Improving Border Check Point Security

Alfredo M. RONCHI
JRC S2D2 – Politecnico di Milano, Milano, Italy
Tel: +39 393 0629373, Email: alfredo.ronchi@polimi.it

Abstract: *The combined effect of the increasing international travellers flows together with the risks due to illicit traffics and terrorism makes the evolution of actual borders control points a must. This both to eliminate borders bottlenecks, improve security and optimise the efforts. The present paper briefly introduces a general view on today's and tomorrow's border control system exploring and proposing new operational methods and solutions for border control procedures to increase the efficacy and efficiency of the whole security screening system at the same time reducing the efforts (costs/resources). The general description of the system logic and architecture introduces the core of the solution, the Trust Assessment System. A "black box" based on risk analysis and advanced machine learning algorithms aimed to assign a Traveller Trust Score to each single individual intentioned to cross the border. Main benefits are: improved checkpoint throughput, improved situational awareness and level of security, better traveller experience, optimisation of resources. The concept is that the traveller risk evaluation starts as soon as she/he applies for a visa, a passport or books a trip by whatever means of transport.*

Keywords: *border security. risk assessment, big data, human factors*

Setting the scene

The international travel flows continue to rise both thanks to low cost flights and countries that recently approached the tourism market playing a key role due to the huge number of travellers. This scale up of flows causes a growing pressure on border's check points and the need to process large volumes of people and goods at the crossing points without creating bottlenecks; at the same time, there is a need to provide better security at the borders (land, sea, air), keeping technology costs related to border crossing points (BCP – extended control area[1]) as low as possible. While security cannot be compromised, the traveller's experience should be positive. Trans-border crime causes border instability and vice-versa; hence strengthening border control helps to reduce crime, apprehend terrorists and detect prohibited weapons thus making safer the country. Yet, at the same time, measures need to be appropriate, in terms of efficiency (i.e. large numbers of crossings require

[1] e.g. BCP area may include part of the motorways or railroad stations equipped with cameras and sensors.

quick control checks; maintaining the current level of checks is becoming increasingly expensive), while assuring the effectiveness (i.e. potential threats have to be detected, whereas bona fide crossings should be made smoother or seamless). In order to achieve such goals, risk-based methods and systems for screening at border crossing must be defined and actually implemented[2] The use of smart and novel detection technology along with advanced data analytics can truly help to improve detection of potentially dangerous people and goods while limiting to fewer accurate checks informed by pre-selected and preliminary (and non-disruptive) risk-based analysis of the flows, in respect of the quality of life of the traveller, and adding economic vitality to the union of states.

European external borders

There is a need to define tomorrow's European's border control system and inter BCP real time information sharing, exploring and proposing new operational methods and solutions for border control procedures and identify new paths toward the effective and efficient adoption in real scenarios. The primary objective will be to provide the border control operators and practitioners with **enhanced situational awareness**, and capabilities to **timely and proper identification of potentially dangerous people and goods**, thus preventing smuggling and human trafficking.

Assumptions

In the proposed system perspective, the security check starts the moment a person buys a ticket or applies for a passport or visa (i.e., the earlier the information is provided, the better). New technologies enable the creation or integration of a personal traveller profile. In order to enhance security, improve efficiency and reduce costs, we start from four assumptions:

a) **NOT all EU borders are equal** – maritime and terrestrial perimeters, as well as Northern and Southern perimeters, require different screening strategies because the people crossing borders and the chorography shaping them are different;
b) **NOT all travellers and goods bring the same risk**. Bona-fide travellers need to feel safe, secure and at ease with the related 'bureaucratic' process. On the other hand, travellers and goods that compromise security and safety should be better detected;
c) **The flow of travellers is increasing** due to many reasons: tourism, economic migration, political and war refugees;
d) **The scarcity of human resources** to perform security screenings compared to the increasing flow of travellers.

[2] Such methods have to particularly pay attention to data protection and ethical concerns, such as social sorting/discrimination, increased exposure to violence, reduction of physical liberty/bodily integrity, invasive searches, reduction of freedom of movement, lack of transparency, lack of accountability, data protection, surveillance, use of irrelevant data, function creep and chilling effects.

Time management is essential to efficiently perform security checks, thus ensuring an increasing need of higher throughput. The outcomes will range from a light check for bona-fide travellers to a in depth-check or denial to access for risky travellers.

Today's and tomorrow's security screenings concept

In today's security screenings:

- Travellers are all the same (and, thus, bring the same risk);
- The screening process is entirely performed at the Border Crossing Point (BCP) (if no visa is required there are no security-related pre-screenings);
- The (security) screening targets are mainly the dangerous goods carried by travellers;
- (Human) Screeners interpret the outcomes of X-ray and ultrasonic scanners and no (or very little) interpretation of both the "(historical) profile of the traveller" and the human behaviour shown at the Border Crossing Point (BCP) is performed;
- Security screens are concentrated in relatively small, typically congested Border Crossing Point areas only.

In today's concept the human function is then used for interpreting what the machine says (i.e. what sensors read). The range of technologies employed is substantially limited to x-ray and ultrasonic equipment. More rarely, sniffers (for explosives) and thermo-graphic cameras (as those used with the SARS infection to quarantine monitoring of visitors to a country) are employed to screen travellers and support decision-making. In terms of data sharing[3], today the European situation is all but harmonised both in terms of data processing and assessment protocols, as well as in terms of Key Security Indicators (KSI) and security resources usage.

In tomorrow's security screenings:

- The screening target will be both smuggling (e.g., concealed weapons, stowaways, illegal substances) and the abnormal behaviour of travellers and their estimated intentions;
- Travellers will be clustered into virtual homogenous, risk-based groups and processed accordingly;
- Checks will be performed at different stages in the travel process, from the time the traveller arranges his or her travel until arrival at his or her destination[4];
- Human functions will directly contribute, with the support of machines and/or animals, in evaluating the traveller's profile, behaviour and intentions.

[3] Air carriers still do not share with airport security relevant information about passengers till the last minute.
[4] e.g. in new "global" approach - even outside airports' perimeters in case of a flying traveller

Human functions are more precisely termed Human Factors. This is a scientific discipline concerned with the understanding of the interactions among humans and other elements of a system, data and methods to design in order to optimize well-being and overall system performance; this approach to the check system involves more in general the human, technological and organisational (HTO) model.

Tomorrow security screenings HTO model: We must re-think the way technological and human functions are linked. The new human, technological and organisational (HTO) model must be defined based on three innovative pillars: A) Risk-based security screening; B) Security checks typology and, when possible, positioning; C) Real-time and batch networked information sharing.

Main components and objectives

The proposed solution will implement an innovative, international alert system based on the real time updated information stored in the system platform. The basic concept includes a" combined" risk–analysis-based system for border and customs authorities and security, this will improve: Coordination and enable close cooperation among authorities; Solutions for remote detection of abnormal behaviours, could this also include behaviour in the social media. A double tier risk-based approach proposes innovation around the concept of customised configuration of border control points (European Modular Border Crossing Point - EMC), the adoption of a risk-based BCP decision-making process (Trust Assessment System – TAS) and, for the purposes of improved risk-management coordination and cooperation, the EU Security Dashboard (ESD). More effective use of intelligence to reduce risks at borders.

Objective 1. Change the border crossing point paradigm from the current "check-everything-at-the-border" to the more efficient "check-everything-till-the-border" (i.e., from a "checkpoint" to a "check-process") by exploiting intelligence to assess and reduce the risk at BCPs, while improving the coordination, cooperation, and information sharing among all relevant stakeholders, such as border control authorities.

Objective 2. Improve security checks from the current "memory-less" approach to a more advanced risk-based approach (i.e. based on both historical and current quantity and quality of information provided);

In the proposed model a risk-based pre-screening (i.e. before the border crossing point) is not just possible but needed to start profiling the traveller and better use the resources at the BCP, the personal information relating to the traveller matters as well as "when" it is provided (i.e. timely or not). The proposed model starts from the assumption that bona fide travellers may be willing to share their personal information to ensure a safer and more secure society, given the assurance that their

information is securely stored, properly used and not manipulated[5]. In addition, the Fast Track APP will include soft incentives for them to cooperate, in the form of nudges, or small incentives like free Wi-Fi or points on the frequent traveller card. The user experience of the whole service will be analysed to avoid cumbersome and lengthy data entry.

Double tier risk-based approach

One of the key innovation factors is a double tier risk-based approach. On the top level the dynamic Modular Border Crossing Point (MBCP) risk-based approach considers the first assumption "*NOT all borders are equal*" in the specific field of typical risks related to the single BCP optimising the use of resources. An additional goal is to reduce the cost of technologies in border security applications as a result of risk-based scalable modular border crossing point (MBCP) configuration, and on the shelf low cost technologies to integrate current physical-inspections-based security checks with contactless or low-invasive detection mechanisms. This early and proactive risk analysis results in an evaluation that represents an input to cross-border checks enabling the identification of bona-fide travellers, with the ultimate goal of improving the accuracy and effectiveness of border crossing activities while reducing costs.

Trust Assessment System

As a consequence of the second assumption "*NOT all travellers and goods bring the same risk*" we find the Trust Assessment System (TAS)[6]. The approach proposes a mix of technological and human functions to identify the "level of trust" characterising each traveller, a score plus some "instructions" about how to interpret the score will represent the output of the "black box" we call TAS. For the purposes of this document we term "sensor" any "module" providing a normalised input to the TAS, that means we consider as input a wide range of data coming from personal information voluntarily provided by travellers to CBRN detectors. Each BCP is configured accordingly with the local needs; this means a potentially different arrangement of "sensors", each active sensor will transfer on the system hub a rich set of normalised data[7], TAS will receive such normalised data including historical data coming from the Dashboard[8] and process them thanks to the harmonious balance of technology and human factors to identify a Traveller Trust Score[9]. The TTS will provide the basis for each traveller screening and will be broadcasted on the system Dashboard. In the proposed HTO model,

---

5 Personal information will be provided on a voulountary basis and will managed in compliance with the EU General Data Protection Regulation (GDPR)

6 Trust Assessment System - the adoption of a risk-based decision-making process will allow to "process" travellers according to five risk-based groups, namely: Very high-risk passengers (those with a negative security record & negatively signalled by authorities); High risk passengers (those with a negative security record but not signalled by authorities); Medium risk passengers (those with no security record and not signalled by authorities); Low risk (those with positive security record); Very low risk passengers (those with a positive security record and positively signalled by authorities).

7 sensor data plus annotations, these data will contribute to better interpret raw data provided by sensors and enable the evaluation of human factors

8 The dashboard connects clustered BCPs and provide access to the system data base and LEA's criminal data banks.

9 TAS output includes both TTS score & some "instructions" to correctly interpret the TTS underlining the combined use of tech. and human resources.

the risk level of a traveller will determine, for every journey, the screening groups into which the traveller will fall for security clearance.

The collection and analysis of information from multiple sources represents an important factor of innovation, as the risk assessment will be based on: information provided by the traveller on a voluntary basis (duly checked), agreement with "carriers" and destination managers, as well as sensors, PNR, criminal databases and other relevant resources (such as social media, that might provide additional info or weak signal on travellers' movement and intentions). The usage of multiple sources of information is motivated by the following reasons:

- "Official" data (such as PNR or traditional security databases) do not often allow to achieve a whole picture of travellers' movement due to the lack of pieces of information;
- "Weak signals" on travellers' movement (provided by or extracted from additional data sources such as social media) can complement such a picture;
- The information on travellers' movements is not enough for assessing the risk level of passengers: we also need information on people behaviour and other attitudes to create an effective (and informed) risk profile to support decisions at the checkpoints. Additional sources such as social media and sensors can provide relevant information to inform advanced analytics with the aim of assessing such a risk profile and perform the so-called "digital screening"[10].
- Lastly but not less relevant main information about travellers are shared with security officers only when the traveller is already "on board" concentrating all the security measures in an overcrowded space and limited timeframe.

We can consider the "additional" information[11] according to the "fitness for purpose" approach, considering the practicability in collecting them and the "user acceptance". The outlined solution is a system of systems, where multiple sources providing heterogeneous data will be organised, modelled and processed, based on a set of novel data analytics and analysis algorithms. Through adaptive cost-effective solutions for border crossing points and selective checks, the main aim is to quickly identify "bona-fide" travellers through the collection of relevant information about each single traveller from the time the travel ticket is bought or visa is issued, thus creating (as much as reasonably practicable) a personal trust profile for each traveller approaching EU crossing points.

Big data and social media

One of the "sensors" providing input "signals" to the TAS is "big data and social media", an objective of the project is to selectively collect and analyse data coming from different sources including: Social

[10] The "digital screening" (which also includes the analysis of social media, but also the analysis of other sources in Internet) is an interesting trend that is being pursued also by US (actually they already started with automatic tools). See this article: https://www.forbes.com/sites/kalevleetaru/2017/01/29/we-already-screen-cell-phones-at-the-border-will-social-media-be-any-different/#450fe3a25fa3.

[11] which could also include personal information

media information (time, location when available, networks, content/semantic); Traditional structured data from institutional databases (ERP, etc.); Travel process events (visa applications, tickets, etc.); ID checks; GeoTime Series, Sensors data, etc.. The traveller's data would generally be collected from publicly available sources or will be provided voluntarily by the passenger to gain access to the "Fast-Track"; private information will not be collected without informed consent, in respect of privacy regulations[12] and confidentiality. This integration represents a major challenge of social media analytics, as insights from the semantic processing and analysis of social media information are tightly bound to the ability of identifying the author of posts and tie his/her activity on social media with historical data from more traditional sources.

The semantic engine part of the solution will be in charge of deep semantic text analysis. This analysis will start from the output of Open Source Intelligence (OSINT) crawler (either Surface or Deep/Dark Web) or from other kind of sensors acquiring unstructured contents (also web form filled by traveller). If this content will be a multimedia one, a Speech to Text technology (STT) is needed in order to transcribe audio into electronically and accessible text. Understanding events/intentions in advance (Ex-Ante) and apply reasoning to the lessons learned (Ex-Post) are a crucial point from the investigation and deduction point of view. Prevention is the first step useful to understand if someone is writing/telling "bad" words regarding a politician of a country, a critical infrastructure, an organization. At the same time analysing the information coming from historical use cases, so after the event occurred, can give added value either to the live analysing or to the prevention one.

As already mentioned this solution will implement also a crawling for both Surface and Deep/Dark web, to complement and integrate the other sources of information already described previously. The surface crawling component will be based on open technologies allowing end users to set the sources they need to acquire data from. The surface crawler engine will be able to gather content from open sources like RSS, Social Networks (Twitter, Facebook, Instagram), Web and Search Engines (mainly Google, Bing and Yahoo). Surface crawler will be then extended to Deep Web by integrating additional and dedicated crawlers for these types of sources and combining the overall solution with anonymizers to access Dark Web. Plain text will be then extracted from the original content acquired by the sources under crawling and delivered to the semantic engine, for elaboration (content categorization, entity/relation/emotions extraction, stylo-metric analysis, etc.). The Deep Web crawler will be based on the adoption and integration of multiple dedicated crawlers, both proprietary and open, in order to have a synergy of their best functionalities and capabilities. In order to extend this capability also to Dark Web, making it even more relevant for illegal activities monitoring, an integration of dedicated proxy solution will be required: TOR and I2P will be mainly considered for this purpose. The fundamental concept is to achieve speed and mobility during the stop and search

[12] i.e. EU - General Data Protection Regulation

routine of travellers in every physical location they are. The solution can be used as well for accessing the data of the travellers prior to the date of the planned travel adding value to the Trust Assessment and delineating a picture of the traveller prior to his arrival to the departure gate.

Traveller's Trust Level

As already stated more times, the idea is that the traveller risk evaluation starts as soon as she/he applies for a visa, a passport or books a trip by whatever means of transport. The travellers' journey is broken down into the following phases:

- Booking phase, when the tickets are bought;
- Preparation, the time between the booking phase and the actual initiation of the trip;
- Pre-screening phase, all the trip segments before the border crossing;
- Screening points, the border crossing itself;
- After screening, the moments after the border crossing before the end of the trip.

In each of these phases, the system may collect information on the traveller, with the aim of determining the Traveller's Trust Level (TTL). The information to be used to determine the TTL are the following:

- Personal information: including data collected by LEAs (National Polices, Interpol, Europol, Frontex, FBI, etc.), or soft data like social network data on published contents and network of contacts,
- Travel specific information, like number of the flight/train/bus, hotel booking (if any), transports booking at destination (car, motorbike, public transport…), period of stay, reason of the visit, and so on. For the travellers moving by car: the type, colour and identification marks of the vehicle (number plate) used to cross the border, the number of travelling passengers, the expected time range of the border crossing;
- Behavioural data: including historical data from frequent traveller's fidelity cards and credit cards, data collected by the platform during previous travels, or real-time acquisition of behavioural data via different "sensors".
- Passenger shadowing (train stations, bus stations, terminals, automatic identification of car plates, etc.);
- Advanced big data analytics (Internet, social media, fake news, WIFI connections, etc.);
- ID verification / Biometrics etc. etc.;
- Remote sensing, sensors, etc. etc. (IoT, satellites, drones, etc.); In depth personal checks.

Furthermore, the casting of the information net and the reliability of information need to be accurate; moreover, building of trust between parties and the sharing of data are as important as technology advancement. We outline again the initial concept - while security cannot be compromised, the traveller's experience should be positive.

Results

This solution aims to apply technologies in an efficient but effective manner by integrating new technologies with a risk-based outcome focussed approach to increase the reliability of the border crossing process and at the same time the experience of the traveller. This solution has been conceived as a system level goal-oriented project, which means that the impact relies on the capacity of the system to integrate in a sound architecture for individual technologies that will provide a larger benefit as a whole than in individual deployment.

The primary objective of the project is to make an economically sustainable technological improvement in security at crossing points based on a risk analysis that combines information from multiple sources to enhance situational awareness for border control practitioners. The technology component is deployed based upon a researched operational concept for risk analysis. Flow management innovation (fair and fast) through innovative multiple information processing and use of advanced sensors / input channels to identify the TTS. Integrate current physical-inspection-based security checks with contactless or non-obvious detection mechanisms (like border physical checks) – progressive migration from actual solutions to the new approach, from the current "check-everything-at-the-border" to the more efficient "check-everything-till-the-border" (i.e., from a "checkpoint" to a "check-process"), from the current "memory-less" approach to a more advanced risk-based approach (i.e. based on both historical and current quantity and quality of information provided).

Potential Benefits

The underlying concept is that not all borders crossing points are equal and particular situations and events could change substantially operational conditions, so potentially each BCP could be tailored to suit the needs of an environment at a given time saving unnecessary resources. Thanks to the full implementation of the solution the BCP will improve its throughput without the need to add more personnel. Use of on the shelf technologies as needed by the specific crossing point and situation. Economic benefits will derive by reinforcing the effectiveness of crossing borders through approved techniques and procedures this should be seen as an encouragement and reassurance to travel, thus increasing the GDP collectively across and through the countries. Additional benefits are: Ensure privacy and human rights are respected within new approaches to risk-based border crossing; Decrease border crossing times for the majority of travellers; Significantly reduce the cost of border security checks as a result of risk-based scalable border crossing point (BCP) configuration, and on-the-shelf, low-cost technologies. In addition, the availability of TAS "sensors" open standards may offer a business opportunity to hard and soft companies.

Future developments

<<For the traveller it would be ideal to cross borders without being slowed down. It is indeed likely that, in the next ten years or so, technologies make it possible to implement "no gate crossing point solutions"…>> [European Commission Study]

Recent years have witnessed technological and social changes appearing at an unexpected pace and spanning a wide set of aspects, such as technologies for personal identification, detection systems, social habits, new threats and new privacy and personal (ethical and social) issues. As a consequence, the challenge is to foresee technological solutions and social behaviours ten years from now, and the adoption of different technologies and behavioural models from those in play now. In the transport domain, a trade-off will emerge between the need to guarantee security of travellers, even against unexpected threats, and speed of security controls. Accordingly, it would be ideal for the traveller to be able to cross borders without being slowed down by queuing at crossing points gates as it was experimented in Dubai. The risk-based solution described above represents a sounding a building block to achieve the result. In a decade[13] from now, technologies will make it possible to implement "no gate crossing point solutions[14]" that based on risk assessment methods, allow for seamless crossing of borders and security checks for the vast majority of travellers who meet the conditions of entry, and make sure that those who do not fulfil such conditions are refused entry.

Main aspects to be considered: to understand how these technologies will be accepted (or rejected) by the public and key stakeholders[15] requires greater insight into: (1) the likely constellations of technologies; (2) their potential ethical, legal and societal impacts, and (3) real-world, contextualised acceptability experiments assessing the passenger's "feeling of safety".

Conclusions

This paper proposes a new approach to border security checks based on risk analysis and trust assessments shared at the international level, it applies a "harmonisation by design" principle to ensure the progressive harmonisation and homogeneity of the procedures. The key technologies foreseen have been already tested on different borders both in Europe and South America / Africa. The system platform acts on six lines: Innovative double tier risk-based approach to security checks; High-penetration safe technologies for remote and flexible on-the-go screening of persons and

13 PROTECT H2020 project: http://projectprotect.eu/ FRONTEX organizes workshops on Biometrics on the move for gateless BCPs.

14 *Refer also to the IATA and ACI Smart Security Initiative http://www.iata.org/whatwedo/security/Pages/smart-security.aspx*

15 Air companies, Shipping companies, Railroad companies, Bus companies, Airports, Harbours, Highways companies, Destination managers,, Tourism operators, IATA, EDA, Frontex, Interpol, Europol, etc.

vehicles; Mobile solutions based on mass market devices; Travellers' pre-registration; real-time information sharing, traveller's trust profile. "Bona Fide" travellers will benefit from simplified security controls based on prior processing of travel and relevant Internet data. The solution proposes a risk-based, outcome-focused approach to security controls rather than the current "one size fits all" scheme - pre-evaluating a personal risk profile on the basis of the traveller's "history", integrating available international police data, API[16] and PNR data, and public data available on line, within the legal capacity of border authorities. The paper focus on one of the innovative solutions the Trust Assessment System – TAS, a kind of "black box" receiving as input a specific set of data coming from "sensors" analysing traveller's information and behaviour and evaluating a traveller trust score (TTS) that together with additional "instructions" will determine the classification of the specific traveller and consequently the required security check procedure.

16 Advance Passenger Information

References

[1.] Baggio, Battista, et al., "Security evaluation of biometric authentication systems under real spoofing attacks", IET biometrics, Vol. 1, No. 1, 2012, pp. 11-24.

[2.] Cano, J., Rios Insua, D., Tedeschi, A., Turhan, U. (2014), Security Economics: A Multi-objective Adversarial Risk Analysis Approach to Airport Protection, Annals of Operations Research (ANOR),

[3.] Ceri Stefano, Bozzon Alessandro, Brambilla Marco, Della Valle Emanuele, Fraternali Piero: Web Information Retrieval. Data-centric systems and applications, Springer 2013, ISBN 978-3-642-39313-6, pp. I-XIV, 1-284

[4.] Colombo Simone, "Risk-based Decision Making in Complex Systems: the ALBA Method", IEEE Conference on Industrial Engineering and Engineering Management (IEEM), Bali, Indonesia, 2016, In press.

[5.] Colombo Simone and Golzio L., "The Plant Simulator as viable means to prevent and manage risk through competencies management: Experiment results", Safety Science, Volume 84, 2016, pagg. 46–56.

[6.] Colombo Simone, Nazir S., Gallace A., Manca D., "Experiment-based decision making in complex systems", Chemical Engineering Transactions, Volume 36, 2014, pagg. 85-90, ISBN: 19749791.

[7.] Daugman, J., "How iris recognition works", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, 2004, pp. 21-30.

[8.] Di Giacomo V., Felici M., Meduri V., Presenza D., Riccucci C., Tedeschi A. (2008), Using Security and Dependability Patterns for Reaction Processes, Proceedings of the Nineteenth International Workshop on Database and Expert Systems Application (DEXA 2008), 1-5 September 2008, Turin, Italy

[9.] Iris Challenge Evaluation (ICE) http://www.nist.gov/itl/iad/ig/ice.cfm

[10.] Lenharo, S., "Brazilian National Biometric Selection", Keynote speech, International Joint Conference on Biometrics, 2014.

[11.] Mtsweni Jabu, Shozi Nobubele Angel, Matenche Kgwadi, Mutemwa Muyowa, Mkhonto Njabulo, van Vuuren Joey Jansen. 2016. Development of a Semantic-enabled Cybersecurity Threat Intelligence Sharing Model. In the proceedings of the ICCWS2016, Boston, USA, May 2016. ISBN: ISBN:978191081083-5

[12.] PNR Directive was approved in April 2016 and published in the Official Journal of the EU on 4 May 2016 – see Directive (Eu) 2016/681 of The European Parliament and of The Council of 27 April 2016

[13.] Pollini, A., Tedeschi, A., Cano, J. (2013), Modeling an Emerging Terrorist Threat against Airport Security Scenario, EUROInform Conference, Rome, July 2013.

[14.] Ronchi Alfredo M., WSIS Forum 2015, High Policy Statements. https://www.itu.int/net4/wsis/forum/2015/Content/doc/outcomes/Policy_Statements_Booklet_WSIS2015.pdf

[15.] Ronchi Alfredo M., Duggal Pavan, et al., WSIS Forum 2016 Outcomes, https://www.itu.int/net4/wsis/forum/2016/Outcomes/

[16.] Alfredo A.M., Data: ownership, use, abuse and misuse, ISBN 978-93-5254-019-8, The International Journal on Cyberlaw, Cybercrime and Cybersecurity Volume 1 Issue 1 - 2016

[17.] Ronchi A.M., ICTs for Safety & Security: Their potential relevant impact in the African continent, ISBN 978-1-905824-57-1, IEEE Explore - IIMC International Information Management Corporation, 2017

[18.] Shozi NA & Mtsweni J.. 2016. Big data privacy and security: A systematic analysis of current and future challenges. In the proceedings of the ICCWS2016, Boston, USA, p.296-303. 17-18 May 2016. ISBN:978191081083-5

EUROSUR http://frontex.europa.eu/intelligence/eurosur/ ABC4EU - www.abc4eu.com

EFFISEC - http://www.effisec.eu Fast Pass - https://www.fastpass-project.eu