IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 15 June 2022, accepted 30 June 2022, date of publication 11 July 2022, date of current version 26 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3189674

APPLIED RESEARCH

Real Time Threat Assessment of Truck Cargos Carrying Dangerous Goods for Preventing Terrorism Attacks on Neighboring Critical Infrastructures

ATHANASIOS SKRAPARLIS[1,2], KLIMIS S. NTALIANIS[2], AND NIKOS E. MASTORAKIS[3], (Senior Member, IEEE)

[1]SymBioLogic Ltd.–Senior Security Expert, 11257 Athens, Greece
[2]Department of Business Administration, University of West Attica, Egaleo, 12243 Athens, Greece
[3]Industrial Engineering Department, Technical University of Sofia, 1000 Sofia, Bulgaria

Corresponding author: Athanasios Skraparlis (askraparlis@uniwa.gr)

This work was supported in part by the Interbit Research, and in part by the European Union under Grant 2021-1-EL01-KA220-VET-000028082.

ABSTRACT Critical infrastructures are assets of invaluable importance, essential for the whole world. Since they serve core functions of our societies, they often become targets of terrorists. Many critical infrastructures are vulnerable, due to their short distance from public roads and in the past years, several vehicle-bomb incidents have been recorded. This paper focuses on the case of truck-bombs, which can either be created from scratch, or terrorists can easily hijack truck cargos carrying dangerous goods and turn them into bombs. The latter are typically called ADR truck cargos, according to the respective agreement of the 30th of September 1957, concerning the international carriage of dangerous goods by road. The proposed scheme performs threat assessment of neighboring critical infrastructures, aiming at preventing explosions of truck-bombs. To do so, each crucial point of a critical infrastructure is initially associated with a level of importance. Next, three scenarios are analyzed: (a) single-attack single-infrastructure, (b) multiple-attack single-infrastructure, and (c) multiple-attack multiple-infrastructure. To reduce computational complexity, the third scenario is simplified to one of the two other scenarios, by introducing a novel fusion technique for the non-overlapping segments of the Voronoi tessellation. By this way, an area of threat assessment is estimated for each critical infrastructure. Then, the threat level is assessed in real time by an innovative algorithm, which: (a) estimates the impact of multiple consecutive explosions, (b) uses five adapted threat levels and (c) introduces multiple criteria and minimum classification conditions based on the number of crucial points and their levels of importance. Extensive real world experimental results and comparisons to other works, exhibit the pros and cons of the proposed scheme. In particular, compared to related work, the proposed scheme improves: (a) computational time by 74.5%, (b) threat notification time by 86.9% and (c) estimated surveillance cost by 98.6%.

INDEX TERMS ADR, critical infrastructure, multiple explosions, real time, terrorism attacks, threat assessment, truck-bomb, Voronoi tessellation.

I. INTRODUCTION

Even though several human constructions demand huge efforts, time and money, they can be destroyed with very little effort, at the speed of the light and for an insignificant fragment of the cost of construction. For example, an Airbus A380/Boeing 747 costs approximately 400 million Euro and its construction takes several months, but its destruction just needs either an accident or 200 Euro (100 liters of petrol to set fire) and less than 2 hours. Human history is full of

The associate editor coordinating the review of this manuscript and approving it for publication was Alba Amato.

devastating accidents such as the Wanggongchang explosion (30 May 1626) in Beijing, China which destroyed part of the city and killed 20,000 people [1] or the Brescia explosion (18 August 1769) in Italy, which destroyed one-sixth of the city and killed 3,000 people [2]. On the other hand, acts of terrorism always happened. Many people remember the 11th September 2001 attacks in New York City, Washington, DC and Shanksville, PA, USA, which killed 2,996 and injured about 25,000 people, while they also caused at least 10 billion Euro damage in infrastructure and property [3]. Unfortunately, acts of terrorism happen very often.

The current work examines truck-bombs, which are commonly used as weapons by terrorists to kill people near the blast site or to damage infrastructures. Truck-bombs carry large amounts of explosives without attracting suspicion. For example, in the Oklahoma City bombing (19 April 1995), USA, more than 3,200 kg of ammonium nitrate fertilizer and fuel oil (ANFO) have been used, killing 168 people, 19 of whom were children, injuring more than 680 others, destroying one third of the Alfred P. Murrah Federal Building which had to be demolished, damaging 324 neighboring buildings within a 16-block radius and 86 cars and causing about 600 million Euro damage [4].

Similar attacks can target any critical infrastructure (*CI*) such as dams, airports, ports, power plants, refineries, bridges, telecommunication infrastructures, water supply networks and more, which have been built to be cost-effective, with little concern for belligerent attacks [5]. Moreover, multiple attacks could be organized, where the target is hit by several truck-bombs. To do so, terrorists can either create truck-bombs, or easily hijack ADR cargos and turn them into extremely dangerous moving bombs. More specifically ADR, formally the Agreement of 30 September 1957 concerning the International Carriage of Dangerous Goods by Road, is a 1957 United Nations treaty that governs transport of hazardous materials. In case of ADR cargos, truck drivers usually cannot confront hijacking events and the cargos are not followed by guards. Furthermore, in case of long distances, truck drivers stop on rest areas, which may become weak links of a route's security chain.

This paper aims at performing threat assessment of neighboring *CIs*, in order to prevent ADR truck-based terrorism attacks. To do so, crucial points of each *CI* are initially detected, and each crucial point is associated with a level of importance. Next, the following three scenarios are analyzed: (a) single-attack single-infrastructure, where a single ADR truck explodes near a single *CI*, (b) multiple-attack single-infrastructure, where multiple ADR trucks explode near a single *CI* and (c) multiple-attack multiple-infrastructure, where multiple ADR trucks explode near neighboring multiple *CIs*. Reduction of the computational complexity is achieved by simplifying and reducing the third scenario (scenario (c)) to one of the two previous scenarios ((a) and (b)). This is accomplished by proposing *CI*-based fusion of the non-overlapping segments of the Voronoi tessellation. By this way, an area of threat assessment (*ATA*) is estimated for each *CI*. Then, the threat level is assessed within the *ATA* of each *CI*, by an innovative algorithm which: (a) can estimate the impact of multiple explosions (overpressure and positive incident impulse), (b) uses five adapted threat levels, according to the proposal of the Joint Terrorism Analysis Centre & Security Service of MI5 [6] and (c) introduces multiple criteria and minimum classification conditions based on the number of crucial points and their levels of importance. After initialization (Voronoi tessellation and estimation of *ATAs*), the proposed scheme performs in real time. Experimental results and comparisons to other works on real world settings, exhibit the strengths and shortages of the proposed scheme.

To summarize, the major contributions of this paper are:

- Proposal of *CI*-based fusion of the non-overlapping segments of the Voronoi tessellation, leading to estimation of an *ATA* for each *CI*.
- Proposal of a real time innovative algorithm to assess the threat of each *CI*, which considers the impact of multiple explosions, uses five adapted threat levels and incorporates multiple criteria and classification conditions based on the number of crucial points and their levels of importance.
- Aggregation of the impact of multiple consecutive explosions, in case of multiple attacks.
- Examination of neighboring *CIs*, possibly connected through the road network.

Some more contributions include:

- Adaptation of the threat levels proposed by [6], to the problem of threat assessment of *CIs*, considering truck-bombs (introduction of specific levels of threat).
- Proposal of a framework for threat assessment of different explosive substances.
- Extensive experimentation on real world settings.

The rest of the paper is structured as follows: Section 2 provides necessary background information. Section 3 discusses related work. In Section 4 the proposed scheme is fully described, while real world experimental results are exhibited in Section 5. Finally, Section 6 concludes this paper, pointing out some future research directions.

II. BACKGROUND

A. DEFINITIONS

Useful terms and required information are provided next:

- Atmospheric pressure: also known as barometric pressure, is the pressure within the atmosphere of Earth. The standard atmosphere (atm) is a unit of pressure equal to 14.696 psi. The Earth's atmospheric pressure at sea level is approximately 1 atm. On average, a column of air with a cross-sectional area of 1 cm2 measured from mean sea level to the top of Earth's atmosphere, has a mass of about 1.03 kilogram and exerts a force or "weight" of 1.033 kg/cm2.
- Pounds per square inch gauge (psig) or Gauge Pressure: is typically the pressure difference between a supply tank and the outside air; it ignores atmospheric pressure.

TABLE 1. Expected damage to infrastructure in relation to overpressure (psig).

Overpressure* (psig)	Expected Damage
0.04	Loud noise (143 db); sonic boom glass failure
0.15	Typical pressure for glass failure
0.40	Limited minor structural damage
0.50-1.0	Windows usually shattered; some window frame damage
0.70	Minor damage to house structures
1.0	Partial demolition of houses; made uninhabitable
1.0-2.0	Corrugated metal panels fail and buckle. Housing wood panels blown in
1.0-8.0	Range for slight to serious laceration injuries from flying glass and other missiles
2.0	Partial collapse of walls and roofs of houses
2.0-3.0	Non-reinforced concrete or cinder block walls shattered
2.4-12.2	Range for 1-90% eardrum rupture among exposed populations
2.5	50% destruction of home brickwork
3.0	Steel frame buildings distorted and pulled away from foundation
5.0	Wooden utility poles snapped
5.0-7.0	Nearly complete destruction of houses
7.0	Loaded train cars overturned
9.0	Loaded train box cars demolished
10.0	Probable total building destruction
14.5-29.0	Range for 1-99% fatalities among exposed populations due to direct blast effects

*These are peak pressures formed in excess of normal atmospheric pressure by blast and shock waves.

To convert psi to psig, atmospheric pressure is added to the psig value.

- Overpressure (or blast overpressure): is the pressure caused by a shock wave over and above normal atmospheric pressure. In case of blasts, overpressure is equal to gauge pressure. Table 1 [7] provides the expected damage to infrastructures in relation to overpressure.
- ADR: formally the Agreement of 30 September 1957 concerning the International Carriage of Dangerous Goods by Road, is a 1957 United Nations treaty that governs transnational transport of hazardous materials. Thus, ADR truck is defined as a truck that carries dangerous goods such as: explosives, gases, flammable liquids, flammable solids, spontaneous combustibles, oxidizers, organic peroxides, toxic substances, infectious substances, radioactive materials, corrosives etc.

B. SUBSTANCES' RELATIVE EFFECTIVENESS FACTORS

Each substance S_i, $i = 1, \ldots, n$, has a different degree of danger per unit. Here it should be stressed that different substances may encapsulate different types of dangers, expressed by demolition power, toxicity, radioactivity, carcinogenesis, mutagenesis, teratogenesis etc. This paper focuses on the demolition power of each substance, for two reasons: (a) vehicle bombing incidents of the past, mainly fall into the demolition category and (b) *CIs* are more vulnerable to destruction/demolition attacks.

TABLE 2. $RE(S_i^u)$ of different substances.

Substance Name	$RE(S_i^u)$
Trinitrotoluene (TNT)	1
Propane (in a stoichiometric mixture with oxygen, based on the peak hydrostatic overpressure)	0.28
Ammonium nitrate	0.32
Hexamine dinitrate	0.6
Dinitrobenzene	0.6
ANFO	0.74
Nitrourea	1.05
Nitrocellulose	1.10
Picric acid	1.17
Trinitrobenzene	1.2
Nitroglycerin	1.54
Hexogen	1.6
Octanitrocubane	2.38

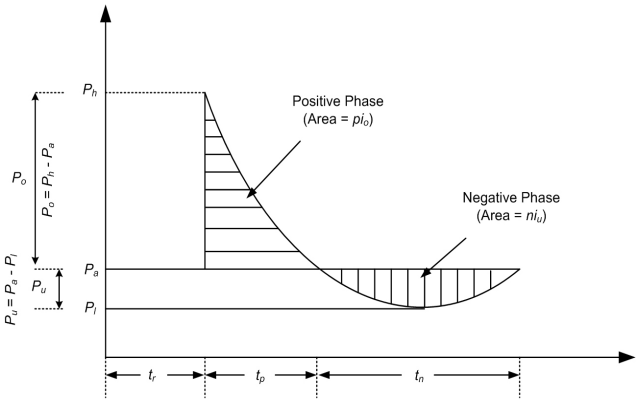

FIGURE 1. Ideal blast waveform in the air.

Let us denote by $RE(S_i^u)$ the relative effectiveness factor of one unit of S_i. The relative effectiveness factor relates a substance's demolition power to that of TNT, in units of the TNT equivalent/kg (TNTe/kg) and thus it expresses the degree of demolition danger of each S_i. Table 2 [8]–[11] provides the $RE(S_i^u)$ of different substances.

According to Table 2 and to give an example of how $RE(S_i^u)$ is used, if 1 kg of TNT is required to demolish a wall, then the same job can be done by 0.42 kg (1.0/2.38) of octanitrocubane.

C. DESCRIPTION OF BLAST WAVES

When an explosive is detonated in the free air, hot gases at extremely high pressure are produced, which cause a high velocity shock wave. Figure 1 visualizes the Friedlander equation [12], which describes the pressure-time waveform of an ideal explosion at distance R from the explosion's center. P_a is the atmospheric pressure. The

waveform can be divided into positive and negative phases. In general, the positive phase is more dangerous for critical infrastructures, due to large overpressures and concentrated impulses. The positive phase lasts t_p, while t_r is the time of arrival of the blast wave and t_n is the duration of the negative phase. The area under the pressure-time waveform during the positive phase is the positive incident impulse (pi_o). Blast pressure variation is the difference of the peak overpressure (P_o) and peak underpressure or negative pressure (P_u).

For calculating the positive blast pressure, Flynn introduced the linear decaying pressure equation [12]:

$$P(t) = P_a + P_o \frac{(t_p - t)}{t_p}, \quad 0 < t \leq t_p \tag{1}$$

while Ethridge [12] proposed a more accurate form:

$$P(t) = P_a + P_o e^{-ct} \tag{2}$$

where c is the decay rate of the wave and t is measured from the time of arrival (t_r).

Additionally, the most common blast scaling law, namely the Hopkinson-Cranz law [13], [14] defines the scaled distance or proximity factor SD:

$$SD = \frac{R}{\sqrt[3]{M}} \tag{3}$$

where R denotes the distance in meters from the center of a spherical charge, while M represents the charge mass in kilograms of TNT.

1) INCIDENT BLAST WAVE

After an explosion, the blast load can lead not only to disproportionate structural failure of *CIs* but also to tremendous casualties (dead and injured). During the second half of the 20th century, a large number of experimental and analytical works studied the nature of blast waves and structural response [15]–[19]. These works led to several empirical relations to predict blast overpressure based on the analysis of large sets of experimental data at different scaled distances and charge sizes. Even though most of them have focused on small ranges, this paper incorporates Kinney and Graham's equation [15], which does not have limits on the valid range:

$$P_o = P_a \frac{808\left[1+\left(\frac{SD}{4.5}\right)^2\right]}{\sqrt{\left[1+\left(\frac{SD}{0.048}\right)^2\right]}\cdot\sqrt{\left[1+\left(\frac{SD}{0.32}\right)^2\right]}\cdot\sqrt{\left[1+\left(\frac{SD}{1.35}\right)^2\right]}} \tag{4}$$

or in terms of distance and TNT mass (5), as shown at the bottom of the next page.

Based on Eq. (5) and for a specific quantity of TNT equivalent (M), the overpressure (P_o) of a blast wave can be calculated for any distance R from the blast's location.

III. RELATED WORK

The problem of *CIs'* threat assessment and protection has been studied in the past. In particular, in [20], the protection of *CIs* against a malicious attacker is modeled as a simultaneous game and the Nash equilibrium solution is imposed. In [21] the most prominent threats and attacks against Industrial Control Systems and critical infrastructures, are described. In [22] Digital Twins to secure *CIs* are developed, which are built using real-time, high fidelity replicas of Programming Logic Controllers. Denial of Service attacks are examined. In [23] a model trained using deep learning is proposed to evaluate EEG signals and detect insider threats. The algorithm classifies different mental states based on four category risk matrices. The work in [24] documents and analyzes cyber-attacks at the oil and gas sector. It also builds a vulnerability taxonomy and connects each vulnerability to the respective attack paths. In [25] a trilevel optimization model is proposed that integrates protection, restoration, and adaptive flow redistribution. Complexity is minimized using an evolutionary algorithm. In [26] a defender-attacker-defender model is proposed that analyzes the potential impacts of intelligent attacks and worst-case disruptions on the U.S. air transportation network. The effects of intermodal connections on the resilience of the air network are also considered through a hypothetical bus network. In [27], the security of smart city service infrastructure is modelled at a higher level of abstraction. Multiple tiers of defense at component/system level, and security operation center are introduced, while for a given component vulnerability vector, the model assesses key security parameters. In [28] the impact of node placement and clustering on LWSN network lifetime is analyzed. Existing node placement and clustering schemes are classified for LWSN and various topologies for disparate applications are introduced. In [29] systemic integration of granular computing (GrC) and resilience analysis for CIs is performed. The paper also considers that adverse events suddenly occur and evolve rapidly, giving little time to react. In [30] visual surveillance data, channel state information from Wi-Fi signals for human-presence detection, and ICS sensor data from the utility are analyzed for protecting critical water infrastructures. In [31] wired signal distinct native attribute finger-printing is investigated as a non-intrusive physical-based security augmentation. Results are based on remote transducer differential pressure transmitter devices, where time domain and slope-based FSK fingerprints' analysis is incorporated. In [32] an automated attack generation method is proposed that can produce detailed, scalable, and consistent attack trees. The paper also discusses identification of the adversarial strategies. In [33] six existing threat assessment frameworks are examined. The paper argues that the complexities associated with modern *CIs*, make existing methods insufficient to assess systems security risks exposure. In [34] a Unified Modelling Language profile is proposed that enables the modelling and security specification for *CIs*. Security assessment is carried out through survivability analysis and stochastic

analysis, carried out with Generalized Stochastic Petri nets is discussed. Other interesting works include [35]–[47], which cover different aspects of *CIs*' threat assessment and protection.

Even though very interesting, most aforementioned works are not tested on real world settings and do not provide specific levels of threat. This paper builds on previous extensive experience on surveillance, authentication, illicit goods detection and location-based action analysis [48]–[53], to perform threat assessment of neighboring *CIs*. Three scenarios are analyzed, multiple explosions are considered, a *CI*-based fusion algorithm is proposed for non-overlapping segments of the Voronoi tessellation and a real time innovative algorithm to assess the specific threat of each *CI* is presented. Strengths and weaknesses are exhibited and compared to other schemes through an extensive experimentation phase on real world settings.

IV. THE PROPOSED THREAT ASSESSMENT FRAMEWORK

A. FRAMEWORK OVERVIEW

This paper focuses on ADR trucks, approaching *CIs*, as it can be seen in Figure 2. If ADR trucks are hijacked by terrorists or other extremists, they can be used as truck-bombs that can cause serious damage to *CIs*. Even an accident (non-terrorism event) can lead to devastating results.

In this subsection, definitions cover all required concepts, objects and actors of the proposed framework. Towards this direction, let us define by $CI_k^{cp_b}$, $k = 1, \ldots, l$, $b = 1, \ldots, q$, the kth *CI* under anti-terrorism/security intelligent surveillance, which has b crucial points (cp_b). For example, an airport (transportation *CI*) has several crucial points that can be stricken by terrorists. These crucial points include fuel tanks, the flight control tower, airstrips etc.

Let $ADR_{r_j \leq \rho}^{cp_b}$ be the jth ADR truck, $j = 1, \ldots, m$, which is located within a radius ρ from crucial point b of a *CI*. More specifically r_j is the distance of $ADR_j^{cp_b}$ from crucial point b of a *CI* under surveillance. In this case, an ADR truck may be in the vicinity of more than one crucial points. Here it should be mentioned that a different r_j (e.g. $r_j^{cp_b}$ for each crucial point b of any individual CI_k) could be used, according to the importance of each point, but for simplicity reasons and without loss of generality, it is avoided in this paper.

Let us also denote by $IPC_k^{cp_b}$, $k = 1, \ldots, l$, $b = 1, \ldots, q$, the level of importance (*IPC*) of the bth crucial point of the kth *CI*. Each cp_b may have a different level of importance. For example, in case of a petroleum refinery, the desalter unit (which washes out salt from the crude oil before it enters the atmospheric distillation unit) has a high level of importance. In the same example, a gasoline storage tank with capacity of 70,000 m^3 has an extremely high level of importance, since if it catches fire, it may destroy the whole refinery. In this paper and since the focus is on *CIs*, three levels of importance are considered for *IPC*: ''high'', ''very high'', ''extremely high''.

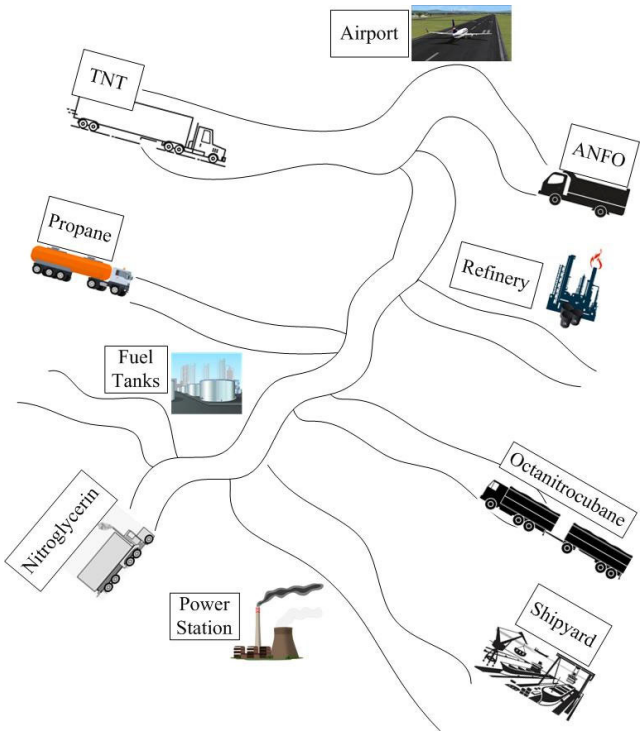

FIGURE 2. Overview of the scheme: ADR trucks approaching neighboring *CIs*, through the road network.

B. SINGLE-ATTACK SINGLE-INFRASTRUCTURE THREAT ASSESSMENT

In case of single-attack single-infrastructure threat assessment, it is assumed that a single ADR truck explodes near a single *CI*. In this case the overpressure (P_o) of the blast wave can be calculated by Eq. (5) and the positive incident impulse (pi_o), expressing the overall shock that cp_b of *CI* receives, can be calculated by:

$$pi_o = \int_{t_r}^{t_r} (P(t) - P_a)\, dt \tag{6}$$

and by using Eq. (2):

$$pi_o = P_o \int_{t_r}^{t_r} e^{-ct} dt = P_O \cdot \left(\frac{e^{-c \cdot t_r} - e^{-c \cdot (t_r + t_p)}}{c} \right)$$

$$P_o = P_a \frac{808 \left[1 + \left(\frac{R}{4.5 \sqrt[3]{M}} \right)^2 \right]}{\sqrt{\left[1 + \left(\frac{R}{0.048 \sqrt[3]{M}} \right)^2 \right]} \cdot \sqrt{\left[1 + \left(\frac{R}{0.32 \sqrt[3]{M}} \right)^2 \right]} \cdot \sqrt{\left[1 + \left(\frac{R}{1.35 \sqrt[3]{M}} \right)^2 \right]}} \tag{5}$$

TABLE 3. MI5's adapted *LoT* for *CIs*.

Level #	LoT	Description
1	Low	Explosion is likely to produce no malfunction to the *CI*
2	Moderate	Explosion is likely to produce non-significant malfunction to the *CI*
3	Substantial	Explosion is likely to produce significant malfunction to the *CI*
4	Severe	Explosion is likely to produce severe malfunction to the *CI*
5	Critical	Explosion is likely to produce critical malfunction to the *CI*

$$= = P_O \cdot \frac{e^{c\cdot(t_r+t_p)} - e^{c\cdot t_r}}{c \cdot e^{c\cdot(t_r+t_p)} \cdot e^{c\cdot t_r}} \tag{7}$$

Equations (5) and (7) are calculated for all cp_b's, $b = 1, \ldots, q$, of the *CI*, since in case of an explosion more than one crucial points may be affected. In order to assess the threat of the *CI*, the MI5's [6] five levels of threat (*LoT*) are adapted. These five levels can be seen in Table 3:

In order to assess the *LoT* of the *CI*, in this paper the following novel algorithm is introduced:

Algorithm 1 provides the minimum conditions to classify a threat as critical, severe or substantial. Towards this direction, overpressure thresholds T_1, T_2, T_3, T_4 ($T_2 > T_1 > T_3 > T_4$), positive incident impulse thresholds t_1, t_2, t_3, t_4 ($t_2 > t_1 > t_3 > t_4$) and cardinality thresholds T_{crd1}, T_{crd2}, T_{crd3} are incorporated such as: (a) T_2 / t_2 consider very high overpressure / positive incident impulse, (b) T_1 / t_1 consider high overpressure / positive incident impulse, (c) T_3 / t_3 consider significant overpressure / positive incident impulse and (d) T_4 / t_4 consider medium overpressure / positive incident impulse.

According to *Algorithm 1*, a critical threat is distinguished if the explosion: (a) possibly generates high overpressure or high positive incident impulse to at least one crucial point (cp_b), which has extremely high *IPC*, (b) possibly generates very high overpressure or very high positive incident impulse to at least one crucial point (cp_b), which has very high *IPC*, (c) possibly generates very high overpressure or very high positive incident impulse to at least T_{rcd1} crucial points, which have high *IPC*. Severe and substantial threats can be described in a similar manner. Additionally, since low and moderate *LoT* are not of specific concern and in order to reduce computational complexity, minimum conditions for classifying an event into low and moderate *LoT* are not included.

On the other hand, for analyzing time and space complexity of Algorithm 1, the big *O* (Bachmann–Landau or asymptotic) notation is used. In particular, regarding time complexity of Algorithm 1, let us assume that each computer operation takes approximately constant time, denoted as *ct*. Let us also assume that the worst-case scenario is considered,

Algorithm 1 Threat Assessment in Case of Single-Attack Single-Infrastructure

// ######## INITIALIZATION ########
Data: one *CI* ; one *ADR* ; all cp_b's of *CI*;
form set EH = $\{cp_b | IPC_k^{cp_b} ==$ "extremely high"$\}$ // set of extremely high level of importance points
form set $VH = \{cp_b | IPC_k^{cp_b} ==$ "very high"$\}$ // set of very high level of importance points
form set $H = \{cp_b | IPC_k^{cp_b} ==$ "high"$\}$ // set of high level of importance points
$CR_H = card(H)$ //cardinality of set H
for $b = 1 : q$ *//for all* $cp_b's$
estimate $P_O^{cp_b}$; //overpressure at each cp_b
form vector $\boldsymbol{OP_O} = [P_O^{cp_1}, P_O^{cp_2}, \ldots, P_O^{cp_q}]$;
estimate $pi_O^{cp_b}$; // positive incident impulse at each cp_b
form vector $\boldsymbol{Opi_O} = [pi_O^{cp_1}, pi_O^{cp_2}, \ldots, pi_O^{cp_q}]$;
end for ;

// ######## THREAT ASSESSMENT ########
$\forall P_o^{cp_b} \in \boldsymbol{OP_O}$; $\forall pi_o^{cp_b} \in \boldsymbol{Opi_O}$;
{
//Minimum conditions for critical level of threat ($LoT = 5$)
if $\exists cp_b$: $\{(P_O^{cp_b} > T_1$ OR $pi_o^{cp_b} > t_1)$ && $IPC_k^{cp_b} ==$ "extremely high"$)\}$ **then** $LoT =$ "5";
if $\exists cp_b$: $\{(P_O^{cp_b} > T_2$ OR $pi_o^{cp_b} > t_2)$ && $IPC_k^{cp_b} \geq$ "very high"$)\}$ **then** $LoT =$ "5";
if $\{\{\exists SH \subseteq H$: $(card(SH) \geq T_{crd1})\}$ && $(\forall cp_b \in SH$: $(P_O^{cp_b} > T_2$ OR $pi_o^{cp_b} > t_2)\}\}$ **then** $LoT =$ "5";
//Minimum conditions for severe level of threat ($LoT = 4$)
if $\exists cp_b$: $\{(T_1 > P_O^{cp_b} \geq T_3$ OR $t_1 > pi_o^{cp_b} \geq t_3)$ && $IPC_k^{cp_b} ==$ "extremely high"$)\}$ **then** $LoT =$ "4" ;
if $\exists cp_b$: $\{(T_2 > P_O^{cp_b} \geq T_1$ OR $t_2 > pi_o^{cp_b} \geq t_1)$ && $IPC_k^{cp_b} \geq$ "very high"$)\}$ **then** $LoT =$ "4" ;
if $\{\{\exists SH \subseteq H$: $(card(SH) \geq T_{crd2})\}$ && $(\forall cp_b \in SH$: $(P_O^{cp_b} > T_2$ OR $pi_o^{cp_b} > t_2)\}\}$ **then** $LoT =$ "4" ;
//Minimum conditions for substantial level of threat (LoT =3)
if $\exists cp_b$: $\{(T_3 > P_O^{cp_b} \geq T_4$ OR $t_3 > pi_o^{cp_b} \geq t_4)$ && $IPC_k^{cp_b} ==$ "extremely high"$)\}$ **then** $LoT =$ "3" ;
if $\exists cp_b$: $\{(T_1 > P_O^{cp_b} \geq T_3$ OR $t_1 > pi_o^{cp_b} \geq t_3)$ && $IPC_k^{cp_b} \geq$ "very high"$)\}$ **then** $LoT =$ "3" ;
if $\{\{\exists SH \subseteq H$: $(card(SH) \geq T_{crd3})\}$ && $(\forall cp_b \in SH$: $(T_2 > P_O^{cp_b} \geq T_1$ OR $t_2 > pi_o^{cp_b} \geq t_1)\}\}$ **then** $LoT =$ "3" ;
}

for $LoT < 3$ (in this case, all minimum conditions of Algorithm 1 are examined). Then the number of operations to be executed depends on the number of cp_b's (input length). The major operations for an input length N are: (a) $ct{*}N$ input operations (b) $ct{*}N$ operations to estimate overpressure (c) $ct{*}N$ operations to estimate positive incident impulse (d) $ct{*}N{*}logN$ to short the overpressure set (e) $ct{*}N{*}logN$ to short the positive incident impulse set and (f) $ct{*}N$ operations to check all minimum conditions. Hence the time complexity

of Algorithm 1 is $O(N{*}logN)$. So, if the number of cp_b's increases, the time of execution also increases in a non-linear way ($O(N{*}logN)$).

Regarding space complexity of Algorithm 1, let us assume that each element occupies a unit space of memory, denoted by sp. Then the occupied space also depends on the number of cp_b's (input length). In particular, for an input length N, the used memory space (for the major data to be stored) is: (a) $sp{*}N$ for forming sets EH, VH and H, (b) $sp{*}N$ for forming vector $\boldsymbol{OP_O}$, (c) $sp{*}N$ for forming vector $\boldsymbol{Opi_O}$, (d) $sp{*}N$ to short the overpressure set and (e) $sp{*}N$ to short the positive impulse set. Hence the space complexity of Algorithm 1 is $O(N)$. So, if the number of cp_b's increases, the required memory also increases in a linear way ($O(N)$).

C. MULTIPLE-ATTACK SINGLE-INFRASTRUCTURE THREAT ASSESSMENT

Before proceeding to full analysis of this scenario, it should be stressed that the scope of this paper is to establish the foundations for ADR threat assessment of critical infrastructures and not to examine case-based blast waves' interferences, reflections, angles of incidence etc. In any case, an individual threat assessment plan should be prepared for each CI, by taking into full consideration the specifics of the infrastructure (e.g. location, elevation level, crucial points, distance from road, obstacles etc.).

Now, in case of multiple-attack single-infrastructure threat assessment, it is assumed that multiple ADR trucks explode near a single CI. Explosions may happen at the same time, may have time overlap or may be successive. For simplicity reasons: (a) this paper focuses on successive explosions, where the next explosion occurs after the previous explosion is completed (typically after milliseconds) and (b) only the positive incident impulse of each explosion is estimated, which is typically much larger than the negative phase. Figure 3 visualizes the scenario of consecutive, non-overlapping explosions. In this case the overpressure (P_o) of each blast wave (for each explosion) can be calculated by Eq. (5) and the overall positive incident impulse (OPI), expressing the overall shock that cp_b of CI receives after N consecutive explosions (Figure 3 shows the first three out of N explosions), can be calculated by:

$$OPI^{cp_b} = \sum_{i=1}^{N} pi_o \tag{8}$$

by using Eq. (6):

$$OPI^{cp_b} = \int_{t_{1a}}^{t_{1a}} (P_1(t) - P_a)\,dt + \int_{t_{2a}}^{t_{2a}} (P_2(t) - P_a)\,dt + \int_{t_{3a}}^{t_{3a}} (P_3(t) - P_a)\,dt + \ldots \tag{9}$$

by using Eq. (7):

$$OPI^{cp_b} = P_O^1 \cdot \frac{e^{c_1\cdot(t_{1a}+t_{1b})} - e^{c_1\cdot t_{1a}}}{c_1 \cdot e^{c_1\cdot(t_{1a}+t_{1b})} \cdot e^{c_1\cdot t_{1a}}}$$

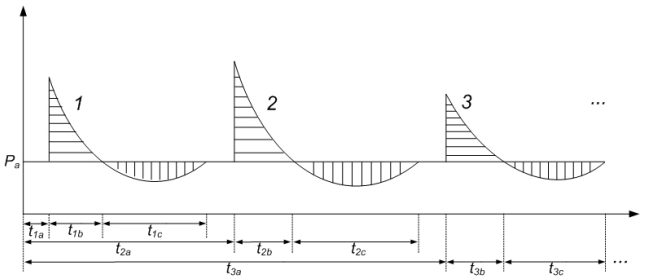

FIGURE 3. Consecutive non-overlapping explosions, near a single critical infrastructure.

$$+ P_O^2 \cdot \frac{e^{c_2\cdot(t_{2a}+t_{2b})} - e^{c_2\cdot t_{2a}}}{c_2 \cdot e^{c_2\cdot(t_{2a}+t_{2b})} \cdot e^{c_2\cdot t_{2a}}} + P_O^3 \cdot \frac{e^{c_3\cdot(t_{3a}+t_{3b})} - e^{c_3\cdot t_{3a}}}{c_3 \cdot e^{c_3\cdot(t_{3a}+t_{3b})} \cdot e^{c_3\cdot t_{3a}}} + .. \tag{10}$$

$$OPI^{cp_b} = \sum_{i=1}^{N} P_O^i \cdot \frac{e^{c_i\cdot(t_{ia}+t_{ib})} - e^{c_i\cdot t_{ia}}}{c_i \cdot e^{c_i\cdot(t_{ia}+t_{ib})} \cdot e^{c_i\cdot t_{ia}}} \tag{11}$$

where P_O^i, c_i, t_{ia}, $(t_{ia}+t_{ib})$ are overpressures, decay factors, times of arrival of the blast waves to cp_b and duration of positive incident impulse of the i_{th}, $i = 1, \ldots N$, explosion respectively.

Equations (5) and (11) are calculated for all cp_b's, $b = 1, \ldots, q$, of the CI and in order to assess the LoT, the proposed *Algorithm 1* is incorporated, with $P_O^{cp_b} = P_O^i$, $i = 1, \ldots, N$ and $pi_o^{cp_b} = OPI^{cp_b}$.

D. MULTIPLE-ATTACK MULTIPLE-INFRASTRUCTURE THREAT ASSESSMENT

In case of multiple-attack multiple-infrastructure threat assessment, it is assumed that multiple ADR trucks possibly explode near multiple neighboring CIs. In order to achieve efficient computational complexity, this scenario is simplified and reduced to one of the two previous scenarios (single-attack single-infrastructure, multiple-attack single-infrastructure). An oblate spheroid or oblate ellipsoid is the regular geometric shape that best approximates the shape of Earth. Thus, Riemannian manifolds could provide better accuracy in case of large geographic areas. However, and for simplicity reasons, in this paper mapped limited geographic areas are considered and handled as 2D euclidean spaces. For simplifying the following notations, crucial points from all CIs are not distinguished according to their origin CI. As a result, the location of crucial point cp_i can be denoted as (x_{cp_i}, y_{cp_i}), providing the corresponding vector $\vec{z}_{cp_i}$. Now let us gather all crucial points from all CIs under consideration, into set $OCP = \{cp_1, cp_2, \ldots, cp_n\} \in \mathbb{R}^2$, where $2 \le n < \infty$ and $cp_i \neq cp_j$, $i \neq j$ and $\forall i, j = 1, 2, \ldots, n$. In this paper the points of set OCP are used as the generator points of a Voronoi tessellation and the region given by

$$VR(cp_i) = \left\{ \vec{z}_{cp} \mid \left\| \vec{z}_{cp} - \vec{z}_{cp_i} \right\| \le \left\| \vec{z}_{cp} - \vec{z}_{cp_j} \right\| \forall j \ni i \neq j \right\} \tag{12}$$

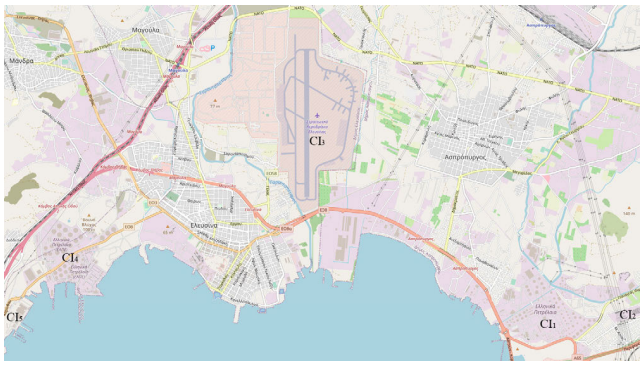

FIGURE 4. Map of the south-west area of Attica prefecture including the locations of the five most important *CIs*.

is called the Voronoi region of cp_i, where $\|\cdot\|$ denotes the Euclidean distance. Then the following set

$$VD_{OCP} = \bigcup_{i=1}^{n} VR(cp_i) \tag{13}$$

is called the Voronoi diagram of *OCP*, which consists of non-overlapping segments. Each segment corresponds to a crucial point of a specific *CI*. In order to reduce the multiple-attack multiple-infrastructure scenario to one of the two previous scenarios, this paper proposes *CI*-based fusion of the non-overlapping segments of the Voronoi diagram. Towards this direction, segments which originate from crucial points that belong to the same *CI*, are fused to provide the *ATA* for each *CI*. More specifically, for the CI_k, $k = 1, 2, \ldots, l$, *CIs*, l classes are created, say C_i, $i = 1, 2, \ldots, l$, as:

$$C_i = \left\{ \bigcup_{b=1}^{q} VR\left(cp_b\right) : cp_b \in CI_i \right\}, \quad i = 1, 2, \ldots, l \tag{14}$$

Then, if only one ADR truck is within the *ATA* of a *CI*, this case is considered as single-attack single-infrastructure and the respective approach of subsection 4.2 is followed. On the other hand, if several ADR trucks are within the *ATA* of a *CI*, this case is considered as multiple-attack single-infrastructure and the respective approach of subsection 4.3 is followed.

V. EXPERIMENTAL RESULTS

A. EXPERIMENTAL SETUP

The unpredictable and persistent nature of terrorism makes it a very difficult issue to tackle. Typically, security authorities do not know whether, at which time and in which place, a terrorist attack will take place. On the other hand and in some cases, current technologies may be able to somehow speculate the cargo of a truck [54]. However, there is not yet any mature technology to distinguish between terrorist and regular trucks, ADR and non-ADR cargo, or terrorist and regular driver. In addition to acts of terrorism, accidents and explosions of trucks also occur often [55]. Furthermore, the crucial points of a critical infrastructure, as well as their levels of importance are confidential information.

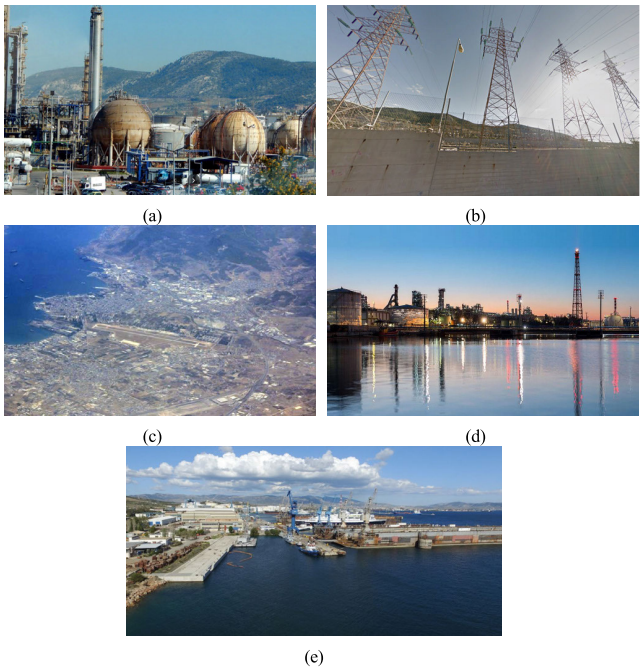

FIGURE 5. The selected five most important *CIs* located at the south-west area of Attica prefecture.

By taking into consideration all aforementioned remarks and limitations, an extended experimentation phase was properly designed and carried out within the interval March 1st – March 30th, 2022 (30 days). Initially the five most important *CIs* located at the south-west area of Attica prefecture (Figure 4) were selected:

a) CI_1: Hellenic Petroleum Industrial site of Aspropyrgos, one of the main public refineries of Greece (Figure 5(a))

b) CI_2: DEH – KYT Koumoundourou, one of the two main high voltage electrical power distribution centers of Attica prefecture (covering 1/3 of the total electrical power of Attica prefecture), (Figure 5(b))

c) CI_3: the Military Airport and Airforce base of Elefsina region, (Figure 5(c))

d) CI_4: the Hellenic Petroleum industrial site of Elefsina, another one of the main public refineries of Greece (Figure 5(d)) and

e) CI_5: Elefsis Shipbuilding & Industrial Enterprises S.A., the largest shipyard in Greece (Figure 5(e)).

Here it should be stressed that: (a) more than 5 million people live within the Attica prefecture, (b) the south-west area of Attica prefecture was selected for experimentation, since it hosts some of the most important *CIs* of Greece, which are also concentrated within a radius of about 5 km (neighboring *CIs*) and (c) similar experiments and analysis can be performed for any region worldwide and for any number of *CIs*.

During the experiments, all trucks moving only on main access roads and highways, neighboring to the *CIs* under examination, were considered as ADR and were analyzed. In particular, traffic passing by the following main

TABLE 4. Latitude, longitude and type of the 39 crucial points, for the five *CIs*.

CI	*cp*	Latitude	Longitude	Type
1	1	38.031287	23.597916	Storage Tank
	2	38.031824	23.597494	Storage Tank
	3	38.032197	23.615452	Storage Tank
	4	38.032191	23.614451	Storage Tank
	5	38.031456	23.614292	Storage Tank
	6	38.031002	23.613503	Storage Tank
	7	38.030596	23.612752	Storage Tank
	8	38.030062	23.611979	Storage Tank
	9	38.029563	23.611292	Storage Tank
2	1	38.033341	23.619775	Power Pylon
	2	38.033397	23.620048	Power Pylon
	3	38.033462	23.620314	Power Pylon
	4	38.033522	23.620585	Power Pylon
	5	38.033594	23.620914	Power Pylon
	6	38.033721	23.621642	Power Pylon
	7	38.033439	23.622358	Power substation
	8	38.033527	23.622691	Power substation
3	1	38.054289	23.555997	Aeroway
	2	38.075054	23.556128	Aeroway
	3	38.065867	23.550570	Control Tower
	4	38.062697	23.563463	Repair Station
4	1	38.039885	23.504270	Storage Tank
	2	38.040427	23.505214	Storage Tank
	3	38.041040	23.506184	Storage Tank
	4	38.042698	23.508889	Storage Tank
	5	38.046948	23.516366	Storage Tank
	6	38.046366	23.515128	Storage Tank
	7	38.045552	23.514056	Storage Tank
	8	38.045763	23.509540	Storage Tank
	9	38.045100	23.508493	Storage Tank
	10	38.044346	23.507345	Storage Tank
	11	38.043402	23.505942	Storage Tank
	12	38.043211	23.504755	Storage Tank
	13	38.047474	23.505084	Storage Tank
	14	38.046631	23.504045	Storage Tank
5	1	38.032592	23.495531	Industrial Building
	2	38.032839	23.496693	Industrial Building
	3	38.033719	23.497204	Industrial Building
	4	38.034367	23.497554	Industrial Building

roads/highways, was considered: Old Highway Athinon-Korinthou (passing near CI_4 and CI_5), NATO Avenue (passing near CI_3), A8-E94 highway (passing near CI_1, CI_3 and CI_4,), A65 highway (passing near CI_1), Panagias Faneromenis Avenue (passing near CI_1 and CI_2) and Dimiourgias Avenue (passing near CI_1 and CI_2). Then, crucial points of the *CIs* under consideration were filtered, based on the main access roads and highways. More specifically, the closest to the main access roads and highways crucial points were kept and as a result 39 crucial points were considered in this experimentation phase. The

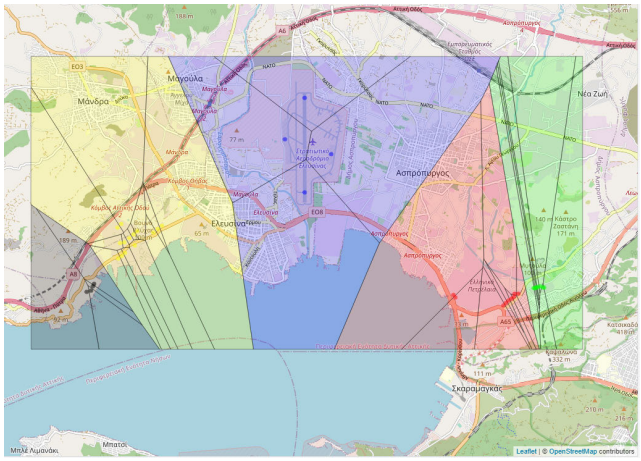

FIGURE 6. The five clusters formed by fusing segments of the Voronoi diagram.

latitude, longitude and type of each crucial point are presented in Table 4, where the decimal degrees format is incorporated.

Set *OCP* includes all these 39 points, used as the generators of the Voronoi tessellation. Then the proposed *CI*-based fusion algorithm of the non-overlapping segments of the Voronoi diagram was applied and five clusters (C_1, C_2, C_3, C_4, C_5) were created, one for each *CI*. Figure 6, which presents all data, was created using the R libraries *leaflet* [56], *sf* [57], *dismo* [58], *sp* [59] and *deldir* [60], as well as *OpenStreeMap* [61]. In Figure 6 the *OCP* points are represented with different colors (red, green, blue, yellow and black) and for each point a polygon is created (the lines of which are visualized in grey color). In particular, C_1 (red area within the bounding box) is formed by fusing the segments of the Voronoi diagram, originating from the 9 crucial points (red circles) of CI_1. C_2 (green area within the bounding box) is formed by fusing the segments, originating from the 8 crucial points (green circles) of CI_2. C_3 (blue area within the bounding box) is formed by fusing the segments, originating from the 4 crucial points (blue circles) of CI_3. C_4 (yellow area within the bounding box) is formed by fusing the segments, originating from the 14 crucial points (yellow circles) of CI_4. C_5 (black area within the bounding box) is formed by fusing the segments, originating from the 4 crucial points (black circles) of CI_5. Here it should also be mentioned that a Voronoi diagram is typically extended to the whole map. However, in this paper threat assessment is considered as local in nature, since an ADR truck explosion should occur near a *CI*, in order to cause damage. For this reason, a bounding box is estimated, so that it includes all aforementioned roads/highways and limits the *ATA* to a maximum distance of 1,000 meters away from the outer crucial points. Thus, when ADR trucks are outside the bounding box, threat assessment is not performed, reducing the computational complexity of the proposed scheme. When ADR trucks enter the bounding box, threat assessment is carried out separately for each cluster, by following the

FIGURE 7. Example of truck and license plate detection using [62]–[64].

single-attack / multiple-attack single-infrastructure methodologies. Additionally, in order to maintain a high degree of awareness of the surroundings of each *CI* and since it may be difficult to install surveillance cameras everywhere, in our experiments traffic surveillance cameras were installed: (a) at the intersections of the considered roads/highways and the bounding box and (b) at the intersections of the considered roads/highways and the limits of the five clusters (C_1, C_2, C_3, C_4, C_5). In total 13 surveillance cameras were installed.

B. ADR TRUCKS CHARGE ESTIMATION

The recorded (from the 13 surveillance cameras) content was collected daily and analyzed by three PCs with Intel(R) Core(TM) i7-9700 CPU @ 3.00GHz and 16 GB DDR4 RAM. Under these settings, content analysis is performed in real time, for up to four video streams per PC. For more than four video streams, either a parallel processing architecture satisfies the real time condition or frame skipping. Initially the following two sample projects were installed and properly adjusted, in order to analyze only trucks: ''Vechicle Detection, Tracking and Counting'' using TensorFlow Object Counting API [62] and ''License Plate Detection and Recognition in Unconstrained Scenarios'' [63], [64]. The first project: (a) detects and classifies vehicles (cars, trucks, bicycles, motorcycles, buses) and (b) estimates the speed of a vehicle, while the second project detects and recognizes license plates.

Only vehicles classified as trucks were further processed. For each truck, its speed was estimated, while its license plate was detected and recognized. In the current experiments the estimated speed of each truck was assumed to be constant, until another camera provides information for a new estimation. The constant speed assumption enables real time estimation of the location of each truck, within each *ATA*. Furthermore, due to plates' recognition, our scheme is aware of the trucks entering/exiting each *ATA*. Figure 7 presents a truck, detected within a rectangle (detection rectangle), where its license plate is concealed for privacy issues.

Next, a worst-case scenario is analyzed for the three most characteristic substances of Table 2. In this scenario it is assumed that all trucks are truck-bombs and carry the maximum amount of explosive matter. In case of terrorist attacks, this is a reasonable scenario, since terrorists aim at maximizing the overall impact of an attack. In order to estimate the possible maximum amount of the explosive matter carried by a truck, the detection rectangle is used, which provides an estimation of the size of the truck. In particular, the detection rectangle for each truck and for a specific distance from the surveillance camera is selected, so that mapping to a specific truck size is accomplished. In this paper, mapping parameters have been estimated and tested by performing several experiments. Then, each truck is classified to one of the categories presented in [65], having a capacity between 82 and 120 m^3. The most dangerous substance of Table 2, octanitrocubane, has a density of 1.98 tons per m^3, thus, in the worst-case scenario, the aforementioned trucks could carry from 162.4 to 237.6 tons of octanitrocubane, or 386.5 (Mass2) to 565.5 (Mass1) tons of charge mass of TNT (parameter M of Eq. (5)). The most characteristic explosive substance is TNT, which has a density of 1.65 tons per m^3, thus, in the worst-case scenario, the aforementioned trucks could carry from 135.3 (Mass4) to 198 (Mass3) tons of TNT. Furthermore, the cheapest and easiest to produce is ANFO, which has a density of 0.82 tons per m^3, thus, in the worst-case scenario, the aforementioned trucks could carry from 67.2 to 98.4 tons of ANFO, or 49.7 (Mass6) to 72.8 (Mass5) tons of charge mass of TNT. Based on the cost of each explosive, terrorists are more likely to use ANFO (∼400 Euro/ton) [66], which, in its worst case, it is represented by Mass5. TNT may require 5 times the cost of ANFO [67], while octanitrocubane is extremely unlikely to be used, since the commercially available starting material for octanitrocubane, dimethyl cubane-1,4-dicarboxylate, costs about 36,000 Euro per kg [68]. Similar calculations can be performed for all substances of Table 2. Figure 8 shows overpressure versus distance, for the six different masses (Mass1-Mass6) and for samples every 50 meters, where the minimum distance is 40 meters (some cp_b's are ∼40 meters away from the roads/highways under examination). The maximum distance is 1,000 meters (see Section 5.2). As it can be observed from Figure 8: (a) for Mass1 the maximum overpressure is 89.4 psig at a distance of 40 meters and the minimum is 0.16 psig at a distance of 1,000 meters, (b) for Mass3 the maximum overpressure is 46.3 psig at a distance of 40 meters and the minimum is 0.11 psig at a distance of 1,000 meters and (c) for the smallest Mass6 the maximum overpressure is 17.6 psig at a distance of 40 meters and the minimum is 0.07 psig at a distance of 1,000 meters. Additionally, explosion of a truck full of octanitrocubane (Mass1) is extremely dangerous even for a distance of 180 meters away from a crucial point of LoT=5, while in case of ANFO (Mass5) the distance falls to 80 meters.

C. THREAT ASSESSMENT AND VULNERABILITY ANALYSIS OF CIs

For the 30 days experimentation interval, in total 33,810 unique trucks, or on average 1,127 unique trucks per day,

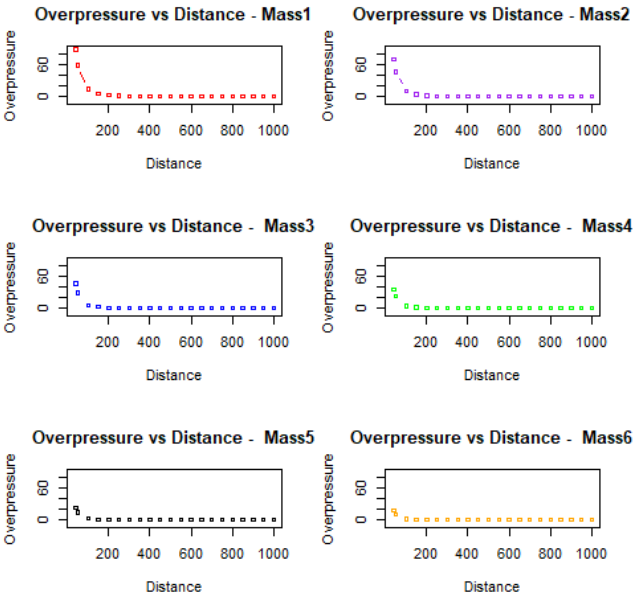

FIGURE 8. Overpressure (psig) versus distance, for the six different masses (Mass1-Mass6).

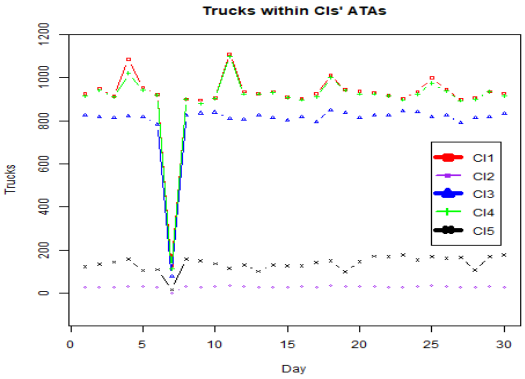

FIGURE 9. Trucks within *CIs' ATAs* per day.

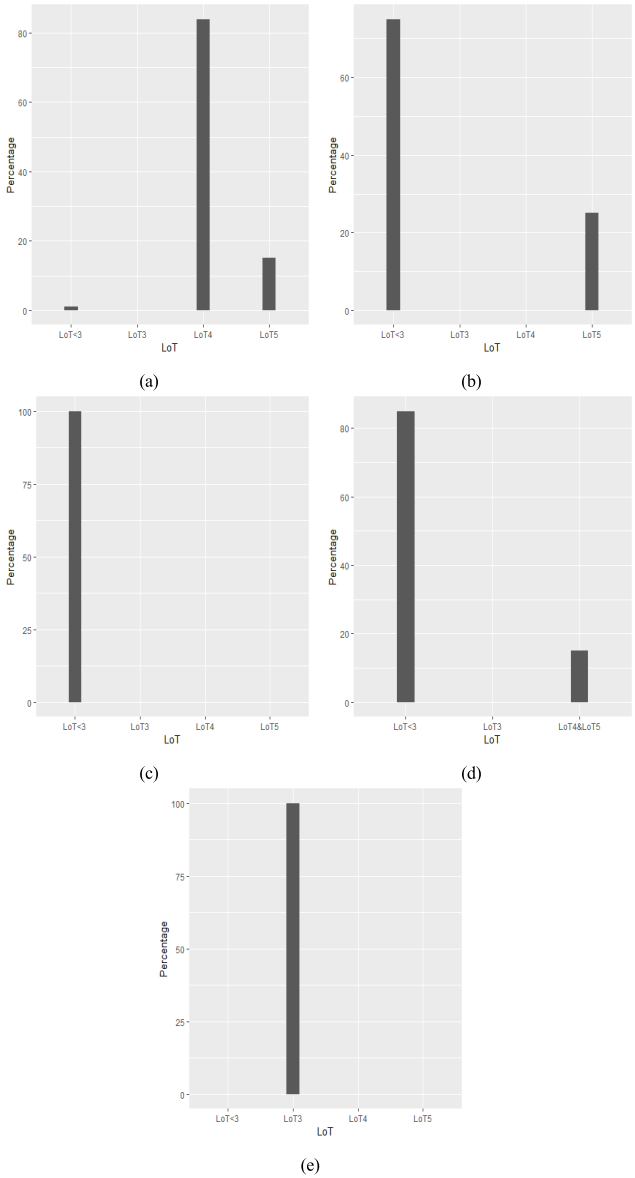

FIGURE 10. Percentage of *LoT* for (a) CI_1, (b) CI_2, (c) CI_3, (d) CI_4 and (e) CI_5.

were detected within the ATAs of the five *CIs* under examination, 72.4% of which passed through A8-E94 highway. Here it should be mentioned that a truck moving on A8-E94 highway, usually passed near all related *CIs* (CI_1, CI_3 and CI_4), one at a time. Similar cases were observed for Old Highway Athinon-Korinthou, Panagias Faneromenis Avenue and Dimiourgias Avenue, which pass from more than one *CIs*. Thus, a unique truck could threaten more than one *CIs*, at different time instances. This paper focuses on the overall threat assessment of each *CI* per time instance and subsequently the total charge mass of TNT per time instance within an *ATA* is considered.

The diagram of the flow of the number of trucks within each area of threat assessment for the 30 days period is provided in Figure 9. As it can be observed, numbers of trucks within the *ATAs* of CI_1 and CI_4 are similar, since these two *CIs* are connected with A8-E94 highway and both of them also have a secondary important source (A65 for CI_1 and the Old Highway Athinon-Korinthou for CI_4). Furthermore, the number of trucks dropped substantially on the 7th of March 2022, which was a public holiday (Green Monday) and trucks were not allowed to move on highways. Additionally, the total number of trucks was 83,379, which means that each of the 33,810 unique trucks, passed from the ATAs of 2.47 *CIs* on average. In particular 27,368 passed from CI_1, 891 from CI_2, 23,859 from CI_3, 27,095 from CI_4 and 4,166 from CI_5.

Next, based on Table 1, thresholds T_1, T_2, T_3, T_4 (in psig) and the respective t_1, t_2, t_3, t_4 (in kPa-ms) were selected as $T_2 = 5 > T_1 = 3 > T_3 = 2 > T_4 = 1$, $t_2 = 200 > t_1 = 100 > t_3 = 70 > t_4 = 40$. Additionally, T_{crd1}, T_{crd2}, T_{crd3} were selected to be 70%, 50% and 30% of the

cp_b's with high *IPC*. Figure 10 presents the *LoT* barplots (*LoT* instances) of the five *CIs*, in case of Mass5 and for the total surveillance period. Axis *x* represents the *LoT* while axis *y* the percentage (%).

As it can be observed in Figure 10: (a) CI_1 is extremely vulnerable with an almost 84% of *LoT*=4 and almost 15% of *LoT*=5. This is due to the fact that all trucks moving on A8-E94 highway, pass near (∼90 meters) a large fuel tank. Additionally, all trucks moving on A65 highway / Panagias Faneromenis avenue, pass very near (∼50 meters / ∼40 meters) large fuel tanks, (b) CI_2 is extremely vulnerable with an almost 25% of *LoT*=5. This is due to the fact that all trucks moving on Dimiourgias avenue pass very near (∼25 meters) from several power pylons, (c) CI_3 is the least vulnerable *CI*, since its crucial points are far away (distance > 400 meters) from the highways/avenues under examination. Even in case of Mass1, the estimated overpressure is less than 0.6 psig. (d) CI_4 is extremely vulnerable and it also presents a peculiarity: all trucks moving on the Old Highway Athinon-Korinthou pass very near (∼40 meters) from large fuel tanks and then, the same trucks, pass near (∼90 meters) other large fuel tanks. In the first case they lead to *LoT*=5 and in the second to *LoT*=4. As a result the two *LoTs* are merged (Figure 10(d)) into one class, (e) finally CI_5 is under substantial risk, since all trucks moving on the Old Highway Athinon-Korinthou pass near (∼100 meters) the machinery buildings of CI_5.

Here it should be mentioned that similar analysis can be performed for any of the aforementioned masses (Mass1 – Mass6), any substance of Table 2 as well as any other explosive substance.

Figure 11 presents the evolution of *LoT* versus time. More specifically, results for the rush hour 15:00 – 16:00 pm (UTC+2) of the 11th of March 2022 are depicted. The specific date was the busiest of the period under consideration, according to the overall number of trucks that passed from the five *CIs*. In Figure 11: (a) the rush hour (60 minutes) is represented by 3,600 seconds, (b) each highway/avenue that a truck passes from and generates a *LoT* (*LoT* 3 to 5), is represented by different color (purple color for Old Highway Athinon-Korinthou, blue color for A8-E94 highway, red color for A65 highway, green color for Panagias Faneromenis Avenue and orange color for Dimiourgias Avenue).

As it can be observed in Figure 11: (a) due to the distance of the cp_bs of CI_1 from A8-E94 highway, A65 highway and Panagias Faneromenis Avenue, CI_1 may suffer critical, severe or significant malfunction several instances per hour, (b) compared to CI_1, things are better for CI_2, however CI_2 may suffer critical malfunction often (2 time instances for the specific date and time), c) CI_3's *LoT* is always less than 3 and thus it is not depicted, (d) CI_4 may suffer critical or severe malfunction several instances per hour, (e) finally CI_5 may suffer significant malfunction several instances per hour, however, compared to CI_1, CI_2 and CI_4, it is in a better position. Here it should be mentioned that similar diagrams

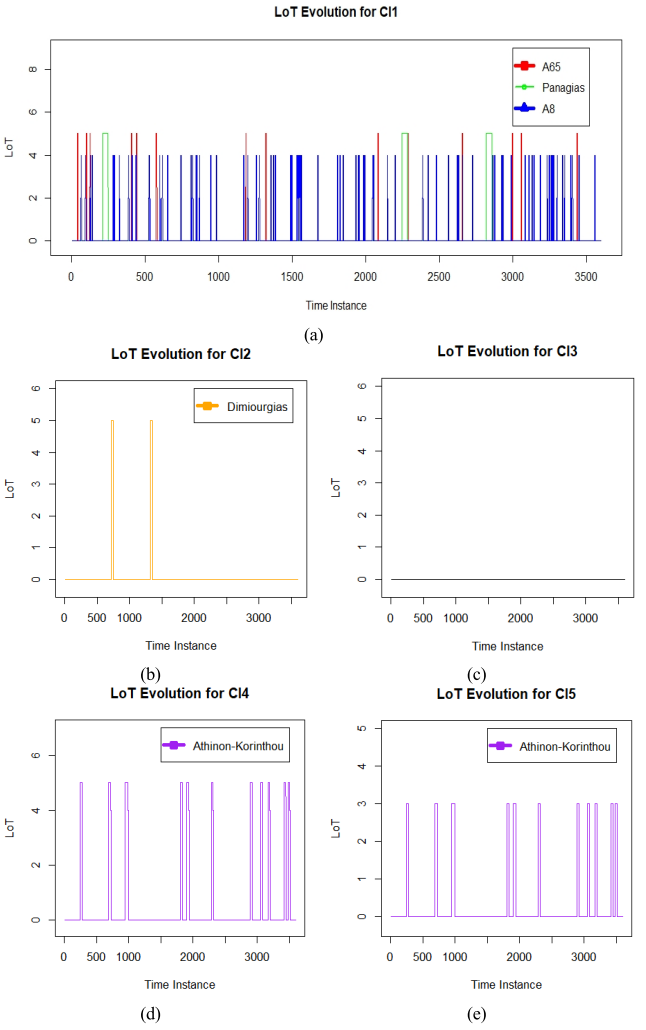

FIGURE 11. Evolution of *LoT* versus time for a specific date and time.

can be provided for any date and time of the surveillance period under consideration, however, the busiest date was analyzed to better illustrate the maximum threat (worst case).

D. COMPARISON TO OTHER APPROACHES

Most of the existing schemes present interesting theoretical solutions to perform threat assessment of *CIs* (based on simulations), while a limited number examines real world settings. To the best of the authors' knowledge, there are not any similar schemes, providing threat analysis of *CIs*, based on the cargos and routes of ADR trucks and using specific *LoTs*. Nevertheless, in this subsection, comparison of the proposed to three existing schemes is provided. In particular: (a) the complexity of the proposed scheme is compared to the complexity of a linear scheme [69], where the concept of omni-directional propagation of the blast wave is presented, (b) the threat notification time of the proposed scheme is compared to the one presented in [70], where sensors/cameras are mounted along the perimeter fence of a *CI* and (c) the estimated surveillance equipment cost of

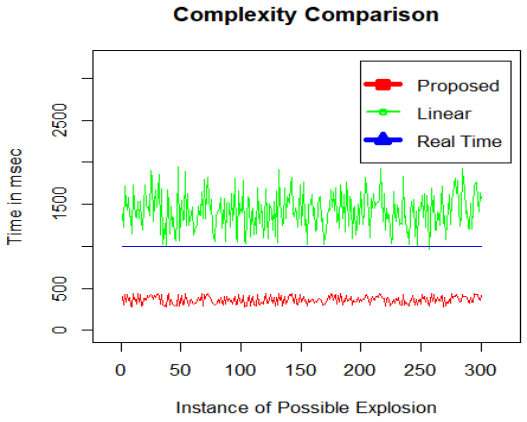

FIGURE 12. Complexity comparison of the proposed scheme and of [69].

the proposed scheme is compared to the cost of [71], where surveillance of the area of a *CI* is accomplished by a grid of sensors.

In terms of complexity, our scheme proposes fusion of Voronoi segments to estimate the *ATA* of each *CI*. In the linear case (omni-directional wave propagation), the threat is estimated for all $cp_b s$, irrespectively of their distance from the blast. Figure 12 illustrates complexity of the proposed scheme and of [69] for a random selection of 300 different time instances (300 instances of possible explosion). As it can be observed, the proposed method reduces computational complexity compared to the linear approach. The average reduction is 3.92 times, providing an average calculation time of 362.73 msec versus 1,422.83 msec for the linear approach (74.5% improvement). Additionally, for the specific settings and for the performed experiments, in most cases the linear approach cannot work in real time (blue line), while the proposed approach is always real time.

In terms of threat notification time, the proposed scheme suggests starting the surveillance of each *CI* at a maximum distance of 1,000 meters away from the outer crucial points. This is due to the fact that in case of Mass5, an explosion becomes extremely dangerous for a cp_b, less than 100 meters away. Even for Mass1, an explosion is extremely dangerous for less than 200 meters. Furthermore, for a truck moving with a speed of 60- 90 km/h, it takes 48/32 seconds to cover 800 meters (approach at 200 meters) and 54/36 seconds to cover 900 meters (approach at 100 meters). This time is enough for trained forces to stop a possible attack. On the other hand, in [70] sensors/cameras are mounted along the perimeter fence of a *CI*. Even if a truck can be detected and its size can be estimated at every point of the field of view of a fence-mounted sensor/camera, in several cases the structure and morphology of the roads do not allow large radiuses of surveillance, for the specific settings and for the performed experiments.

Figure 13 provides the comparison of the average threat notification time of the proposed scheme and of [70]. As it can be observed, the average threat notification time is: (a) 7.7 seconds for [70] and 42.2 seconds for the proposed,

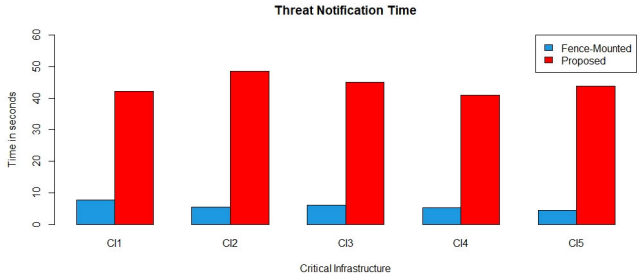

FIGURE 13. Threat notification time comparison of the proposed scheme and of [70].

in case of CI_1, (b) 5.5 seconds for [70] and 48.5 seconds for the proposed, in case of CI_2, (c) 6.1 seconds for [70] and 45.1 seconds for the proposed, in case of CI_3, (d) 5.3 seconds for [70] and 41 seconds for the proposed, in case of CI_4, (e) 4.4 seconds for [70] and 43.9 seconds for the proposed, in case of CI_5. On average, the proposed scheme notifies of a threat 7.9 times faster than [70] (86.9% improvement). Here it should be stated that threat notification times are estimated for the minimum distance that a truck may approach a *CI*. For this minimum distance, threat is at a maximum level, thus threat notification times are even smaller for lower threat levels.

Finally, in terms of estimated surveillance basic equipment cost, the proposed scheme is compared to [71], where surveillance of the area of a *CI* is accomplished by a grid of sensors. In particular the scheme in [71] presents a grid (with grid size 5m $\times$ 5m). In the performed experiments about 21 – 35 % of the rectangles of the grid contained a set of hardware components (ARM-based CPU with 800 MHz, 512 MB RAM, 512 MB flash memory, power requirement of about 1.5 W, iSense sensor node, iSense Core Module (CM30I), iSense Gateway Module (GM20-P) and iSense GPS Module (GPSM10S)). There are several different combinations of similar hardware components in Farnell, Ebay and other sites, starting at about 30 Euro. On the other hand, 4G outdoor wireless cameras start at about 100 Euro (Amazon, Ebay etc.). A rectangle to include all *CIs* under examination, covers an area of about 70 km^2 (56 km^2 by excluding sea segments) and in this case the cost of [71] would be enormous. In order to provide an as fair comparison as possible, this paper considers a surveillance area at a maximum distance of 1,000 meters from a *CI*. Figure 14 provides comparison of the proposed scheme and for [71], for the same maximum distance and for the same highways/avenues.

Here it should be mentioned that: (a) some highways/avenues pass from more than one *CI* and in these experiments the cost has been properly split between *CIs*, (b) for [71], the lowest equipment coverage (21%) was assumed, (c) the total cost (March 2022) for the proposed scheme is about 1,300 Euro, while for [71] it is about 96,000 Euro (98.6% improvement), and (d) [71] may provide higher accuracy regarding the exact position of each truck compared to the proposed approach, but for a significantly higher cost.

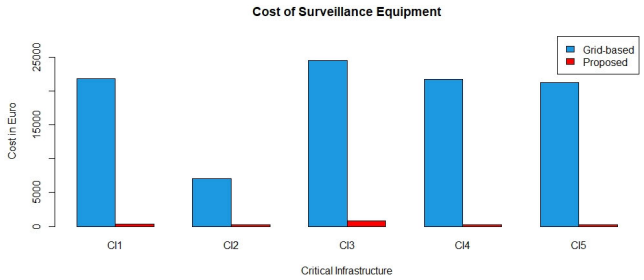

FIGURE 14. Cost comparison of the proposed scheme and of [71] for each of the *CIs* under consideration.

Additionally, for the specific setup and for the performed experiments, the position accuracy of the proposed scheme is satisfactory.

VI. CONCLUSION

CIs can be destroyed in minutes, with insignificant cost or with no cost, if terrorists hijack and turn ADR trucks into moving bombs.

This paper focused on threat assessment of neighboring *CIs*, three scenarios were analyzed and a novel fusion technique of the non-overlapping segments of the Voronoi tessellation was proposed. Additionally, an innovative algorithm was introduced for threat assessment and extensive real-world experiments were carried out.

Future work can focus on different aspects of the problem. For example, toxicity, radioactivity, carcinogenesis, mutagenesis, teratogenesis etc. of the various substances can be considered and a more spherical threat assessment estimation framework can be examined. Sea and air *ATAs* can also be defined, and new surveillance methods can be proposed. Additionally, in detecting trucks, occlusion problems should be confronted, by possibly using multiple cameras/sensors. A lot of work can also be done to provide specific rules of each individual infrastructure. Different scenarios can be covered e.g. for setting the complete *CI* or part of the *CI* out of order.

Furthermore, *CI*-specific blast wave physics could be examined both for a single and for multiple explosions. Finally, *CI*-specific plans for truck ramming attacks could be analyzed, since trucks may forcibly penetrate into *CIs* to approach specific crucial points that are not located near the security fence/wall of the *CI*.

ACKNOWLEDGMENT

The authors would like to thank Dr. Dimitrios Kouremenos, Vasilios Yfantis, Andreas Kener, and Konstantinos Psaraftis for their support, ideas, comments and remarks regarding the experimentation phase.

REFERENCES

[1] G. Liang and L. Deng. *Solving a Mystery of 400 Years—An Explanation to the 'explosion' in Downtown Beijing in the Year of 1626—Research Paper*. Accessed: Mar. 29, 2022. [Online]. Available: https://www.allbestessays.com/essay/Solving-a-Mystery-of-400-Years-An-Explanation-to/47238.html

[2] J. Plester. *Weatherwatch: Lightning Made Castles and Churches Very Dangerous Places*. The Guardian. Accessed: Mar. 29, 2022. [Online]. Available: https://www.theguardian.com/news/2011/jun/16/weatherwatch-lightning-thunderstorm

[3] M. J. Morgan, *The Impact of 9/11 on Politics and War: The Day that Changed Everything?*. New York, NY, USA: Palgrave MacMillan, 2009, p. 264.

[4] W. G. Corley, M. A. Sozen, and C. H. Thornton, "The Oklahoma city bombing: Summary and recommendations for multihazard mitigation," *J. Perform. Constructed Facilities*, vol. 12, no. 3, pp. 100–112, Aug. 1998.

[5] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, "Defending critical infrastructure," *Interfaces*, vol. 36, no. 6, pp. 530–544, Dec. 2006.

[6] *Threat Levels*. Accessed: Mar. 29, 2022. [Online]. Available: https://www.mi5.gov.uk/threat-levels

[7] F. P. Lees, *Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control*, 2nd ed. Oxford, U.K.: Butterworth-Heinemann, 1996, p. 3685.

[8] *TNT Equivalent*. Accessed: Feb. 6, 2022. [Online]. Available: https://en.wikipedia.org/wiki/TNT_equivalent

[9] J. M. Dewey, "Studies of the TNT equivalence of propane, propane/oxygen, and ANFO," *Shock Waves*, vol. 30, no. 5, pp. 483–489, Jul. 2020, doi: 10.1007/S00193-020-00949-W.

[10] Z. Torok and A. Ozunu, "Hazardous properties of ammonium nitrate and modeling of explosions using TNT equivalency," *Environ. Eng. Manage. J.*, vol. 14, no. 11, pp. 2671–2678, 2015, doi: 10.30638/EEMJ.2015.284.

[11] D. Bjerketvedt, J. R. Bakke, and K. van Wingerden. *Gas Explosion Handbook*. Accessed: Feb. 6, 2022. [Online]. Available: https://www.gexcon.com/wp-content/uploads/2020/08/Gas-Explosion-Handbook-1992-version-new-front-page-2019.pdf

[12] A. Ullah, F. Ahmad, H.-W. Jang, S.-W. Kim, and J.-W. Hong, "Review of analytical and empirical estimations for incident blast pressure," *KSCE J. Civil Eng.*, vol. 21, no. 6, pp. 2211–2225, Sep. 2017, doi: 10.1007/S12205-016-1386-4.

[13] B. Hopkinson, "British ordnance board minutes," Brit. Ordnance Office, London, U.K., Tech. Rep., 13565, 1915.

[14] C. Cranz, *Lehrbuch Der Ballistik*. Berlin, Germany: Springer, 1926.

[15] G. F. Kinney and K. J. Graham, *Explosive Shocks in Air*. Berlin, Germany: Springer, 1985, p. 281.

[16] J. Henrych and R. Major, *The Dynamics of Explosion and Its Use*. Amsterdam, The Netherlands: Elsevier, 1979, p. 558.

[17] H. L. Brode, "Numerical solutions of spherical blast waves," *J. Appl. Phys.*, vol. 26, no. 6, pp. 766–775, Jun. 1955, doi: 10.1063/1.1722085.

[18] C. A. Mills, "The design of concrete structure to resist explosions and weapon effects," in *Proc. 1st Int. Conf. Concrete Hazard Protection*, Edinburgh, Scotland, Sep. 1987, pp. 61–73.

[19] C. N. Kingery and G. Bulmash, "Air blast parameters from TNT spherical air burst and hemispherical surface burst," Ballistic Res. Laboratories, Aberdeen Proving Ground, MD, USA, Tech. Rep., BRL 02555, 1984.

[20] Y. Li, Y. Xiao, Y. Li, and J. Wu, "Which targets to protect in critical infrastructures—A game-theoretic solution from a network science perspective," *IEEE Access*, vol. 6, pp. 56214–56221, 2018.

[21] G. M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger, and J. Benjamin, "Industrial and critical infrastructure security: Technical analysis of real-life security incidents," *IEEE Access*, vol. 9, pp. 165295–165325, 2021.

[22] B. Sousa, M. Arieiro, V. Pereira, J. Correia, N. Lourenco, and T. Cruz, "ELEGANT: Security of critical infrastructures with digital twins," *IEEE Access*, vol. 9, pp. 107574–107588, 2021.

[23] A. Y. A. Hammadi, D. Lee, C. Y. Yeun, E. Damiani, S.-K. Kim, P. D. Yoo, and H.-J. Choi, "Novel EEG sensor-based risk framework for the detection of insider threats in safety critical industrial infrastructure," *IEEE Access*, vol. 8, pp. 206222–206234, 2020.

[24] G. Stergiopoulos, D. A. Gritzalis, and E. Limnaios, "Cyber-attacks on the oil & gas sector: A survey on incident assessment and attack patterns," *IEEE Access*, vol. 8, pp. 128440–128475, 2020.

[25] H. Zhu, C. Zhang, J. E. Ramirez-Marquez, S. Wu, and R. Monroy, "The integration of protection, restoration, and adaptive flow redistribution in building resilient networked critical infrastructures against intentional attacks," *IEEE Syst. J.*, vol. 15, no. 2, pp. 2959–2970, Jun. 2021.

[26] K. H. Thompson and H. T. Tran, "Operational perspectives into the resilience of the U.S. Air transportation network against intelligent attacks," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 4, pp. 1503–1513, Apr. 2020.

[27] N. Mohammad, "A multi-tiered defense model for the security analysis of critical facilities in smart cities," *IEEE Access*, vol. 7, pp. 152585–152598, 2019.

[28] F. Subhan, M. Noreen, M. Imran, M. Tariq, A. Khan, and M. Shoaib, "Impact of node deployment and routing for protection of critical infrastructures," *IEEE Access*, vol. 7, pp. 11502–11514, 2019.

[29] H. Fujita, A. Gaeta, V. Loia, and F. Orciuoli, "Resilience analysis of critical infrastructures: A cognitive approach based on granular computing," *IEEE Trans. Cybern.*, vol. 49, no. 5, pp. 1835–1848, May 2019.

[30] N. Bakalos, A. Voulodimos, N. Doulamis, A. Doulamis, A. Ostfeld, E. Salomons, J. Caubet, V. Jimenez, and P. Li, "Protecting water infrastructure from cyber and physical threats: Using multimodal data fusion and adaptive deep learning to monitor critical systems," *IEEE Signal Process. Mag.*, vol. 36, no. 2, pp. 36–48, Mar. 2019.

[31] J. Lopez, N. C. Liefer, C. R. Busho, and M. A. Temple, "Enhancing critical infrastructure and key resources (CIKR) level-0 physical process security using field device distinct native attribute features," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1215–1229, May 2018.

[32] G. Falco, A. Viswanathan, C. Caldera, and H. Shrobe, "A master attack methodology for an AI-based automated attack planner for smart cities," *IEEE Access*, vol. 6, pp. 48360–48373, 2018.

[33] S. Tweneboah-Koduah and W. J. Buchanan, "Security risk assessment of critical infrastructure systems: A comparative study," *Comput. J.*, vol. 61, no. 9, pp. 1389–1406, Sep. 2018.

[34] R. J. Rodríguez, J. Merseguer, and S. Bernardi, "Modelling security of critical infrastructures: A survivability assessment," *Comput. J.*, vol. 58, no. 10, pp. 2313–2327, Oct. 2015.

[35] G. Giannopoulos, R. Filippini, and M. Schimmer, "Risk assessment methodologies for critical infrastructure protection. Part I: A state of the art," Eur. Commission, Joint Res. Centre, Inst. Protection Secur. Citizen, Publications Office Eur. Union, Luxembourg, U.K., Tech. Rep. EUR 25745 EN, 2012.

[36] J. Moteff, "Risk management and critical infrastructure protection: Assessing, integrating, and managing threats, vulnerabilities and consequences," Congressional Res. Service, Washington, DC, USA, Tech. Rep. ADA454038, 2004.

[37] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," *Int. J. Crit. Infrastruct. Protection*, vol. 8, pp. 53–66, Jan. 2015.

[38] D. A. Linger, G. H. Baker, and R. G. Little, "Applications of underground structures for the physical protection of critical infrastructure," in *Proc. North Amer. Tunneling*, Lisse, The Netherlands, 2002, pp. 333–339.

[39] D. Dominguez, M. J. Parks, A. D. Williams, and S. Washburn, "Special nuclear material and critical infrastructure security modeling and simulation of physical protection systems," in *Proc. IEEE Int. Carnahan Conf. Secur. Technol. (ICCST)*, Boston, MA, USA, Oct. 2012, pp. 10–14.

[40] T. Lovecek, J. Ristvej, and L. Simak, "Critical infrastructure protection systems effectiveness evaluation," *J. Homeland Secur. Emergency Manage.*, vol. 7, no. 1, pp. 1–25, Jan. 2010, doi: 10.2202/1547-7355.1613.

[41] C. Pursiainen, "The challenges for European critical infrastructure protection," *J. Eur. Integr.*, vol. 31, no. 6, pp. 721–739, Nov. 2009.

[42] J. Depoy, J. Phelan, P. Sholander, B. Smith, G. B. Varnado, and G. Wyss, "Risk assessment for physical and cyber attacks on critical infrastructures," in *Proc. IEEE Mil. Commun. Conf.*, vol. 3. Atlantic City, NJ, USA, Oct. 2005, pp. 1961–1969.

[43] C. Aradau, "Security that matters: Critical infrastructure and objects of protection," *Secur. Dialogue*, vol. 41, no. 5, pp. 491–514, Oct. 2010.

[44] J. Monaghan and K. Walby, "Surveillance of environmental movements in Canada: Critical infrastructure protection and the petro-security apparatus," *Contemp. Justice Rev.*, vol. 20, no. 1, pp. 51–70, Jan. 2017.

[45] J. Isern, F. Barranco, D. Deniz, J. Lesonen, J. Hannuksela, and R. R. Carrillo, "Reconfigurable cyber-physical system for critical infrastructure protection in smart cities via smart video-surveillance," *Pattern Recognit. Lett.*, vol. 140, pp. 303–309, Dec. 2020.

[46] Z. Sabeur, Z. Zlatev, P. Melas, G. Veres, B. Arbab-Zavar, L. Middleton, and N. Museux, "Large scale surveillance, detection and alerts information management system for critical infrastructure," in *Environmental Software Systems. Computer Science for Environmental Protection* (IFIP Advances in Information and Communication Technology). Cham, Switzerland: Springer, 2017, pp. 237–246.

[47] D. Procházková and J. Procházka, "Risk management quality in selected critical facilities," *WSEAS Trans. Comput. Res.*, vol. 4, pp. 96–108, Jan. 2016.

[48] A. Doulamis, N. Doulamis, K. Ntalianis, and S. Kollias, "An efficient fully unsupervised video object segmentation scheme using an adaptive neural-network classifier architecture," *IEEE Trans. Neural Netw.*, vol. 14, no. 3, pp. 616–630, May 2003.

[49] K. Ntalianis, A. Doulamis, N. Tsapatsoulis, and N. Doulamis, "Human action analysis, annotation and modelling in video streams based on implicit user interaction," in *Multimedia Tools and Applications*, vol. 50. Cham, Switzerland: Springer, Oct. 2010, pp. 199–225.

[50] K. Ntalianis, N. Tsapatsoulis, and A. Drigas, "Video-object oriented biometrics hiding for user authentication under error-prone transmissions," *EURASIP J. Inf. Secur.*, vol. 2011, pp. 1–12, Feb. 2011. [Online]. Available: https://jis-eurasipjournals.springeropen.com/articles/10.1155/2011/174945

[51] K. S. Ntalianis, A. Doulamis, N. Doulamis, and A. Drigas, "Unsupervised segmentation of stereoscopic video objects: Proposal and investigation of two depth-based approaches," *J. Signal Process. Syst.*, vol. 81, no. 2, pp. 153–181, 2015.

[52] K. Ntalianis and N. Tsapatsoulis, "Remote authentication via biometrics: A robust video-object steganographic mechanism over wireless networks," *IEEE Trans. Emerg. Topics Comput.*, vol. 4, no. 1, pp. 156–174, Jan. 2016.

[53] A. Skraparlis, K. Ntalianis, D. Kouremenos, and N. Mastorakis, "An innovative security screening architecture for detecting illicit goods and threats," *Int. J. Math. Comput. Simul.*, vol. 15, pp. 153–160, Dec. 2021.

[54] W. Visser, A. Schwaninger, D. Hardmeier, A. Flisch, M. Costin, C. Vienne, F. Sukowski, U. Hassler, I. Dorion, A. Marciano, G. Koomen, M. Slegt, and A. C. Canonica, "Automated comparison of X-ray images for cargo scanning," in *Proc. IEEE Int. Carnahan Conf. Secur. Technol. (ICCST)*, Orlando, FL, USA, Oct. 2016, pp. 1–8.

[55] *List of Explosions*. Accessed: Apr. 4, 2022. [Online]. Available: https://en.wikipedia.org/wiki/List_of_explosions

[56] (2022). *Leaflet: Create Interactive Web Maps With the JavaScript 'Leaflet' Library*. [Online]. Available: https://cran.r-project.org/web/packages/leaflet/index.html

[57] (2022). *SF: Simple Features for R*. [Online]. Available: https://cran.r-project.org/web/packages/sf/index.html

[58] (2022). *Dismo: Species Distribution Modeling*. [Online]. Available: https://cran.r-project.org/web/packages/dismo/index.html

[59] (2022). *SP: Classes and Methods for Spatial Data*. [Online]. Available: https://cran.r-project.org/web/packages/sp/index.html

[60] (2022). *Deldir: Delaunay Triangulation and Dirichlet (Voronoi) Tessellation*. [Online]. Available: https://cran.r-project.org/web/packages/deldir/index.html

[61] *Open Street Map Foundation*. Accessed: Apr. 4, 2022. [Online]. Available: https://www.openstreetmap.org/

[62] A. Özlü. (2018). *Vehicle Detection, Tracking and Counting by TensorFlow*. [Online]. Available: https://github.com/ahmetozlu/vehicle_counting_tensorflow

[63] S. M. Silva and C. R. Jung, "License plate detection and recognition in unconstrained scenarios," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, Munich, Germany, Sep. 2018, pp. 580–596.

[64] S. M. Silva and C. R. Jung. (2018). *License Plate Detection and Recognition in Unconstrained Scenarios*. [Online]. Available: https://github.com/sergiomsilva/alpr-unconstrained

[65] *Dimensions and Sizes of Trucks*. Accessed: Apr. 4, 2022. [Online]. Available: http://fess.su/news/dimensions-and-sizes-of-trucks

[66] *Fertilizer Savings*. Accessed: Apr. 4, 2022. [Online]. Available: https://www.nrcs.usda.gov/wps/portal/nrcs/detail/null/?cid=nrcs144p2_056386

[67] *Effect of Nuclear Weapons on Historic Trends in Explosives*. Accessed: Apr. 4, 2022. [Online]. Available: https://aiimpacts.org/discontinuity-from-nuclear-weapons/

[68] *Design and Synthesis of Explosives: Polynitrocubanes and High Nitrogen Content Heterocycles*. Accessed: Apr. 4, 2022. [Online]. Available: https://chemistry.illinois.edu/system/files/inline-files/8_LaFrate_Abstract_SP05.pdf

[69] M. Esa, M. S. Amin, and A. Hassan, "Relative performance of novel blast wave mitigation system to conventional system based on mitigation percent criteria," *Defence Technol.*, vol. 17, no. 3, pp. 912–922, Jun. 2021.

[70] Z. Sabeur, Z. Zlatev, P. Melas, G. Veres, B. Arbab-Zavar, L. Middleton, and N. Museux, "Large scale surveillance, detection and alerts information management system for critical infrastructure," in *Proc. 12th Int. Symp. Environ. Softw. Syst.*, Zadar, Croatia, May 2017, pp. 237–246.

[71] M. Niedermeier, X. He, H. de Meer, C. Buschmann, K. Hartmann, B. Langmann, M. Koch, S. Fischer, and D. Pfisterer, "Critical infrastructure surveillance using secure wireless sensor networks," *J. Sensor Actuator Netw.*, vol. 4, no. 4, pp. 336–370, Nov. 2015.

ATHANASIOS SKRAPARLIS received the master's degree in environmental, disasters and crises management strategies from the National and Kapodistrian University of Athens. He is currently pursuing the Ph.D. degree with the Department of Business Administration, University of West Attica, his Ph.D. thesis entitled "Intelligent Approaches for Tackling Cyber-Physical Threats of Critical Infrastructures." He also works as an External Security Expert with SymBioLogic Ltd. He has published three scientific articles, receiving more than 100 citations. He has also prepared various project proposals in security topics for the Horizon Europe framework. He also participates in the COST Action CA17102–Police Stops. During his master's thesis, he has done research on the topic of EU Host Nation Support Policy. In particular, he studied topics relevant to the European Strategy for Host Nation Support Policy, the EU Civil Protection Mechanism and the international cooperation in case of a crisis-disaster. His main research interests include security and critical infrastructures' protection.

KLIMIS S. NTALIANIS received the Diploma and Ph.D. degrees from the Electrical and Computer Engineering Department, National Technical University of Athens (NTUA), in 1998 and 2003, respectively. Since 1998, he has participated in more than 25 research and development projects in different frameworks. From 2004 to 2009, he was a Senior Researcher and Projects Coordinator at the Image, Video and Multimedia Laboratory, NTUA. In 2020, he became a Professor at the University of West Attica. He has published more than 160 scientific articles (IEEE, ACM, Springer, and Elsevier) and has received more than 850 citations. He also worked as a Research Evaluator for several international journals and conferences, such as the European Union, the Romanian Executive Agency for Higher Education Research Development and Innovation Funding, the Greek Secretariat of Research and Technology, the Cyprus Promotion Foundation, the Polish National Science Center, the Natural Sciences and Engineering Research Council of Canada, the University of Jeddah (Saudi Arabia), the University of Magdeburg (Germany), the Sant Longowal Institute of Engineering & Technology (India), the Cyprus University of Technology, and other organizations. His main research interests include multimedia analysis, social computing, and new technologies for disruptive business and innovation. He has served as the General Executive Chair for the 3rd IEEE Cyber Science and Technology Congress, the 16th IEEE International Conference on Dependable, Autonomic Secure Computing, the 16th IEEE International Conference on Pervasive Intelligence and Computing, and the 4th IEEE International Conference on Big Data Intelligence and Computing.

NIKOS E. MASTORAKIS (Senior Member, IEEE) received the B.Sc. and M.Sc. (Diploma) degrees in electrical engineering and the Ph.D. degree in electrical engineering and computer science from the National Technical University of Athens (NTUA), Athens, Greece, and the B.Sc. (Ptychion) degree in pure mathematics from the National and Kapodistrian University of Athens, Athens. He studied medicine with the Medical School of Athens, National and Kapodistrian University of Athens. He was a Special Scientist in computers and electronics with the Hellenic (Greek) Army General Staff, from 1993 to 1994, where he taught several courses in the Electrical and Computer Engineering Department, NTUA, from 1998 to 1994. He was a Visiting Professor with the School of Engineering, University of Exeter, Exeter, U.K., in 1998; and a Visiting Professor with the Technical University of Sofia, Sofia, Bulgaria, from 2003 to 2004; where he is currently a Professor. He is a Registered Professional Electrical and Mechanical Engineer. He has authored more than 800 papers in international journals and conferences and has received more than 6,600 citations. He is a member of the New York Academy of Sciences, the A. F. Communications and Electronics Association, the American Association for the Advancement of Science, and other smaller scientific societies. He is the Editor-in-Chief in many international journals. He was the General Chairperson in more than 30 international conferences. He has organized more than 40 special sessions and three workshops and has given many plenary lectures.