies and, where necessary, take urgent remedial action to rectify weaknesses. Border control does not feature within national critical infrastructure priorities, presumably due to its multi-dimensional nature and complexity. Staff training, focused risk assessments, enhanced information exchange and strengthened collaboration with the private sector, are essential actions requiring implementation.

This research has specified a comprehensive border-related cyber-threat landscape which can be used as a reference and basis in future research and in border-specific risk and vulnerability assessments. Future work could further elaborate on specific border types, explore the synergies between the different threat actors or expand the threat landscape to develop border-control attack scenarios, especially those related to the emerging technologies e.g., artificial intelligence, which can be utilized to build incident handling capabilities.

Acknowledgements

Authors would like to thank the experts who provided valuable input to the research and validated the results.

References

[1] Al Jazeera, “Coronovirus: Travel Restrictions, Border Shutdowns by Country,” 2020. [Online]. Available: https://www.aljazeera.com/news/2020/03/coronavirus-travel-restrictions-border-shutdowns-country-200318091505922.html. [Accessed 05 04 2021].

[2] S. Camarota, "The Open Door: How Militant Islamic Terrorists Entered and Remained in the United States, 1993-2001.," Center for Immigration Studies, Washington, 2002.

[3] D. Broeders and J. Hampshire, “Dreaming of Seamless Borders: ICTs and the Pre-Emptive Governance of Mobility in Europe,” *Journal of Ethnic and Migration Studies,* vol. 39, pp. 1201-1218, 2013.

[4] The Guardian, "Paris attacks: European leaders link terror threats to immigration," 2015. [Online]. Available: https://www.theguardian.com/world/2015/nov/14/paris-attacks-european-leaders-link-terror-threats-to-immigration. [Accessed 04 05 2021].

[5] C. Baker-Beall, "The threat of the ‘returning foreign fighter’: The securitization of EU migration and border control policy," *Security Dialogue,* vol. 50, no. 5, pp. 437- 453, 2019.

[6] European Commission, “Communication From The Commission: A European Agenda On Migration,” 2015. [Online]. Available: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-migration/background-information/docs/communication_on_the_european_agenda_on_migration_en.pdf>. [Accessed 04 05 2021].

[7] S. Scheel, Autonomy of Migration? Appropriating Mobility Within Biometric Border Regimes, Routledge, 2019.

[8] European Commission, “Commission Presents Action Plan For Immediate Measures To Support Greece,” 2020. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_384. [Accessed 04 05 2021].

[9] European Parliament and Council, "Regulation (EU) 2016/399 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code)," 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0399. [Accessed 05 04 2021].

[10] K. F. Olwig, K. Grünenberg, P. Møhl and A. Simonsen, The Biometric Border World: Technology, Bodies and Identities on the Move, Routledge, 2019.

[11] R. Al-dhubhani, W. Al Shehri, R. Mehmood, I. Katib, A. Algarni and S. Altowaijri, “Smarter Border Security: A Technology Perspective.,” Saudi Arabia, 2017.

[12] European Commission, "Overview Of Natural And Man-Made Disaster Risks The European Union May Face," 2017. [Online]. Available: https://ec.europa.eu/echo/sites/echosite/files/swd_2017_176_overview_of_risks_2.pdf. [Accessed 08 03 2021].

[13] Department of Homeland Security, "National Infrastructure Protection Plan," 2013. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf. [Accessed 08 03 2021].

[14] US Homeland Security, "National Infrastructure Protection Plan (NIPP) 2013: Partnering for critical infrastructure security and resilience," 2013. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf. [Accessed 04 05 2021].

[15] The Council of the European Union, "Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection," 2008. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114. [Accessed 04 05 2021].

[16] E. H. Alkhammash and T. M. Alkhaldi, "A Survey on The Use of Technologies in the Context of Border Safety and Security," *Border Security and Safety,* vol. 281, 10 2017.

[17] D. Wright, M. Friedewald, S. Gutwirth, M. Langheinrich, E. Mordini, R. Bellanova, P. De Hert and D. Bigo, "Sorting out smart surveillance," *Computer Law & Security Review,* vol. 26, no. 4, pp. 343-354, 2010.

[18] S. Papastergiou, N. Polemi and A. Karantjias, "CYSM: an innovative physical/cyber security management system for ports.," *International Conference on Human Aspects of Information Security, Privacy, and Trust,* pp. 2019-230, 2015.

[19] O. Yvon, "Blue Border Security," Saudi Arabia, 2017.

[20] A. Chiappetta and G. Cuozzo, "Critical infrastructure protection: Beyond the hybrid port and airport firmware security cybersecurity applications on transport," 2017.

[21] J. Ahokas, T. Kiiski, J. Malmsten, L. M. Ojala and (2017)., "Cybersecurity in ports: a conceptual approach," *Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL),* vol. Vol. 23, pp. 343-359, 2017.

[22] B. Genge, I. Kiss and P. Haller, "A system dynamics approach for assessing the impact of cyber-attacks on critical infrastructures," *International Journal of Critical Infrastructure Protection,* vol. 10, pp. 3-17, 2015.

[23] M. E. Paté-Cornell, M. Kuypers, M. Smith and P. Keller, "Cyber risk management for critical infrastructure: a risk analysis model and three case studies," *Risk Analysis,* vol. 38, no. 2, pp. 226-241, 2018.

[24] A. Tantawy, S. Abdelwahed, A. Erradi, K. Shaban and 9. 1. (2020). ., "Model-based risk assessment for cyber physical systems security," *Computers & Security,* vol. 96, no. 101864, 2020.

[25] J. P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," *Microprocessors and Microsystems,* vol. 77, 2020.

[26] S. Horri, "The effect of Frontex's risk analysis on the European border," *European Politics and Society,* vol. 17, no. 2, pp. 242-258, 2016.

[27] ENISA, "Threat Taxonomy," 2016. [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view. [Accessed 04 05 2020].

[28] Center for Strategic & International Studies, “Significant Cyber Incidents Since 2006,” 2020. [Online]. Available: https://csis-website-prod.s3.amazonaws.com/s3fs-public/210326_Significant_Cyber_Events.pdf?ZKJIdGVXdQd2vXW.gFEcFQs2Ay7cDiqt. [Accessed 04 05 2021].

[29] R. S. Ross, “Guide for conducting risk assessments - Special Publication (NIST SP)-800-30 Rev 1,” 2012.

[30] Reuters, "UN shipping agency says cyber attack disables website," 01 10 2020. [Online]. Available: https://www.reuters.com/article/shipping-imo-cyberattack-idUSL8N2GS38E. [Accessed 03 08 2021].

[31] The New York Times, "Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks," 19 05 2020. [Online]. Available: https://www.nytimes.com/2020/05/19/world/middleeast/israel-iran-cyberattacks.html. [Accessed 03 08 2021].

[32] Reuters, "Chinese hackers suspected of stealing details of 9 million easyJet customers," 19 05 2020. [Online]. Available: https://www.reuters.com/article/us-easyjet-cyber-idUKKBN22V1JF. [Accessed 03 08 2021].

[33] J. Stubbs, “China Hacked Asian Telcos To Spy On Uighur Travelers,” 2019. [Online]. Available: https://www.reuters.com/article/us-china-cyber-uighurs/china-hacked-asian-telcos-to-spy-on-uighur-travelers-sources-idUSKCN1VQ1A5. [Accessed 04 05 2021].

[34] J. Taylor, “Major Breach Found In Biometrics System Used By Banks, UK Police And Defence Firms,” 2019. [Online]. Available: https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms. [Accessed 04 05 2021].

[35] United States Coast Guard, “Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels,” 2019. [Online]. Available: https://www.dco.uscg.mil/Portals/9/DCO. [Accessed 04 05 2021].

[36] J. Stone, “After ‘Significant’ Malware Attack, U.S. Coast Guard Issues Maritime Security Advisory,” 2020. [Online]. Available: https://www.cyberscoop.com/coast-guard-significant-malware-attack/. [Accessed 04 05 2021].

[37] S. Levin, “Malicious Cyber-Attack Exposes Travelers' Photos, Says US Customs Agency.,” 2019. [Online]. Available: https://www.theguardian.com/world/2019/jun/10/malicious-cyber-attack-exposes-travelers-photos-says-us-customs-agency. [Accessed 04 05 2021].

[38] M. Burgess, “A Dumb Security Flaw Let A Hacker Download US Drone Secrets,” 2018. [Online]. Available: https://www.wired.co.uk/article/router-hacking-drone-reaper-military-secrets. [Accessed 04 05 2021].

[39] K. Everington, “Chinese Military Reportedly Has Access To Taiwan's E-Gate System,” 2017. [Online]. Available: https://www.taiwannews.com.tw/en/news/3317792. [Accessed 04 05 2021].

[40] P. Tucker, “DHS: Drug Traffickers Are Spoofing Border Drones,” 2015. [Online]. Available: https://www.defenseone.com/technology/2015/12/DHS-Drug-Traffickers-Spoofing-Border-Drones/124613/. [Accessed 04 05 2021].

[41] C. L. Broennimann and G. G. Stigmer, “Integrated Border Management (IBM),” Saudi Arabia, 2017.

[42] European Commission, “Annex to the Commission Recommendation establishing a common "Practical Handbook for Border Guards",” 2019. [Online].

[43] European Parliament and Council of the European Union, *Regulation (EU) No 1052/2013 establishing the European Border Surveillance System (Eurosur),* 2013.

[44] PWC, “Technical Study On Smart Borders. European Commission,” 2014. [Online]. Available: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_technical_study_en.pdf. [Accessed 04 05 2021].

[45] Cambridge Dictionary, 2020. [Online]. Available: https://dictionary.cambridge.org/dictionary/english/asset.

[46] United Nations, “Counter-Terrorism Travel Programme Summary,” 2020. [Online]. Available: https://www.un.org/cttravel/content/summary. [Accessed 04 05 2021].

[47] Frontex, “Ethics of Border Security,” 2010. [Online]. Available: https://frontex.europa.eu/assets/Publications/Research/Ethics_of_Border_Security_Report.pdf. [Accessed 04 05 2021].

[48] European Council, "EU - Schengen catalogue," 2003. [Online]. Available: https://www.consilium.europa.eu/en/documents-publications/publications/eu-schengen-catalogue-volume-4/. [Accessed 04 05 2021].

[49] ENISA, “Threat Landscape Report 2018,” 2019. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018. [Accessed 04 05 2021].

[50] Frontex, “Common Integrated Risk Analysis Model Summary Booklet,” 2013. [Online]. Available: https://frontex.europa.eu/assets/CIRAM/en_CIRAM_brochure_2013.pdf. [Accessed 04 05 2021].

[51] European Commission, “Guidelines For Integrated Border Management In European Commission External Cooperation,” 2010. [Online]. Available: https://europa.eu/capacity4dev/file/21153/download?token=3lOSGDjf. [Accessed 04 05 2021].

[52] Merriam-webster dictionary, 2020. [Online]. Available: https://www.merriam-webster.com/dictionary/travel. [Accessed 04 05 2021].

[53] A. Essif, “Refugees forced to depend on human smugglers: study,” DW.com, 2016. [Online]. Available: https://www.dw.com/en/refugees-forced-to-depend-on-human-smugglers-study/a-36266888. [Accessed 04 05 2021].

[54] United Nations, "The Protection Of Critical Infrastructures Against Terrorist Attacks: Compendium Of Good Practices," 2018. [Online]. Available: https://www.un.org/sc/ctc/wp-content/uploads/2019/01/Compendium_of_Good_Practices_Compressed.pdf. [Accessed 04 05 2021].

[55] G. Gluschke, M. C. Hakki, M. Macori and R. Leszczyna, Cyber security policies and critical infrastructure protection, 2018.

[56] Sengupta K., “Gaddafi planned to flood Europe with migrants as final revenge,” 2020. [Online]. Available: https://www.independent.co.uk/news/world/africa/gaddafi-planned-to-flood-europe-with-migrants-as-final-revenge-2354322.html. [Accessed 04 05 2021].

[57] Positive Technologies, “Cybersecurity Threatscape 2019,” 2020. [Online]. Available: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2019/>. [Accessed 04 05 2021].

[58] P. Chen, L. Desmet and C. Huygens, “A study on advanced persistent threats,” Berlin, 2014.

[59] V. S. Kenk, J. Križaj, V. Štruc and S. Dobrišek, “Smart surveillance technologies in border control,” *European Journal of Law and Technology,* vol. 4, p. 2, 2013.

[60] G. G. Clavell, “Protect rights at automated borders,” *Nature News,* vol. 543, p. 34, 2017.

[61] D. Sutton, “Cyber Security: A Practitioner's Guide,” B. Learning and D. Limited, Eds., 2017.

[62] O.S.C.E., “Strengthening Border Security And Information Sharing In The OSCE Region: A Parliamentary Oversight Exercise,” 2019. [Online]. Available: https://www.oscepa.org/documents/ad-hoc-committees-and-working-groups/ad-hoc-committee-on-countering-terrorism/3905-strengthening-border-security-and-information-sharing-in-the-osce-region/file>. [Accessed 04 05 2021].

[63] T. A. Johnson, Ed., Cybersecurity: Protecting critical infrastructures from cyber-attack and cyber warfare, CRC Press, 2015.

[64] V. M. Manjarrez Jr, "Border Security: Defining it is the Real Challenge," *Journal of Homeland Security and Emergency Management,* vol. 12, no. 4, pp. 793-800, 2015.

[65] A. Edward, "Immigration and Border Control," *Cato Journal,* vol. 32, no. 1, 2012.

[66] J. Blazakis, “Border security and unmanned aerial vehicles,” *Connections,* vol. 5, pp. 154-159, 2006.

[67] Department of Homeland Security, “Russian Government Cyber Activity Targeting Energy And Other Critical Infrastructure Sectors,” 2018. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA18-074A. [Accessed 04 05 2021].

[68] M. Gridneff and C. Gall, "Erdogan Says, ‘We Opened The Doors,’ And Clashes Erupt As Migrants Head For Europe," 2020. [Online]. Available: https://www.nytimes.com/2020/02/29/world/europe/turkey-migrants-eu.html. [Accessed 04 05 2021].

[69] S. Hawley, B. Read, C. Brafman-Kittner, N. Fraser, A. Thompson, Y. Rozhansky and S. Yashar, “APT39: An Iranian Cyber Espionage Group Focused On Personal Information,” 2019. [Online]. Available: https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html. [Accessed 04 05 2021].

[70] Symantec, “Thrip: Espionage Group Hits Satellite, Telecoms, And Defense Companies,” 2018. [Online]. Available: https://symantec-blogs.broadcom.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets. [Accessed 04 05 2021].