An Innovative Security Screening Architecture for Detecting Illicit Goods and Threats

[1]Athanasios Skraparlis, [2]Klimis Ntalianis, [3]Dimitris Kouremenos, [4]Nikolaos Mastorakis

[1]University of West Attica, Egaleo, Athens, Greece
[2]Department of Business Administration, University of West Attica, Egaleo, Athens, Greece
[3]National Centre for Scientific Research "Demokritos", Athens, Greece
[4]Industrial Engineering Department, Technical University of Sofia, Sofia, Bulgaria

Abstract— **Every year, millions of letters/parcels containing illicit goods are detected by customs authorities, which use traditional security screening equipment. However this equipment cannot detect all kinds of illicit goods and the detection procedure heavily depends on the attention of the customs officer. In order to achieve sufficiently fast intelligent screening of the large volumes of letters/parcels and detect all common kinds of threats, this paper proposes a highly innovative architecture well-beyond the state-of-art. In particular the proposed architecture monitors every letter/parcel by incorporating: (a) terahertz/X-ray sensors, (b) chemical, biological, radiological and nuclear (CBNR) sensors, (c) artificial robot-noses for narcotics, explosives etc., (d) magnetometers for weapons, firearms, banknotes etc., (e) acoustic sensors for liquids/gases/solids, (f) weight/pressure sensors to measure weight distribution, size and shape. Sensory information can be: (a) used to create a "Spectral Signatures Dictionary of Illicit Goods and Threats", (b) fused to segment/isolate illicit goods and (c) visualized in the form of annotated high-resolution tensor-structured (3D/4D) multisensory image data. The proposed solution also gathers available information for the sender/recipient from various resources, while it also analyzes data from the dark web. All information is forwarded to an AI-based knowledge infrastructure.**

Keywords— **security screening architecture, sensory/non-sensory, border protection, knowledge infrastructure.**

I. INTRODUCTION

IN 2019, the United Nations Office on Drugs and Crime (UNODC) estimated the annual value of the trade in narcotics to lie between EUR/USD 344/400 and 516/600 billion worldwide. Illicit trade in tobacco represents 10 to 12% of global tobacco consumption, with an estimated illicit volume of up to 600 billion illegal cigarettes [1]. Global trade in counterfeits amounted to EUR 412 billion in 2019. This corresponds to 2.5% of world trade. Imports into the European Union (EU) of counterfeits in 2019 reached EUR 119 billion, corresponding to 5.8% of total EU imports from the rest of the world. The main provenance economy of counterfeit goods remains China. Other important sources of fakes include Turkey, the United Arab Emirates and Singapore [2].

Economic leakages from illicit trade create an annual drain on the global economy of EUR/USD 1.89/2.2 trillion – nearly 3% of the world's economy [3].

The delivery of drugs purchased on the darknet is generally carried out by public and private postal services without their knowledge, with parcels often being sent to anonymous post office boxes, including automated booths, or "packstations", for self-service collection. In jurisdictions with strong secrecy-of-correspondence laws, drugs are often dispatched in letters. Existing postal services are used not only for drug deliveries but also for money transfers [4] and other threats such as chemical, biological, nuclear, radiological and explosive materials, firearms, waste, trafficked wildlife, cultural goods, contraband or counterfeit items including counterfeit identity documents, and fake medicines. This is due to the fact that organized crime groups feel that they run a relatively low risk of being arrested when using postal services.

In order to enter/exit the EU through postal/express courier flows, all these threats and dangerous and illicit goods (TDIGs) have to pass across the EU's external borders, which are protected by the EU's customs authorities and Law Enforcement Agencies (LEAs). EU's customs and LEAs authorities not only face increasing volumes but they also have a range of tasks to fulfill besides security. Furthermore, Western Europe is among the largest markets of cross-border postal and express services with 3.2 billion items per year, a volume that increases with the years [3], [5]. Full examination of these flows means:

- manual intervention, which significantly impedes these flows and heavily intrudes into privacy;
- extremely high levels of human effort. In particular customs and LEAs authorities' officers have to spend about 53 million hours per year (assuming a 60-seconds examination), or 6,625,000 day-labors! To do so, about 25,500 employees should be hired, only to examine these flows!

Currently, customs authorities pass these flows through typical security screening systems that are usually based on X-rays. However, these systems:

- cannot detect all common kinds of threats in all kinds of packaging and distributions within a letter/parcel. So many dangerous letters and parcels may not be detected and easily

pass the EU borders;

• heavily depend on the attention and experience of the practitioners and operators and offer limited ways to stimulate customs and LEAs officers' attention, when possible TDIGs are detected;

• use very limited information to detect possible TDIGs and assess their threat levels.

II. STATE OF ART

In 2015, agents with the Department of Homeland Security posing as passengers snuck fake explosives through the security lines of several of the nation's busiest airports. During the test, Transportation Security Administration (TSA) officers missed 67 of the 70 fake weapons that went through the checks — a failure rate of 95%. Additionally, TSA officers detected twice as many firearms per million passengers screened at airport security checkpoints nationwide in 2020 compared to 2019 [6]. However, the miss rate for 2019 was at least 63% [7]. Since postal flows pass through these security screening systems, it is estimated that failure of the current screening procedure is very high, since not only firearms travel through these flows but also many other illicit goods. Exact failure of the screening systems can only be measured in a lab environment because the exact number of letters/parcels with illicit goods/threats and the exact number of non-illicit letters/parcels should be known.

Several companies have created different models for security screening such as Leidos's CT-120, Bruker Optik's S1 TITAN Handheld XRF Analyzer, Rapiscan's RTT110, 628DV320KV, GEMINI 100100 and ORION 922CX, Smiths Group's IONSCAN 600 and CTX 9800 DSi and Analogic Corporation's High Speed EDS.

However none of these products can detect all kinds of illicit goods. The proposed architecture is the first to consider all kinds of common illicit goods such as chemical, biological, nuclear, radiological and explosive (explosives and explosive precursors) materials, drugs, firearms, money, waste, trafficked wildlife, cultural goods, contraband or counterfeit items including counterfeit identity documents, and fake medicines. All global leaders in security screening offer different products for different hazards but no one offers an integrated system for all common illicit goods.

Most existing systems are based on Computed Tomography (CT) imaging and some (e.g. Terasense's Terahertz High-Speed Imaging Scanner) are based on Terahertz imaging. The proposed architecture is the first to integrate Terahertz, CT imaging and other sensory technologies for better detection and visualization of all kinds of common illicit goods and threats.

None of the existing systems in the market incorporates artificial robot-noses to better detect drugs and explosives. FP7 SNIFFER (SNIFFER: Grant agreement ID: 285203) [8] has tried out bio-mimicry, synthetic diamond sensors, as a standalone technology. The proposed architecture fuses data from this technology and other sensing technologies, to provide more efficient detection of drugs and explosives. The robot-nose could detect drugs hidden in high-density parcels, in small quantities and different distributions, under

occlusions, inside of shielded material, too thick or deep etc.. In such difficult cases, typical security screenings based on CT or Terahertz usually fail.

None of the existing systems incorporates acoustic sensors and pressure sensors to better distinguish among solid, liquid and gas substances. The proposed architecture is the first to integrate acoustic sensors to better distinguish among substances and pressure sensors to better delimit the occupied space of each substance and as a result: (a) increase the quality of the produced 3D images, by better detecting the occupied area, (b) further increase the knowledge of each substance within a letter/parcel, by recognizing its nature (solid, liquid, gas).

United States Postal Inspection Service (USPIS) is working with Customs and Border Protection (CBP) and foreign postal operators to ensure Advance Electronic Data (AED) inside barcodes, is on all inbound mail. The detailed information in AED, like full names and addresses, weight, date, and more can be instantly captured in both outgoing and incoming processing centers. The proposed architecture is moving a step forward by also considering police records, social media information for sender and recipient and data from the dark web and other criminality data. This sensitive information cannot be attached on AED tags.

USPIS's systems and other existing technologies can test over 300 illicit substances (mainly drugs and narcotics) without needing to open containers or plastic bags [9]. The proposed architecture introduces the first ever "Spectral Signatures Dictionary of Illicit Goods and Threats", for all common illicit goods and threats, passing through postal flows.

On the other hand there are also some important international research and innovation activities, related to the proposed architecture. In particular:

• FP7 TERASCREEN (Grant agreement ID: 312496) [10] developed passive and active operation at several Terahertz frequencies. The resulting multi-frequency, multi-mode images were processed automatically in real-time to reveal the location of potentially harmful objects concealed on a person.

• FP7 SNIFFER (Grant agreement ID: 285203) [8] captured and analyzed odours of explosives using olfactory biosensors. The SNIFFER device combines in a one-stop shop sampling, pre-concentration and pre-treatment with bio-mimicry, synthetic diamond sensor technology and multi-parametric training software.

• FP7 ACXIS (Grant agreement ID: 312998) [11] developed a manufacturer independent reference database for X-ray images of illegal and legitimate cargo, procedures and algorithms to uniform X-ray images of different cargo scanners and measurement parameters, and an automated identification of potentially illegal cargo.

• H2020 C-BORD (Grant agreement ID: 653323) [12] developed technologies for non-intrusive inspection of containerised freight delivering improved X-rays, Target Neutron Interrogation, Photofission, Sniffing and Passive Detection.

• H2020 BorderSens (Grant agreement ID: 833787) [13] develops a portable, wireless single prototype device with

the capability to quickly test for different types of drugs,
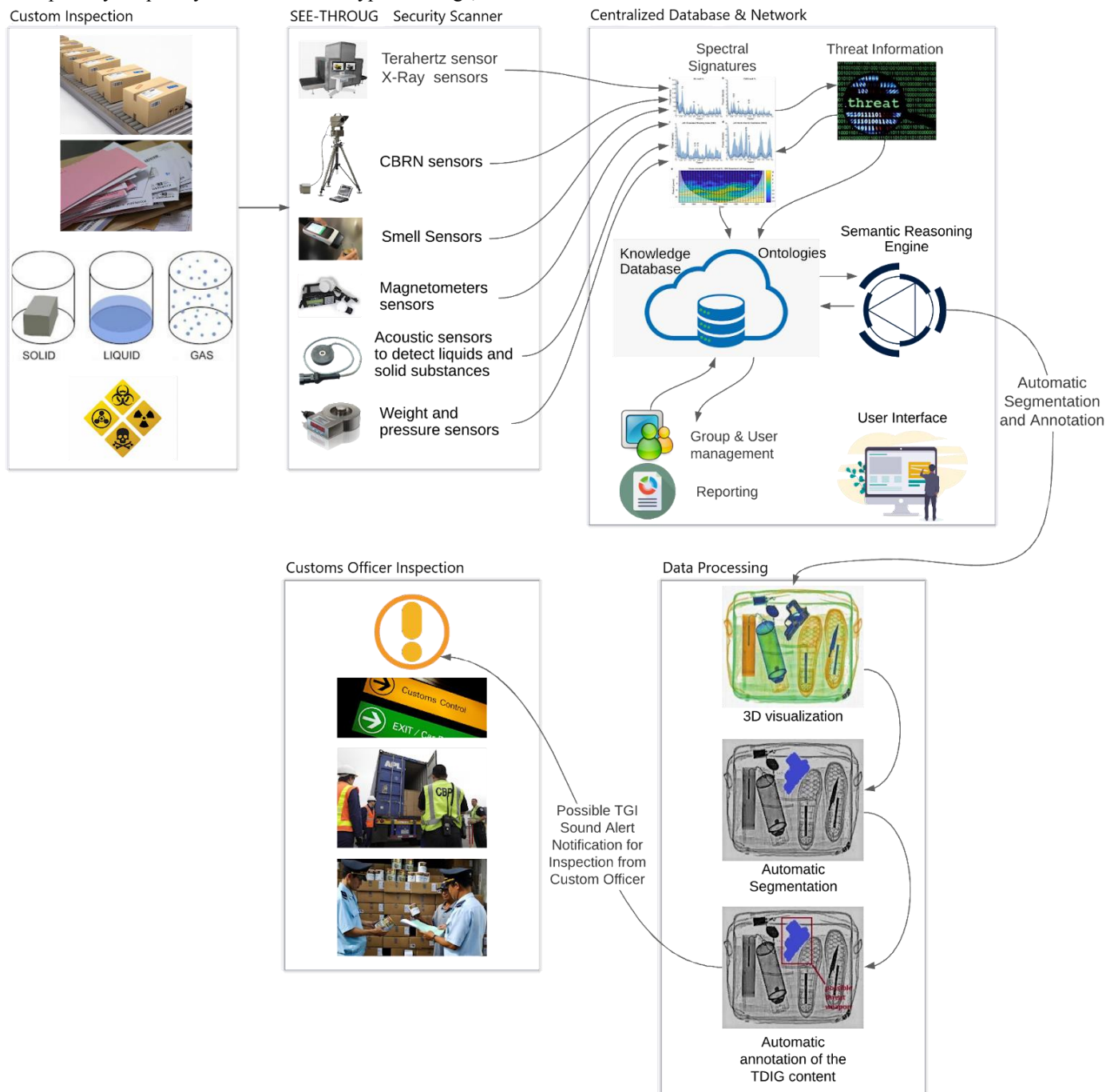
Figure 1: Overall architecture of the proposed security screening architecture

precursors and adulterants/cutting agents. The end date of BorderSens is 31/8/23.

• H2020 ENTRANCE (Grant agreement ID: 883424) [14] delivers: 1) a suite for detecting contraband hidden in high-density cargo, 2) an enhanced relocatable unit for non-intrusive detection of wide number of threats including explosives, illicit drugs, chemical warfare agents, nuclear and radioactive materials (NR) and special nuclear materials (SNM). The end date of ENTRANCE is 30/9/23.

• H2020 MULTISCAN 3D (Grant agreement ID:

101020100) [15] offers a new system that is based on high energy 3D X-ray tomography, neutron interrogation/photofission and narrow gamma ray beam based nuclear resonance fluorescence. The end date of MULTISCAN 3D is 28/2/25.

• H2020 SilentBorder (Grant agreement ID: 101021812) [16] delivered a screening technology based on passive cosmic-ray tomography (CRT). The end date of SilentBorder is 30/4/25.

There are also several other interesting schemes focusing on security screening [17]-[30] . However most of these schemes

consider only X-ray information for security screening. The proposed architecture also extends all aforementioned security screening systems and international research and innovation activities, by incorporating ontologies to describe in a formal way, all gathered information for every letter/parcel. Additionally a semantic reasoning engine is introduced to play the role of a decision support system, which considers all available (visual, textual, acoustic etc.) information and not only parts of it. Existing detection algorithms consider only parts of the available information. Finally, all extracted knowledge is gathered in a continuously expanding knowledge database, to confront new tactics developed by offenders.

Another ambition of the proposed architecture is to provide at least 10% less overall ionizing radiation per year than the existing CT and X-ray systems of the market, since it is supported by non-ionizing Terahertz radiation and other non-ionizing sensory technologies. Furthermore, the proposed architecture is anticipated to lead to an average screening speed of 2,700 items (letters/parcels) per hour, performing 2-5% better than existing state-of-art systems. This is due to the fact that the decision support system visualizes more clearly, automatically segments and annotates all possible threats, so that customs officers can decide faster, compared to existing screening equipment, whether to stop and open an item or to let it pass.

III. THE PROPOSED ARCHITECTURE

The proposed overall architecture is presented in Figure 1. In particular, in order to succeed to its mission, the proposed architecture:
- Enables detection of all common kinds of illicit goods and threats in postal flows, which need different sensors and technologies to be detected, without impeding those flows or introducing disproportionate intrusion into privacy.
- Reinforces customs risk management and effective controls and enables customs authorities to detect illicit goods and threats, without disrupting or unnecessarily hampering trade flows.
- Gathers terahertz sensory information for every letter/parcel.
- Gathers X-rays sensory information for every letter/parcel.

More particularly, according to the absorption law [31] the energy of the X-rays is:

$$K = K_0 e^{-\nu y} = K_0 \exp(-\nu y) \tag{1}$$

where K is the captured intensity expressed as a function of the thickness y and the emitted intensity K_0. The variable ν represents the attenuation coefficient which straightforwardly depends on the captured energy. In case an object has l materials, each material having thickness y_p and coefficients v_p, $p = 1, …, l$, then modeling of the intensity to be captured is provided by the following equation:

$$K = K_0 exp\left(-\sum_j v_j y_j\right) \tag{2}$$

while v can be expressed by the following equation:

$$\nu = \beta(Y, F)\tau \tag{3}$$

where Y represents the atomic number, F is the captured energy, τ is the density and $\beta(Y, F)$ represents the mass attenuation coefficient in terms of the atomic number Y and the captured energy F.

There are single-energy and multi-energy X-ray systems, where in the latter, q different X-ray images can be recorded for q different energies [32]. If $q=2$ then we have two energies: F_1 for high level and F_2 for low level. Then for $j=1, 2$ and by using equations (1) and (3) we conclude to:

$$\frac{K_j}{K_0} = \exp(-\beta(Y, F_j)\tau y) \tag{4}$$

and to the following ratio

$$RT = \frac{ln(K_2/K_0)}{ln(K_1/K_0)} = \frac{\beta(Y, F_2)}{\beta(Y, F_1)} \tag{5}$$

The value for Y (atomic number) is available on publicly available tables.
- Gathers CBRN sensory information for detecting possible CBRN threats.
- Gathers sensory information from artificial robot-noses [33] for smelling narcotics, explosives and other odors from various threats.
- Gathers sensory information from magnetometers to detect metal weapons, firearms, banknotes and other magnetized illicit goods and threats.
- Gathers sensory information from acoustic sensors to detect liquids, gases and solid substances and define separation lines among them within a letter/parcel.
- Gathers sensory information from weight and pressure sensors to measure the weight, weight distribution, size and shape of letters/parcels, as well as of their content.
- Gathers additional, non-sensory, critical information for every letter/parcel: (a) that refers to the sender, the recipient, their addresses and their nationalities, (b) written and non-written on the wrapping of the letter/parcel (such as no return address, restrictive markings, letters sealed with tape and excessive tape usage in parcels, misspelled words, badly typed or written, unknown powder or suspicious substance on the surface of a letter/parcel, oily stains, discolorations, or crystallization on wrapper, strange odor, rigid, bulky, lopsided or uneven areas on the wrapper, protruding wires, addressed to title only (e.g. recipient: Operations Manager, without referring to her/his name)), (c) from police records of sender/recipient as well as other police records (e.g. safety level of neighborhood/city/country of the sender/recipient), (d) from the sender's/recipient's possible social media accounts. Profile analysis of sender/recipient will be performed in order to detect antisocial/strange/extremist behaviors of the sender/recipient as well as of their contacts/followers/friends, (e) coming from dark web (trendy illicit goods and threats, trendy countries that sale/buy illicit goods and threats etc.).
- Proposes the first ever "Spectral Signatures Dictionary of Illicit Goods and Threats". In particular, different substances reflect and transmit characteristic combinations of terahertz

waves, which make them distinguishable from other materials. This is the chemical-discriminating -capability

(a)   (b)   (c)
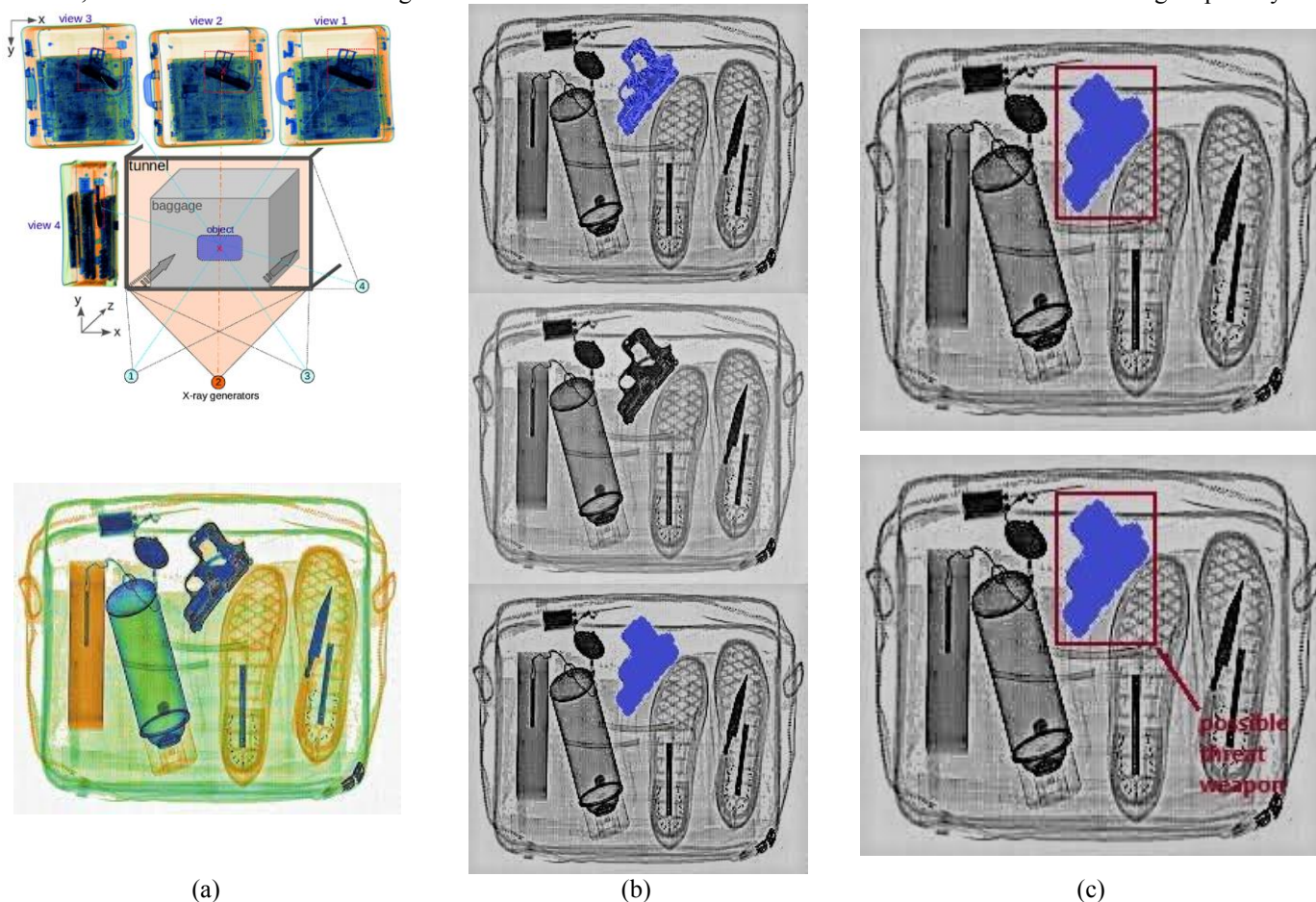
Figure 2: (a) 3D visualization (b) automatic segmentation (c) automatic annotation of the TDIG content

(spectroscopy) of Terahertz imaging systems, which tells what these illicit items are made of. Terahertz sensing provides much high quality information to the dictionary.
The other sensors also provide very useful information for specific illicit goods and threats.

• Performs knowledge modeling using ontologies to describe in a formal way: (a) all common kinds of illicit goods and threats, including information from the Spectral Signatures Dictionary of illicit goods and threats, (b) each letter/parcel, including all gathered non-sensory information.

• Adopts a semantic reasoning engine as a decision support system, supporting the decision of a customs officer to stop and open an item or let it pass.

• Gathers all knowledge/non-knowledge (cases where the system succeeds/fails) to a knowledge database for further use, comparisons, advice, evaluation, re-evaluation, re-training and re-adjusting of the semantic reasoning engine rules.

• Properly fuses multimodal sensory information to provide annotated high-resolution tensor-structured (3D/4D) multisensory image data and segmented/isolated regions-of-interest in the image data to visualize, pinpoint and characterize the whole letter/parcel, as well as possible illicit goods and threats inside the letter/parcel, in an unsupervised

manner. Information fusion, unsupervised annotation and segmentation are carried out by AI-empowered algorithmic tools grounded on Machine/Deep Learning architectures. An example is provided in Figure 2.

• Incorporates visual/sound signaling when illicit goods and threats are detected.

IV. EXPERIMENTAL RESULTS

In this section simulation results of the proposed security screening architecture are provided. In particular, Western Europe is among the largest markets of cross-border postal and express services with 3.2 billion items per year, a volume that increases with the years [3], [5]. Full examination of these flows means: (a) manual intervention, which significantly impedes these flows and heavily intrudes into privacy, (b) extremely high levels of human effort. In particular customs and LEAs authorities' officers have to spend about 53 million hours per year (assuming a 60-seconds examination), or 6,625,000 day-labors. To do so, about 25,500 employees should be hired, only to examine these flows.

On the other hand, the National Institute for Occupational Safety and Health conducted a study to measure the amount of radiation potentially received by materials imaged from

various screening technologies. Sixty-seven dosimeters were intentionally irradiated in groups of three, from one to 10 times, in "checked baggage" and traditional "carry-on baggage" machines to characterize the response of the dosimeters when directly exposed to the beam. Data from dosimeter badges passed through a traditional carry-on baggage machine showed from none to very small amounts of measurable radiation. The study notes that the highest dose measured on a dosimeter that was passed 36 times through the machine was 4 mrem or 0.04 millisievert (mSv). Dosimeters that were passed through the "checked baggage" system that randomly activates the x ray had highly variable doses. If the dosimeters were near the area randomly selected by the software to activate the x-ray source, a higher dose would be measured. The average dose, after 10 passes through this type of system was about 28 mrem per scan (0.28 mSv per scan) [34]. Dosimeters that were passed through the type of "checked baggage" system that stayed active for the entire screening process had an average dose of 156 mrem per scan (1.56 mSv) per scan.

On the other hand, one rem carries with it a 0.05% chance of eventually developing cancer. Doses greater than 100 rem, received over a short time period are likely to cause acute radiation syndrome (ARS), possibly leading to death within weeks if left untreated. Additionally, the U.S. Nuclear Regulatory Commission (NRC) has established standards that allow exposures of up to 5,000 mrem per year for those who work with and around radioactive material [35].
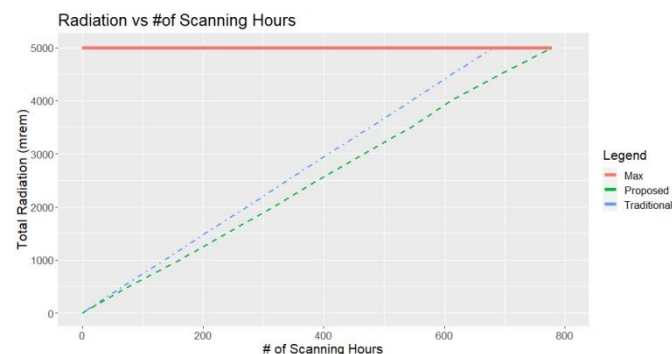

**Figure 3**: Estimated number of scanned items versus total radiation

Based on the aforementioned sources, it is estimated that: (a) if the traditional screening systems stay active for the entire screening process, the customs officer will receive 1/1,000 of the dose or 0.156 mrem per scan. Thus, in about 32,000 entire screening processes, the customs officer reaches the exposure limit, (b) if the traditional screening systems stay active for a part of the screening process, the customs officer will receive 1/1,000 of the dose or 0.028 mrem per scan. Thus, in about 180,000 partial screening processes, the customs officer reaches the exposure limit. Furthermore, if we assume that in real world screening only 1 out of 10 sessions is an entire screening process and the rest 9 are partial screening processes, then in about 123,000 screening processes $\left(\frac{entire\ screening}{partial\ screening} = \frac{1}{10}\right)$, the customs officer reaches

the exposure limit. If each screening process lasts 20 seconds on average, then the customs officer reaches the exposure limit in 681 hours or 85 full working days (8 hours per day). Actually, customs officers do not spend all 8 working hours daily on screening equipment, but they work in various positions.

In order to confront the aforementioned problems, the proposed architecture incorporates non-ionizing radiation. In particular, when screening a letter/parcel, initially the terahertz, CBRN, artificial robot-nose, magnetometer, acoustic and weight and pressure sensors monitor the contents of the letter/parcel in a partial screening process. The spectral signatures of the monitored content (of the partial screening process) are compared to the "Spectral Signatures Dictionary of Illicit Goods and Threats". If the system's assessment of detecting illicit goods and threats is 100% negative, then the X-rays sensor is not incorporated and thus ionizing radiation is avoided. It is anticipated that in 10 – 15% of the total number of letters, X-rays will not be incorporated.

Figure 4: Estimated scanning hours versus total radiation
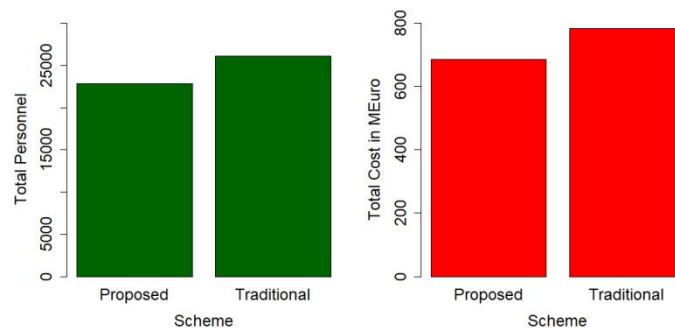
Figure 5: Estimated total personnel and total cost in million Euros

Based on the aforementioned reasonable assumptions, in Figures 3, 4 and 5, the proposed architecture is compared to the existing state-of-art security screening equipment. More specifically in Figure 3 the estimated number of scanned items versus the total radiation exposure is presented. The baseline is 5,000 mrem, marking the maximum allowed exposure. It is estimated that by using the proposed scheme, a customs officer can examine 139,994 letters/parcels, while by using traditional scanning equipment a customs officer can examine 122,549 letters/parcels. The overall difference is 17,445 more items for the proposed scheme. In Figure 4 the number of working hours versus the total radiation exposure is presented. Again the

baseline is 5,000 mrem. It is estimated that by using the proposed scheme, a customs officer can examine letters/parcels for 778 hours, while by using traditional scanning equipment a customs officer can examine letters/parcels for 681 hours until reaching the maximum allowed radiation exposure. The overall difference is 107 more hours for the proposed scheme. Finally in Figure 5 the estimated total personnel and the estimated total cost for the personnel are presented. In particular and by assuming that each customs officer scans letters/parcels for 8 hours/day, the number of required customs officers for traditional schemes is 26,112 to examine the 3.2 billion items (letters/parcels) per year, passing the EU borders. The proposed scheme achieves a reduction of 3,254 customs officers, requiring 22,858 customs officers. This leads to a significant cost reduction (right side of Figure 5). If the cost (salary + social insurance) of European customs officers is 30,000 Euro per year on average, then traditional schemes require 783.3 million Euro per year, while the proposed scheme requires 685.7 million or 97.6 million less.

V. Conclusion

This paper presents a highly innovative security screening architecture, well-beyond the state-of–art. The proposed architecture monitors every letter/parcel by incorporating various sensors (terahertz/X-ray, CBNR, artificial robot-noses, magnetometers, acoustic sensors and weight/pressure sensors), while introducing the "Spectral Signatures Dictionary of Illicit Goods and Threats". The proposed solution also gathers, analyzes and models information from various other resources, and forwards knowledge to an AI-based knowledge infrastructure. The proposed architecture aims at bridging the present gap of traditional security screening equipment, which cannot detect all kinds of illicit goods.

Initial experimental simulation results show the significant potential of the proposed architecture, which may increase the number of scanned items, increase the scanning hours, decrease the required personnel and consequently decrease the personnel cost. In our future research, we aim at attracting funding and implementing the proposed architecture, so that to perform real world experiments and compare the proposed prototype to existing security screening equipment.

References

[1] Illicit Trade Forum. 2020. 3rd to 4th February 2020: Room XXVI, Palais des Nations, Geneva. Available online: https://unctad.org/system/files/non-official-document/DITC2020_BackgroundNote_UNCTAD%20Illicit%20Trade%20Forum_en.pdf

[2] EUIPO. 2019. The European Observatory on Infringements of Intellectual Property (EUIPO) with Organisation for Economic Co-operation and Development (OECD). Global Trade in Fakes: A Worrying Threat. Available online: https://euipo.europa.eu/ohimportal/en/web/observatory/report-on-trade-in-fakes

[3] Illicit Trade Forum, 2021. Definition of Illicit Trade and Illicit Financial Flows. University of Groningen, Netherlands. Available online: https://illicittrade.org/research-overview

[4] World Drug Report. 2019. United Nations publication, Sales No. E.19.XI.8. Available online: https://wdr.unodc.org/wdr2019/prelaunch/WDR19_Booklet_2_DRUG_DEMAND.pdf

[5] Universal Postal Union (UPU). 2010. "Market Research on International Letters and Lightweight Parcels and Express Mail Service Items. BERNE, Switzerland. Available online: https://www.upu.int/UPU/media/upu/publications/reportStrategyConferenceMarketResearchEn.pdf

[6] National Press Release, Tuesday, January 26, 2021. Available online: https://www.google.com/url?q=https://www.tsa.gov/news/press/releases/2021/01/26/tsa-firearm-catch-rate-doubles-2020-highest-agencys-19-year-history&sa=D&source=docs&ust=1636737286857000&usg=AOvVaw1TVKwf3fZx6vs5TCWFIBx9

[7] S. H. Jacobson, "Using Risk-Based Security to Quantify the Number of Firearms Missed at Airport Security Checkpoints," INFORMS Journal on Applied Analytics, Vol. 50, No. 3, p.p. 190-196, 2020.

[8] https://cordis.europa.eu/project/id/285203, SNIFFER

[9] Delivering Justice to Opioid Dealers. 2021. Chicago, USA. Available online: https://www.uspis.gov/the-opioid-epidemic

[10] https://cordis.europa.eu/project/id/312496, TERASCREEN

[11] https://cordis.europa.eu/project/id/312998, ACXIS

[12] https://cordis.europa.eu/project/id/653323, C-BORD

[13] https://cordis.europa.eu/project/id/833787, BorderSense

[14] https://cordis.europa.eu/project/id/883424, ENTRANCE

[15] https://cordis.europa.eu/project/id/101020100, MULTISCAN 3D

[16] https://cordis.europa.eu/project/id/101021812, SilentBorder

[17] J. Skorupski and P. Uchronski, "Evaluation of the effectiveness of an airport passenger and baggage security screening system," J. Air Transp. Manag., vol. 66, 2018, pp. 53–64.

[18] Y. F. A. Gaus, N. Bhowmik, S. Akçay, P. M. Guillen-Garcia, J. W. Barker, T. P. Breckon, "Evaluation of a Dual Convolutional Neural Network Architecture for Object-wise Anomaly Detection in Cluttered X-ray Security Imagery," in: International Joint Conference on Neural Networks (IJCNN), IEEE, 2019.

[19] B. Isaac-Medina, C. Willcocks, T. Breckon, "Multi-view Object Detection Using Epipolar Constraints within Cluttered X-ray Security Imagery," in: Proceedings of the International Conference on Pattern Recognition (ICPR), IEEE, 2020

[20] Y. Gaus, N. Bhowmik, S. Akcay, T. Breckon, "Evaluating the Transferability and Adversarial Discrimination of Convolutional Neural Networks for Threat Object Detection and Classification within X-Ray Security Imagery," in: Procedings of the International Conference on Machine Learning Applications (ICMLA), IEEE, 2019.

[21] T. Hassan, S. Akcay, M. Bennamoun, S. Khan, N. Werghi, "Trainable Structure Tensors for Autonomous Baggage Threat Detection Under Extreme Occlusion," in: Asian Conference on Computer Vision, ACCV, Springer, 2020.

[22] L. D. Griffin, M. Caldwell, J. T. A. Andrews, H. Bohler, "Unexpected Item in the Bagging Area: Anomaly Detection in X-Ray Security Images," IEEE Transactions on Information Forensics and Security 14 (2019) 1539–1553.

[23] Y. Wei, R. Tao, Z. Wu, Y. Ma, L. Zhang, X. Liu, "Occluded Prohibited Items Detection: An X-ray Security Inspection Benchmark and De-occlusion Attention Module," in: Proceedings of the 28th ACM International Conference on Multimedia, ACM, New York, NY, USA, 2020, pp. 138–146.

[24] Dhiraj, D. K. Jain, "An Evaluation Of Deep Learning-Based Object Detection Strategies For Threat Object Detection In Baggage Security Imagery," Pattern Recognition Letters 120 (2019) 112–119.

[25] T. Morris, T. Chien, E. Goodman, "Convolutional Neural Networks for Automatic Threat Detection in Security X-Ray Images," in: International Conference on Machine Learning and Applications (ICMLA), IEEE, 2018, pp. 285–292.

[26] K. Liang, C. Gregory, S. O. Diallo, K. Roe, G. Heilmann, L. Carin, D. Carlson, G. Spell, J. Sigman, "Automatic Threat Recognition of

Prohibited Items at Aviation Checkpoint with X-ray Imaging: A Deep Learning Approach," in: A. Ashok, M. A. Neifeld, M. E. Gehm, J. A. Greenberg (Eds.), Anomaly Detection and Imaging with X-Rays (ADIX) III, SPIE, 2018, p. 2.

[27] J. Yang, Z. Zhao, H. Zhang, Y. Shi, "Data Augmentation for X-Ray Prohibited Item Images Using Generative Adversarial Networks," IEEE Access, Vol.7, p.p. Page(s): 28894 – 28902, 2019.

[28] N. Bhowmik, Y. F. A. Gaus, S. Akcay, J. W. Barker, T. P. Breckon, "On the Impact of Object and Sub-component Level Segmentation Strategies for Supervised Anomaly Detection within X-ray Security Imagery," in: Procedings of the International Conference on Machine Learning Applications (ICMLA), IEEE, 2019.

[29] S. Akçay, T. Breckon, "Towards automatic threat detection: a survey of advances of deep learning within X-ray security imaging," Preprint arXiv:2001.01293, 2020.

[30] M. Baştan, "Multi-view object detection in dual-energy X-ray images," Machine Vision and Applications, Vol. 26, p.p. 1045–1060, 2015. https://doi.org/10.1007/s00138-015-0706-x

[31] H. E. Martz, C. M. Logan, D. J. Schneberk, and P. J. Shull, "X-Ray Imaging: Fundamentals, Industrial Techniques and Applications," Boca Raton, FL, USA: CRC Press, 2017.

[32] V. Rebuffel, M. Tartare, A. Brambilla, V. Moulin, and L. Verger, "Multienergy X-ray techniques for NDT: A new challenge," in Proc. Eur. Conf. Non-Destructive Test. (ECND), Prague, Czech Republic, Sep. 2014, pp. 1-10.

[33] D. Karakaya, O. Ulucan, M. Turkan, "Electronic Nose and Its Applications: A Survey," International Journal of Automation and Computing, Vol. 17, No. 2, p.p. 179–209, 2020. https://doi.org/10.1007/s11633-019-1212-9

[34] C. Achutan, C. Mueller, "Evaluation of Radiation Exposure to TSA Baggage Screeners," Health Hazard Evaluation Report, HETA #2003-0206-3067, Transportation Security Administration, Washington, DC, September 2008, https://www.cdc.gov/niosh/hhe/reports/pdfs/2003-0206-3067.pdf

[35] ICRP Publication 103. The 2007 Recommendations of the International Commission on Radiological Protection. https://www.icrp.org/publication.asp?id=ICRP%20Publication%20103. Retrieved 23 November 2021.