Int. J. Appl. Math. Comput. Sci., 2022, Vol. 32, No. 3, 495–510
DOI: 10.34768/amcs-2022-0036

ATiPreTA: AN ANALYTICAL MODEL FOR TIME–DEPENDENT PREDICTION OF TERRORIST ATTACKS

OUSSAMA KEBIR [a,*], ISSAM NOUAOURI [b], LILIA REJEB [a], LAMJED BEN SAID [a]

[a] SMART-LAB, Tunis Higher Institute of Management
University of Tunis
92, Boulevard 9 Avril 1938, 1007 Tunis, Tunisia
e-mail: direction@isg.rnu.tn

[b] LGI2A Laboratory
University of Artois
9 rue du Temple, 62400 Béthune, France

In counter-terrorism actions, commanders are confronted with difficult and important challenges. Their decision-making processes follow military instructions and must consider the humanitarian aspect of the mission. In this paper, we aim to respond to the question: *What would the casualties be if governmental forces reacted in a given way with given resources?* Within a similar context, decision-support systems are required due to the variety and complexity of modern attacks as well as the enormous quantity of information that must be treated in real time. The majority of mathematical models are not suitable for real-time events. Therefore, we propose an analytical model for a time-dependent prediction of terrorist attacks (ATiPreTA). The output of our model is consistent with casualty data from two important terrorist events known in Tunisia: Bardo and Sousse attacks. The sensitivity and experimental analyses show that the results are significant. Some operational insights are also discussed.

Keywords: terrorist attacks, attack classification, mathematical modeling, dynamic behavior simulation, damage prediction.

1. Introduction

To create a general climate of instability and fear in a population, many armed groups resort to violence. The harmfulness of planned violence has an impact on the socio-economic situation and on government authority. The main objective of these groups is to put pressure on the government to submit to their political demands. This adversarial situation underpins the concept of terrorism (Willis *et al.*, 2005).

To generate widespread fear, attackers carefully choose their victims as well as the location of terrorist actions. They have to carry out increasingly dramatic attacks to attract media attention. Thus, crowded urban areas are the preferred field of action for terrorists (Sandler, 2018). With the purpose of confronting terrorism and providing safety for all potential targets, decision-makers should establish a proactive strategy. This includes infiltrating and destructing terrorist training camps, intelligence gathering securing funding sources, and also the use of new technologies to estimate the victims of a planned attack.

Estimating the number of victims is the cornerstone for deciding the possible course of actions against terrorist attacks. Based on estimation results, experts could re-manage their human and material resources and provide an adapted plan. In a fast-growing and technologically sophisticated theatre of operations, the amount of information available for planning has increased significantly while time has remained constant. The battle of time management is still the hardest one to win. Static modeling of interventions is inefficient in modern operations where time is an essential and decisive factor for success.

In an attempt to solve this problem, we propose our contribution that consists in creating an analytical model for time-dependent prediction of terrorist actions.

*Corresponding author

The strength of our novel analytical model for a time-dependent prediction of terrorist attacks (ATiPreTA) consists in predicting the extent of human casualties incurred by governmental forces and terrorists during an entire operation. It is useful for assessing possible losses in a terrorist attack on likely and sensitive targets as well as evaluating the efficiency of pre-planned response scenarios.

ATiPreTA integrates new parameters such as stress and intelligence. In fact, human behavior is very sensitive to the former. During extreme danger, the body and the brain maintain a state of high alert that affects how a solder fights. The reactions generally converge to two main axes. The first one introduces the combat stress syndromes that include tiredness, slower reaction times, and indecision leading to a decrease in the combatant's fighting efficiency. The second one, called focused stress, helps the combatants to be more situationally aware. This refines their security consciousness and sense of responsibility. This kind of stress is vital for survival and accomplishing the mission (Army, 2006). Throughout our model, we consider two types of focused stress. The level of available intelligence during a counter-terrorism mission is estimated from the information flows collected during the operation. Besides, we assume that terrorists do not all pose the same level of threat. This estimation helps to reduce casualties among the civilian and government forces and to recognize the danger level. To our knowledge, this is the first attempt to model the effect of parameters like terrorist types and stress on the victims in dynamic combat settings in general and terrorist attacks in particular. Moreover, in this paper, we propose a classification of terrorist attacks adapted by ATiPreTA due to the variety of terrorist attacks, the widespread field of operation, and the difficulty of creating a model that fits all cases.

The remainder of this paper is organized as follows. In the next section, we present and detail related contributions on modeling and classifying terrorist attacks. Section 3 is dedicated to describing our new model as well as its main assumptions. In Section 4, through experimental analysis, we provide the different results offered by our contribution, according to some evaluation criteria with discussions. Then, we test the sensitivity of ATiPreTA by analyzing the effect on the outputs. Finally, we sum up and draw some conclusions.

2. Related works

In this section, we address different aspects that correspond to our model. We begin by reviewing the different concepts of terrorist-attack classification, highlighting the main criteria used by each, and citing visual analysis systems used to present the results. Through this analysis, we will be able to recognize the work paths of the different models. Furthermore, we move to the analysis of the mathematical models that issue from the Lanchester one (Lanchester, 1916) by focusing on the purpose addressed by each model and on the adapted evolution of Lanchester equations. Then, we emphasize the shortcomings of the mathematical models giving rise to revolutionary decision support systems (DSSs). Finally, we list the various DSSs that unpack the major problems of counterinsurgency operations.

2.1. Terrorist attack classification models. There is very little academic literature regarding the analysis of categorical classification of terrorist groups and the body of knowledge is minimal when it comes to the classification of terrorist acts. This is due to the heterogeneity, the variety of attacks and the confusing definitions of terrorism that have changed over time without even saying about the geopolitical environment. In this context, classification methods are used to analyze terrorism data and extract significant results. The evaluation parameters of a classification are selected according to the phenomenon to be analyzed. Based on the five Ws (who, what, where, when, and why), a visual analytical system was developed by Vilanova *et al*. (2008). The parameters of the five Ws represent one of the most fundamental concepts in investigative analysis. With this approach, an investigator can categorize terrorists efficiently by discovering the reasons for attacks, identifying temporal or geo-spatial patterns between multiple terrorist groups, and combining different methods or modes of attack. Data Rivers (Pagán, 2010) is another interactive visual analysis tool for the Global Terrorism Database[1] (GTD) created at the University of Maryland. This tool allows users to analyze temporal trends in terrorism in the GTD by choosing important variables from the database and creating a comprehensible visualization. Five different classes are selected: Countries Attacked, Regions Attacked, Target Nationalities, Types of Targets and Types of Weapons.

Several classifications even use an assessment model that combines multiple factors (Hu *et al*., 2019). The majority of terrorist attack classifications take as their guidelines only basic parameters. To our knowledge, all research within this framework is partially concordant due to the scarcity of significant exploitable classification criteria. Such classification proposals generally suggest works aiming to assign each terrorist attack to a given class. To model these kinds of attacks, other works have also been proposed to predict terrorist behaviors.

2.2. Lanchester based mathematical models. The first use of mathematical models to describe a battle between two parties was proposed by Lanchester

[1] www.start.umd.edu/gtd.

(1916), who created two nonlinear differential equations to analyze the time dependence of the strengths of two armies. Then, researchers developed this model using various techniques and approaches that are described below. Their results were expanded during World War II to support strategic planning for ground, air, and maritime operations. After the WWII, the military research achievements pushed the early development of the simulation field and notably influenced the institutionalization of military research organizations. Besides, the ascendance of other approaches, e.g., asymmetric warfare, which employed innovative nontraditional tactics obliged leaders to develop their resources. For that reason, Lanchester's model has been modified and adapted to distinguish a type of asymmetric warfare such as guerilla (Deitchman, 1962). However, students of military tactics still appreciate the Lanchester model and its universal application because, above all, it stimulates in-depth reflection on the impact of the conditions of engagement (Lucas and McGunnigle, 2003). This appreciation is shown by the Kress and Szechtman (2009) model, which is based on Lanchester equations and studies anti-insurgent operations including the effect of imperfect intelligence. The authors, there, affirm that collateral damage may lead to an increase in terrorist recruitment. They also explain why terrorists cannot be completely eliminated. Without reliable intelligence, government forces can incur population casualties if they miss their targets. This collateral damage generates support for insurgency, which is demonstrated by new recruits joining their ranks.

Recently, Kress *et al*. (2018) adapted the two-dimensional Lanchester square law to fit a three-part engagement. The work of Coulson (2018) is based on the Lanchester model and extends it to a hyperbolic system of partial differential equations (PDEs) to analyze the influence of intelligence on warfare tactics. A Lanchester-type battle model is offered by Bongers and Torres (2019) to simulate battles in which one or two of the fighting groups are not able to use all forces at the same time due to certain limitations such as topographical constraints that create a bottleneck on the battlefield.

We note that all the previously mentioned models are based on the mathematical Lanchester one (Lanchester, 1916) and the majority of them suffer from the absence of the dynamic aspect. The lack of dynamics is associated with all mathematics-based models, such as those by Okoye *et al*. (2020) or Gambo (2020). Okoye *et al*. (2020) study the dynamism of terrorists and counter-terrorism measures that can mitigate their effects in a given location. Okoye *et al*. (2020) have not been inspired by the Lanchester model, but they aim to conduct a real case and make predictions on the terrorism dynamics in the presence or absence of counter-terrorism measures. In addition, Gambo (2020) designed a mathematical model of counter-terrorism with military strategies and rehabilitation of terrorists. The model is developed to control the spread of terrorist ideologies in society and to describe terrorist groups. In the following subsection, we cite and discuss the merging of the defence sphere and decision support systems.

2.3. Decision support systems in military field. The merging of the defence sphere and DSSs gives life to dynamic and revolutionary models without needing the Lanchester model (Lanchester, 1916). The project Deep Green was established in 2008 and sponsored by the Defense Advanced Research Projects Agency (DARPA). It represents the initiation of the modern perspective on DSSs in military operations. This project involved the development of a decision support system for US Army commanders. All the information published on this project regards only basic theoretical data and the detailed results are considered classified (Surdu and Kittka, 2008).

Şuşnea (2012) selects the possibilities and constraints for the development of an intelligent DSS to support military decision-makers in issuing real-time orders at the appropriate moment with a reasonable cost. Later, the empirical research presented in the work of Lee and Zo (2017) focuses on the factors influencing the assimilation of the military group decision support system (MGDSS) and the mediating impact of structural appropriation in the Korean military in a technology, organization and environment (TOE) framework. Maureen (2017) created a DSS called the mission combat efficiency estimator (MCEE) that helps military commanders to assess the best combination of soldiers for different military operations, based regarding intelligence on the enemy's combat experience. Furthermore, a dynamic causal model of public support for insurgency and terrorism was proposed by Osoba and Kosko (2017). It models the structure of public support for insurgency and terrorism using feedback in the form of fuzzy cognitive maps.

Pechenkina and Bennett (2017) propose another dynamic model of insurgent–soldier interactions that handles two strategies for peacefully recruiting citizens and conducting military engagements against the adversary. Moreover, Chmielewski *et al*. (2018) propose a method for developing situational awareness as well as a support tool developed for individual soldiers and low-level commanders. Seehuus *et al*. (2020) introduced a research prototype (SWAP) of a DSS for military planning. The aim of their research is to convince Norwegian Armed Forces commanders about the value of simulation in tactical operations (cf. Kebir *et al.*, 2020a; 2020c). Udoh and Oladejo (2019) developed and analyzed a differential equation model of terrorist

organizational dynamics. They mainly aim to study the possible strategies to allocate the available human resources toward an optimal counter-terrorism operation.

Oladejo *et al*. (2020) analyze an evolutionary game theoretic model for an interaction between security agencies and terrorist group. They study security implications of undermining a given community's optimal supports.

2.4. Criticism and a discussion. We note that models presented in this section are designed to provide suggestions for decision making in certain situations. They can only sustain recurring decision cases and depend on a specified set of models to work. Besides, we mention that even if the Lanchester based mathematical model (LBMM) presents effective approaches for analyzing different aspects of asymmetric engagements, it does not deal with the dynamic aspects of an armed conflict (El-Douh *et al*., 2022; Junosza-Szaniawski *et al*., 2022). Because asymmetrical wars are limited in time and governed by tactical rules adapted to temporary situations, we aim to integrate the dynamic aspect into a modified Lanchester model. Therefore, integrating time in prediction models and simulations is a crucial requirement for operation assessment.

Using equations from the Kress and Szechtmann model, we create an analytical model for time-dependent prediction of terrorist attacks to tackle the latter problems and forecast fluctuations in numbers during a terrorist attack.

By studying the literature, we found that military decision support systems (MDSSs) are generally based on specific models and dedicated to particular users to clarify some interactions (Sumithra and Vadivel, 2021; Chabir *et al*., 2018). Hence, we aim to be more flexible for our generic model to be adaptable to multiple scenarios. In Fig. 1, we summarize how we linked three disciplines connected with the military field to establish our ATiPreTA. The first, presented in white rectangles, shows different methods of terrorist attack classifications. The second, presented with rectangles, is about hierarchical interrelations between mathematical models based on Lanchester's equations. The third, with hexagon shapes, concerns a DSS designed for decision makers to support making correct decisions in stressful situations (obtaining the most accurate decision). In our work, we seek to exploit and combine the strengths of different state-of-the-art works such as dynamics and efficiency. In addition, we estimate, through our model, human casualties during terrorist attacks by integrating the stress level and the effect of the type of terrorist on their behavior (Kebir *et al.*, 2022).

3. Problem statement and contributions

This section presents the assumptions proposed for our research that will be evaluated in the model (Section 3.1). The last assumption made gives rise to a new classification concept of terrorist acts (Section 3.2). Finally, we proceed to detail and describe our own model (Section 3.3).

3.1. Assumptions. The model has three components: government forces, terrorists and a population. As shown in Fig. 3, ATiPreTA is divided into two phases. The first consists in analyzing the effect of terrorists on a population when government forces do not intervene. The second phase starts with the intervention of government forces. It takes into account the interactions between the three actors based on a three-step process. Consequently, let us define and explain our main assumptions for this work:

A1. Government forces neutralize terrorists and seek to minimize civilian casualties while terrorists attack both government forces and civilians.

A2. During terrorist acts combat is asymmetric. We assume that terrorists initially have good situational awareness regarding governmental forces. However, the advantages of this situation disappear due to the scarcity of intelligence resources during the attack. Over time, government forces acquire an increasing amount of information about the situation and are also supported by a constant number of agents.

A3. Well-trained combatants in defensive fighting positions are capable of facing conventional enemy forces double their size (Aylwin-Foster, 2005).

A4. Our model predicts the values of each component in a minute. This time unit is the most appropriate for two reasons: first, the lack of accurate data on real attacks presents serious difficulties for result analysis and model sensitivity studies. Second, this time unit maintains the dynamic aspect and continuity of the analyzable result.

A5. The process is considered to end at t_{final}, when either government forces, terrorists, or civilians are reduced to zero.

A6. The model considers specific classes of attacks that refer to our scenarios mentioned in the previous five assumptions. As in Section 2, the majority of terrorist-attack classification methods are burdened with serious problems. They are designed either for a particular context to fit well-defined criteria or to be very generic, which makes them hard to adjust (Kebir *et al*., 2021). We propose a method for classifying terrorist attacks in the next subsection that obeys

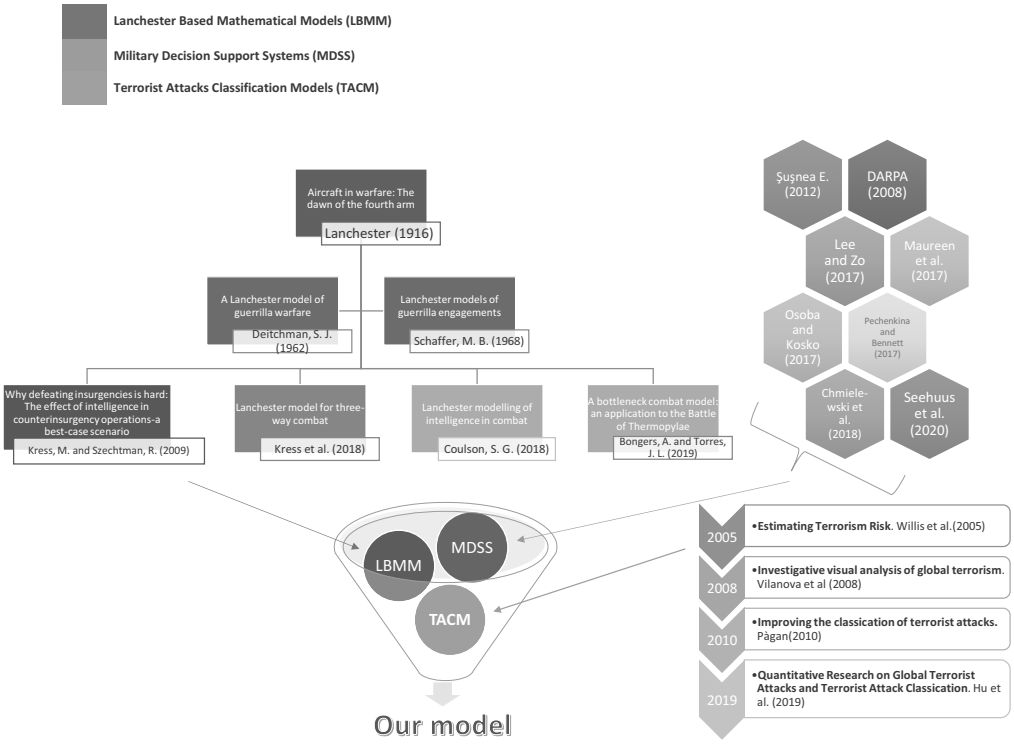

Fig. 1. Related works.

the key notions of terrorist risk (Willis *et al*., 2005), highlights the main classes handled by our model, and precisely identifies the characteristics of targets without abandoning the generic aspect.

3.2. Terrorist attack classification. Classifying terrorist attacks is difficult since they are influenced by various real-world variables and parameters. Hence, regarding the concept of the proactive strategy and using ATiPreTA to anticipate consequences, we offer a new classification of terrorist attacks referring to the nature of terrorist risks. We base our method of classification on two principal rules: (a) the threat level of the assaults and (b) the vulnerability level of the target. Hence, as our starting point, we choose to rely on the definition by Willis *et al*. (2005), who quantify the terrorist risk as the product of the occurrence probability of a terrorist attack (threat), the probability that an attack of a given type will be successful once it has been launched (vulnerability), and the expected value of the distribution of damage (consequences).

We highlight that we are not using consequences as a parameter of classification. In our classification, which is useful for victim-estimation models since its criteria are linked to real-time situations, we deal with attacks after their occurrence and with those that are ongoing. The threat level of an attack depends on terrorists' effectiveness and capacity to cause damage to a specific target. This effectiveness arises from several factors. For example, a terrorist with only assault weapons presents a medium threat level, but it increases with a suicide bomber. That is why we use the types of weapons as a factor to define the level of threat.

In addition, a large number of terrorists could present an important threat even if the individual risk of each one is low. The size of the terrorist group is the second factor. It has a major impact on the threat level. In our case, a terrorist group's strategy in an urban area involves fast concentrated attacks, which maximizes the chances of achieving the desired damages. This strategy does not require a large number of terrorists as they need discretion. In ATiPreTA, we are working with a small number of terrorists along with high and medium threats (see Fig. 2).

A quantification based on threat is focused on a specific type of a certain level of threat on specific targets. We cite three examples of the effect of the same threat on specific targets:

- A bombing attack represents a different threat to a specific target than a chemical attack.
- Attacks on stadiums represent a different threat from attacks on military bases.
- A terrorist armed with a white weapon presents a

lower threat to government forces than for a civil population.

A complete classification of terrorist attacks based on threats only would require consideration of every target separately (Kebir *et al.*, 2020b; 2020d). In practice, however, we must focus on a limited number of attack types, which leads us to consider the vulnerability of a target as an additional scale to recognize the capacity of a target to respond to a specific threat. As shown in Fig. 2, the vulnerability criterion increases from a low to a high level based on the defensive capabilities of the target. For example, military bases are less vulnerable than a police patrol because they have a higher chance to resist a given type of attack. Crowded places with many civilians in urban areas are among the most vulnerable terrorist targets. We consider that kind of target exposed to medium or high threat (Classes 6 and 9 in Fig. 2). Figure 2 illustrates the proposed classification and shows some examples of terrorist attacks from the GTD using different levels of threat and vulnerability. The variation of shades from lighter to darker shows the increasing probability of losses such as the and fatalities, numbers of injuries, and the total property damage in dollars (buildings, building contents, and business interruption). Every class in this scale has a number from 1 to 9 for better recognition.

In the following subsection, we present an analytical model for time-dependent prediction of terrorist attacks that treats attacks under Classes 6 and 9 (see Fig. 2) of our proposed classification strategy.

3.3. Analytical model for time-dependent prediction of terrorist attack behaviors.

Let G, T, and P denote the sizes of government forces, terrorists, and a general population, respectively. $G(t)$, $T(t)$, and $P(t)$ represent their corresponding sizes at instant t. We assume that $G(t)$ and $T(t)$ may vary over time in minutes and that the size of a general population $P(t)$ decreases throughout. We denote by N the fraction of well-trained terrorists in defensive positions, where the effectiveness of each is equal to that of three untrained terrorists (Aylwin-Foster, 2005), as mentioned in the previous section.

Let us normally explain Assumption A3 by creating a combat-multiplier factor called CF as follows:

$$3NT + (1 - N)T = (2N + 1)T = \text{CF} \times T. \quad (1)$$

As the first phase within attacks (Fig. 3), terrorists kill civilians in the absence of any government force. Therefore, we model the number of civilian victims per one minute (VP), during this phase, with the following linear function:

$$\text{VP} = \lambda \text{CF} \times T(0), \quad (2)$$

where λ is the attrition coefficient defined as the rate at which terrorists inflict casualties on civilians. We

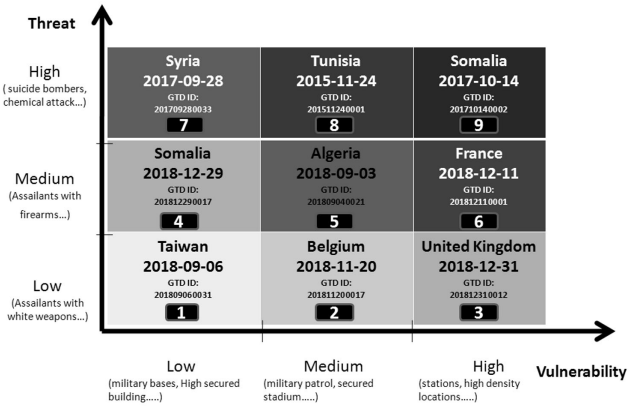

Fig. 2. Classification of terrorist attacks.

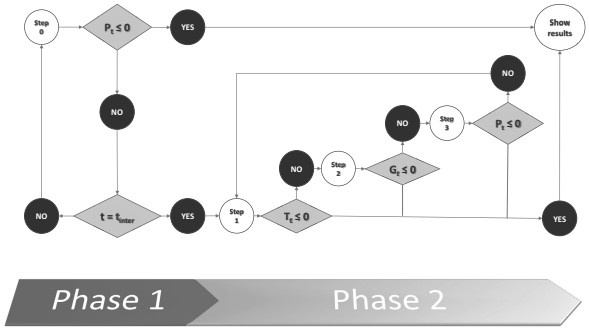

Fig. 3. Logic diagram of ATiPreTA.

define t_{inter} as the starting time of government forces' intervention. The initial number of a population $P(0)$ at $t_0 = 0$ decreases massively and reaches the population number $P(t_{\text{inter}})$. While t $\in [t_0, t_{\text{inter}}]$, terrorists murder civilians without any presence of government forces ($G = 0$); this is a favorable situation for terrorists because they suffer no losses. Consequently, at the end of this phase, the population size is formally modeled as follows:

$$P(t_{\text{inter}}) = P(0) - \sum_{t_0}^{t_{\text{inter}}} \text{VP}. \quad (3)$$

In the second phase in real-world attacks as well as within ATiPreTA (Fig. 3), there is a high interaction between the different actors. We study the dynamic interaction between government forces, as well as terrorists, and their effect on the number of victims. During this phase, terrorists focus their efforts on neutralizing government forces as their primary target. In this analysis, we follow the systematic steps of ATiPreTA detailed in Figs. 4 and 5.

First (Step 1 of Phase 2 in Fig. 5), government

forces intervene to neutralize terrorists (Assumption A1). Following the model of Kress and Szechtman (2009), which describes the effect of intelligence on the recruitment rate of terrorists, we use a similar equation to describe government forces' effect on terrorists, such that

$$\mathrm{VT}(t) = \gamma G(t-1)\left[\mu(t) + (1-\mu(t))\frac{T(t-1)}{P(t-1)}\right], \quad (4)$$

where

- γ is the attrition coefficient interpreted as the general intensity and effectiveness of counter terrorism operations;
- $\mu(t) \in [0,1]$ is the parameter that defines the average rate of information obtained about terrorists in instance t of the operation; besides, the Kress model (Kress and Szechtman, 2009) reflects the ability of terrorists to blend into a civilian population when not actively engaged in attacks;
- the ratio $T(t-1)/P(t-1)$ presents the signature of terrorists, which may be interpreted as the probability that a randomly selected target is a terrorist (Kress and Szechtman, 2009).

There is a logic link between the population density $P(t-1)$ and the signature of government forces on terrorists $\mathrm{VT}(t)$. The more government forces, the higher the density of a population and the weaker the possibility of detecting terrorists. Moreover, the effectiveness of government forces is lower in crowded places (Aylwin-Foster, 2005). Consequently, we use the reciprocal of $P(t-1)$ to model this assumption. Without intelligence, government forces have information on terrorists (Kress and Szechtman, 2009) ($\mu(t) = 0$) and we obtain

$$\mathrm{VT}(t) = \gamma G(t-1)\frac{T(t-1)}{P(t-1)}. \quad (5)$$

Thereafter, the parameter $\mu(t)$ increases linearly with a constant time step (step_μ) until they will have perfect intelligence ($\mu(t) = 1$). Moreover, if we change the size of step_μ (the amount by which μ increases), the intelligence level obtained after a specific time will change in the same way (Assumption A2). Consequently, the size of incrementation has a major impact on the effectiveness of government forces. When $\mu(t) = 1$, we obtain the following relation similar to the classical Lanchester square law of aimed fire (Lanchester, 1916):

$$\mathrm{VT}(t) = \gamma G(t-1). \quad (6)$$

Secondly (Step 2 of Phase 2 in Fig. 5), we model terrorist behaviour toward government forces. Let us

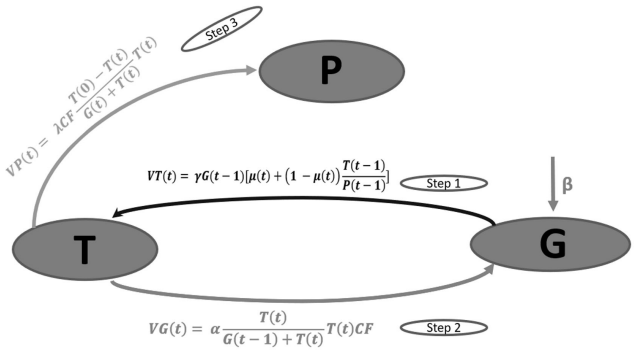

Fig. 4. Three steps of the scenario's second phase.

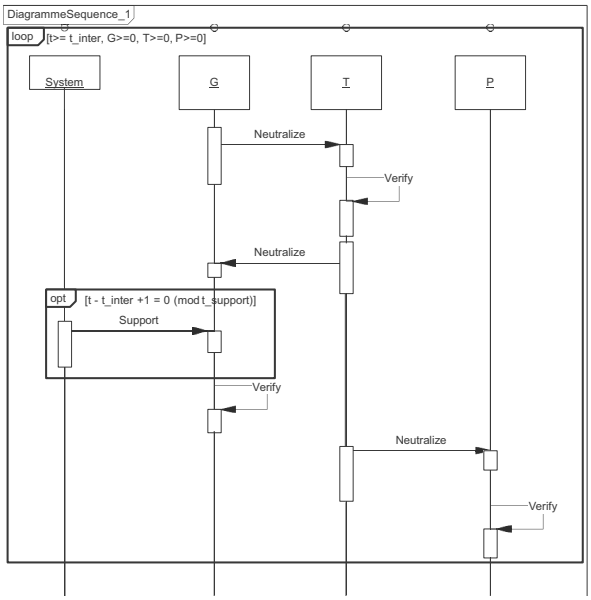

Fig. 5. Sequence diagram of the three steps of the scenario's second phase.

denote by $\mathrm{VG}(t)$ the number of victims of government forces and by α the attrition coefficient interpreted as the general intensity and effectiveness of terrorist operations on government forces. We formally model this idea as follows:

$$\mathrm{VG}(t) = \alpha\frac{T(t)}{G(t-1)+T(t)}T(t)\mathrm{CF}. \quad (7)$$

Generally, the more terrorists perceive the weakness of government forces and their decreasing number, the more they win in terms of increased effectiveness (if $G(t-1)$ increases, then $T(t)/(G(t-1)+T(t))$ decreases). Furthermore, if the number of terrorists decrease, they will be exposed to a higher level of stress termed focused stress and their effectiveness will be enhanced (if $T(t)$

decreases, then $T(t)/(G(t-1)+T(t))$ increases). For example, terrorists under stress commit acts of bravery and acts of heroism (Army, 2006). We summarize those hypotheses by the factor $T(t)/(G(t-1)+T(t))$. If $G(t-1)+T(t)$ varies over time, the latter factor will change in the opposite sense.

After a predefined time t_{support}, government forces will be periodically supported by a constant aid called β. This part is developed in Fig. 5:

$$G(t) = \begin{cases} \text{Val} + \beta & \text{if } t - t_{\text{inter}} + 1 \equiv 0 \pmod{t_{\text{support}}}, \\ \text{Val} & \text{otherwise}, \end{cases} \tag{8}$$

with $\text{Val} = G(t)$.

Such support has a strong influence on the scenario direction and then governmental forces will be effective against terrorists (Assumption A2). This situation will evolve during the operation and is manifested by the decreasing number of victims and the increasing number of neutralized terrorists.

Thirdly (Step 3 of Phase 2 in Fig. 5), we simulate the effect of terrorists on a population in the second phase. For that purpose, we propose a new coefficient in the mathematical equation for $\text{VP}(t)$ as follows:

$$\text{VP}(t) = \lambda \text{CF} \frac{T(0) - T(t)}{G(t) + T(t)} T(t). \tag{9}$$

We model two opposing facts by using the coefficient $T(0) - T(t)/(G(t) + T(t))$. On the one hand, terrorists will be less harmful to a population during government forces' intervention because they have limited human resources and their number is decreasing over time ($T(t-1) \geq T(t)$), faced with government forces' neutralization efforts. Conversely, terrorists called "inghimasi", who are ideologically similar to suicide attackers, generally make attacks in urban areas. When such terrorists lose hope and governmental forces eliminate some of them, they often forgo elementary self-preservation concerns (Janis and Mann, 1977) to do greater damage to a population as an act of revenge. We model the previous certainties by introducing the factor $(T(0) - T(t))/(G(t) + T(t))$, where $G(t) + T(t)$ presents the first fact and $T(0) - T(t)$ represents the second. Figures 4 and 5 summarize the three steps of the scenario's second phase.

To help government forces to be equally prepared for the risk, we presented the previous model that provides a perspective on terrorist attacks using many parameters. Actually, estimating each of them is a challenging task because the effectiveness of each component is subject to tremendous uncertainties. As we try to facilitate an estimation of victim numbers, it is critical to highlight the important sources of effects on a population and to validate ATiPreTA using the mean squared error (MSE) and the Pearson correlation coefficient *r* as developed in the following section.

Table 1. Ranges of parameters in terms of threats and vulnerabilities.

		Low	Medium	High
Threat	λ	[0,0.2]	]0.2,1]	]1,5]
	γ	[3,5]	]0.2,3[	]0,0.2]
	α	[0,0.1]	]0.1,2.5]	]2.5,5]
	N	0	]0,0.6]	]0.6,1]
	t_{inter}	[0,5]	]5,20]	]20,500]
	$T(0)$	1	]1,8]	]8,500]
Vuln.	t_{support}	[0,15]	]15,25]	]25,100]
	β	[20,100]	]10,20]	]10,0]
	$G(0)$	[0,15]	]15,20]	]20,500]
	$P(0)$	[0,15]	]15,35]	]35,500]
	$\mu(0)$	[0.7,1]	[0.4,0.7[	[0,0.4[
	step_μ	[0.03,1]	[0.01,0.03[	[0,0.01[

4. Research questions

To validate our model along with the terrorist attack classification strategy, in Section 4.1 we undertake an experimental analysis using several evaluation criteria. In Section 4.2, we study the parameter settings which influence the resulting class assigned to terrorism attacks. Then, we discuss the obtained results in Section 4.4. To simplify the calculation and to be more realistic, in this section, we use the outputs presented as real numbers.

4.1. Experimental environment. In Section 3.2, we developed a subjective classification of terrorist attacks which is governed by two criteria: threat and vulnerability. In this section, we aim to validate Assumption A6 by highlighting the relation between the proposed classification and ATiPreTA. Therefore, we dissociate those criteria into qualitative numerical parameters extracted from ATiPreTA. Our prediction model includes parameters that have an impact on two basic classification criteria: terrorist threat and victim vulnerability. Each criterion is influenced by a parameter, and the degree of influence varies from one parameter to another. For example, on the one side, the initial size of a population $P(0)$ has a direct impact on the vulnerability level of targets. Conversely, it indirectly influences terrorists' threat level according to Eqn. (4). We assume that a parameter is attributed to a criterion only if it has a direct and high level effect, as will be shown below. Besides, we do not consider the effect of any correlation between parameters on the criterion. To rate those parameters using the different scales shown in Table 1, we elicited knowledge, for evaluation, from experts of the field. Then, we used the results of multiple executions of the simulation to validate them. Thus, we were able to choose the range of each parameter. The obtained intervals become the benchmark for simulation

users to select parameters according to the class of the terrorist attack.

To quantify the two criteria of the proposed classification, the experts used 12 parameters of ATiPreTA. We set λ, α, γ on a scale between 0 and 5, where t_{inter}, t_{support}, $G(0)$, β, $P(0)$ and $T(0)$ vary between 0 and 500. Besides, the parameters N, $\mu(0)$, and step_μ were set between 0 and 1. The range of values, cf. Table 1, shows the increasing level of the threat and the vulnerability in terms of those parameters.

To extract the values of the parameters related to the two terrorist attacks used for validation, we aim to analyze their real operational circumstances, as presented in the following subsection (Tables 2 and 3).

4.2. Parameter settings. First, let us briefly describe facts that happened during a real terrorist attack SA in Tunisia, when 38 persons were killed. The terrorist in question stalked through a Tunisian beach resort in Sousse. He killed people on the beach and then moved into the grounds of a five-star hotel, picking off tourists by the pool, near the lobby and in the parking area. After 22 minutes, government forces intervened and neutralized him eight minutes later in a street near the hotel. Superposing information extracted from our confidential sources onto the attack process, we conclude that even if the terrorist received good training in Libyan hotbeds of tension so that $N = 1$, he would not have significant impact on government forces. Referring to the number of victims, we assume the terrorist's high impact on a population. Based on our information, government forces had some knowledge of the terrorist before their intervention. Table 2 presents the different parameters used to simulate this attack. Those parameters are obtained by analysing the real circumstances of the attack.

Second, a summary is presented of what happened during a real terrorist attack BA. Three assailants attacked tourists at the Bardo National Museum in Tunis City, Tunisia. The assailants first opened fire on people in buses outside the museum. The hostages were rescued several hours later. At least 21 civilians and a policeman were killed. After 15 minutes, government forces intervened. Terrorists were trained in Derna, Libya. This city was controlled by Islamic groups that proclaimed loyalty to the Islamic State. After two hours and 30 minutes, two terrorists were neutralized and one third are currently at large. Based on this information, we use the parameters presented in Table 3 to simulate the BA. Then, we obtained, from different sources, some statistical results about the real characteristics of a population, government forces, and terrorists during the course of action. We note that these data have never been mentioned or used previously in a scientific paper. We present them, for the first time, in Table 4, where we show government forces,

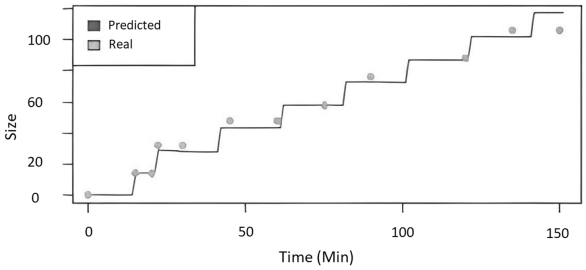

Fig. 6. Real and predicted size of government forces (BA).

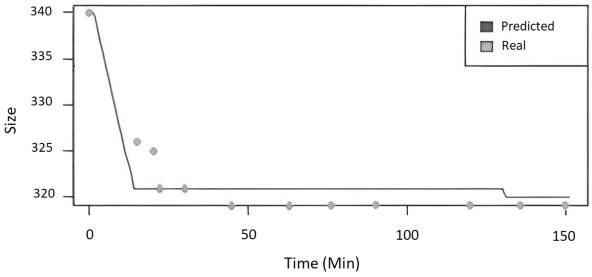

Fig. 7. Real and predicted size of a population (BA).

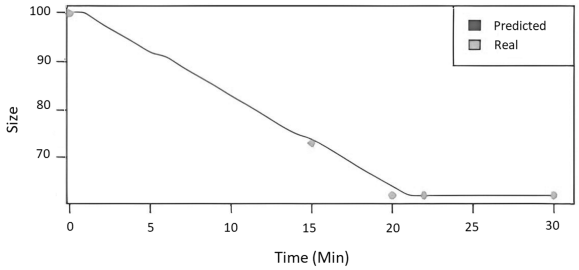

Fig. 8. Real and predicted size of a population (SA).

the number of terrorists, and the size of a population in a five-point time sequence for the SA and a twelve-point time sequence for the BA.

After mentioning the real data used for the experimental analysis, we ran our model to predict the numbers of the three actors in question (G, T, and P) and compare them with real metrics in both attacks. Hence, we show some results in Figs. 6–8, where we note an almost perfect match of values (the next subsection will be devoted to discussing the results).

Once applying ATiPreTA using data for prediction, we use now evaluation criteria to assess and estimate the quality of our simulation results.

4.3. Performance metrics. For the first part of the evaluation, the following two criteria are used:

- *Mean squared error (MSE):* The MSE criterion measures the average of the squares of the errors. These errors refer to the differences between the estimated numbers of the different actors and their

Table 2. Parameter settings used for the Sousse attack simulation.

Parameters	Values	Argumentation
N	1	The terrorist receives good training in Libyan hotbeds of tension.
$G(0)$	15	The initial number of government forces intervening during the attack.
$P(0)$	100	An average number of civilians in range of the terrorist.
$T(0)$	1	Only one terrorist committed the attack.
α	0.06	The terrorist presents a low level of threat to government forces due to his location when they intervene.
λ	0.63	The terrorist presents a medium level of threat to civilians because he is only armed with an assault rifle and not a weapon of mass destruction or explosives.
γ	0.006	The targets were tourists on a beach and are considered high vulnerability targets.
β	0	There was no support until the end of the mission.
step_μ	0.05	Due to the many witnesses, we obtain a significant volume of information. Therefore, we use a large incremental step of intelligence.
$\mu(0)$	0.5	Government forces have initial information about the attack due to two policemen present from the beginning of the attack.
t_{inter}	22	Real time of intervention.
t_{support}	–	There is no support.

Table 3. Parameter settings used for the Bardo attack simulation.

Parameters	Values	Argumentation
N	0.6	Only two terrorists receive good training in Libyan hotbeds of tension.
$G(0)$	14	The initial number of government forces that intervened.
$P(0)$	340	The number of civilians present in the museum.
$T(0)$	3	
α	0.04	The terrorist presents a low level of threat to government forces due to his location when they intervene.
λ	0.22	The terrorist presents a medium level of threat to civilians because he is only armed with an assault rifle and did not use a weapon of mass destruction or explosives.
γ	0.0005	Targets are tourists in a crowded museum which are considered high vulnerability targets.
β	15	There was no support until the end of the mission.
step_μ	0.0065	Due to the panic and contradictory information sources, we use a small incremental step for intelligence.
$\mu(0)$	0	Government forces have no initial information about the attack.
t_{inter}	15	This is the conventional time for intervention. The attack occurred close to several bases.
t_{support}	20	Information extracted from the course of action.

Table 4. Real information about terrorist attacks.

Time (min)		0	15	20	22	30	45	60	75	90	120	135	150
Sousse attack	G	0	0	0	15	15							
	T	1	1	1	1	0							
	P	100	73	62	62	62							
Bardo attack	G	0	14	14	27	27	48	48	58	76	88	106	106
	T	3	2	2	2	2	2	2	2	2	2	1	0
	P	340	326	325	321	321	319	319	319	319	319	319	319

real dynamic values during the attack in time (Chai and Draxler, 2014). The MSE is a risk function corresponding to the expected value of the squared error loss. Let us define $a(t)$ and $p(t)$ respectively as the estimated and the observed values over time and n as the number of observations. Table 5 shows the scale of every component during the attacks obtained by the MSE. This criterion is defined as follows:

$$MSE = \frac{1}{n}\sum_{t=0}^{n}(a(t) - p(t))^2. \tag{10}$$

- *Pearson's correlation coefficient (r):* This criterion refers to the linear association between two sets of values (e.g, real and predicted). It provides a coefficient bounded between -1 and 1 and implies a linear equation that perfectly describes the relationship between the predicted value a_t and the real value p_t (Benesty *et al.*, 2009). A value of 1 implies that all data points lie on a line for which a_t increases as p_t increases. The value -1 implies a totally negative correlation where p_t increases when a_t decreases by the same amount. A value of 0 implies that there is no linear correlation between the variables. If A and P present the two sets of values over time referring, respectively, to the predicted and real data, Pearson's correlation coefficient $(r_{_{AP}})$ is therefore defined as follows:

$$r_{_{AP}} = \frac{\sum_{t=1}^{\text{NbT}}(a_t - \overline{a})(p_t - \overline{p})}{\sqrt{\sum_{t=1}^{\text{NbT}}(a_t - \overline{a})^2}\sqrt{\sum_{t=1}^{\text{NbT}}(p_t - \overline{p})^2}}, \tag{11}$$

where a_t and p_t are the values from A and P, respectively, at instant t, 'NbT' presents the number of instances taken into account for a terrorist attack, and $\overline{a}$ and $\overline{p}$ are their mean values.

The results obtained according to the above evaluation criteria are shown in Table 5 and discussed in the next subsection.

4.4. Results, analysis and a discussion. Our proposed model is developed using the R software for statistical computing. In terms of results, Figs. 6–8 show three plots intended to compare real data with those predicted by ATiPreTA regarding the scale of government forces during BA, a population during the BA, and a population during the SA, respectively. In fact, the links between our six assumptions presented in Section 3.1 and the obtained results are obvious. It is also clear, in these figures, that casualties decrease when government forces intervene. This due to terrorists' conduct, which implies that for government forces terrorists are their primary target that must be neutralized. Moreover, the staircase shape of the predicted size of government forces in Fig. 6 is due to the constant support mentioned in Assumption A2. In the case of the BA, the scale of support has a greater effect than terrorists on government force numbers during a counter-terrorism action.

In addition, Table 6 shows that the ATiPreTA process prevailed in terrorists being killed in the BA and SA. This result calls attention to Assumption A5. The real results are presented in point form because we do not have immediate information on the entire attack. Besides, the outputs of our model are real numbers, but to be more realistic, we have chosen to round them off to integers (as is the case with the values within Table 4).

In terms of the two evaluation criteria used, the results, as shown in Table 5, highly support our proposal. This table offers prediction results obtained by ATiPreTA according to the mean squared error and Pearson's correlation coefficient analyses as well as over five instances for the Sousse attack and twelve instances for the Bardo attack. The mean values of both the criteria have also been calculated.

We remark, from Table 5, that the results also highly support our proposal. For instance, we note that the MSE values are null for both the government (G) and terrorist (T) variables for the Sousse attack. Actually, the best results are reached when the MSE is closest to zero.

Regarding the second evaluation criterion, for both attacks, we note a very high correlation average among the three actors, where the mean r is equal to 0.999 $(\simeq 1)$ for the Sousse attack and 0.934 for the Bardo attack. This supports ATiPreTA and reflects its validity since results mention a good match between the predicted and real values.

Even though we succeed in proving our model's effectiveness, our estimator may not be the most representative terrorist-attack model. This dilemma is due to the variety of scenarios during attacks. We acknowledge that we could not meet all the challenges of tracking terrorism through scenario generation and structuring with only a single model or methodology.

Moreover, integrating intelligence awareness during intervention and the psychology of terrorist behavior and its effects on targeting victims have assigned a greater value to ATiPreTA as a well-established risk-based methodology. We could say that ATiPreTA is a useful tool with a creative aspect. In the next section, we select the parameters with a high impact on the number of victims.

In our case, the large number of parameters is a positive factor because it allows various scenarios to be simulated. The performance of the method is tested for two reasons: the scarce information sources and the secrecy in this field. Hence, we tested ATiPreTA on two real cases that we were able to collect and provide. In this paper, our proposed model treats the increasing number of government forces as a step function.

Table 5. MSE and r in terms of the numbers of actors during attacks.

Time (min)		0		15		20		22		30		45		60		75		90		120		135		150		MSE	Mean MSE	r	Mean r
Actor' size		$a(t)$	$p(t)$	$a(t)$	$p(t)$	$a(t)$	$p(t)$	$a(t)$	$p(t)$	$a(t)$	$p(t)$	$a(t)$	$p(t)$	$a(t)$	$p(t)$	$a(t)$	$p(t)$	$a(t)$	$p(t)$	$a(t)$	$p(t)$	$a(t)$	$p(t)$	$a(t)$	$p(t)$				
Sousse attack	G	0	0	0	0	0	0	15	15	15																0		1	
	T	1	1	1	1	1	1	1	1	0	0															0	0.33	1	0.999
	P	100	100	74	73	64	62	62	62	62	62															1	3.95	0.997	0.966
Bardo attack	G	0	0	14	14	14	29	27	28	27	43	48	43	48	58	58	73	76	87	88	102	106	117	106	16.83			0.994	
	T	3	3	3	2	3	2	2	3	2	3	2	3	2	3	2	3	2	2	2	1	1	0	0	0.66	7.58		0.887	0.934
	P	340	340	321	326	321	325	321	321	321	321	319	321	319	321	319	321	319	319	321	320	319	320	319	5.25			0.922	

4.5. Sensitivity analysis. In this section, we analyse the stability of ATiPreTA through discussing the effect of modifying the input values on the final victim numbers $\mathrm{VP}(t_{\text{final}})$ and on the time needed for the process to end t_{final}; cf. Assumption A5.

4.5.1. Testing strategy. To visualize the effect of each variable separately, we follow a three-step process in this analysis. The process allows us to study the sensitivity of the inputs by modifying them individually ("one-at-a-time": OAT) (Saltelli and Annoni, 2010); the others remain fixed at a nominal value.

As the first step we select the real case that was simulated in Section 4. To obtain more useful results, we choose to perform our sensitivity analysis on the BA. For the second step, we fix the values of all the input parameters at a nominal value for the selected real case excepting the targeted parameter, which varies over its prescribed range in Table 1. In the third step, ATiPreTA is executed for each value of the targeted parameter till the number of terrorists, a population or government forces reaches zero; cf. Assumption A5. In each run, the results of three types of sensitivity criteria are saved to identify those with the greatest impact on the number of victims and on the time needed for the process to end:

- The first sensitivity criterion is the variation produced by ATiPreTA shown in the first and third columns of Table 6. The values are obtained by subtracting the greatest lower bound from the least upper bound of the variation range. For example, if we run ATiPreTA with varying N in its range in Table 1, the number of victims varies in $[9.63, 28.92]$. The amplitude of the interval of the number of victims presents the victim variation for N shown in the first column of Table 6.

- The second sensitivity criterion is the variance of $\mathrm{VP}(t_{\text{final}})$ and t_{final}. If a variance is equal to zero, then this means that all observations are equal to their values' mean, implying that there is no variation. Conversely, the higher the variance, the greater the dispersion of observations. The different variance values are shown in Columns 2 and 4 of Table 6.

- The last evaluation criterion is the average speed of the first criterion in relation to the variation of the inputs. First, we calculate the instantaneous speed S_{inst}, which refers to the derivative for each i-th execution of ATiPreTA:

$$S_{\text{inst}}(i) = \frac{\text{output}(i) - \text{output}(i-1)}{\text{input}(i) - \text{input}(i-1)}. \tag{12}$$

Then, we obtain the average speed by calculating the mean of the instantaneous speeds. This gives us an

Table 6. Sensitivity data.

	Variation	Variance of the number of victims	Variation in the scenario duration	Variance of the scenario duration	Average speed of victim variation	Average speed at which the scenario duration varies
$\mu(0)$	0.4828306	0.02629627	35	147.4727	0.4828306	-35
α	1.114241	0.06946913	156	1541,833	-0,1711104	-28
β	12.34544	2.017563	320	1873.345	-0.02469096	-0.64
λ	338.97	13374.08	160	4755.278	67.79401	-29,6
N	19.29107	40.94239	1	0.2727273	19.29107	1
t_{inter}	337.6689	11592.51	266	2390.2	0.6766912	0.1783567
$T(0)$	333.15	3294.167	374	1280.341	0.6676352	-0.1883768
$G(0)$	0.9696636	0.04742185	151	617.7992	0.000124353	0.11
$step_\mu$	0.4655029	0.01813684	17	26.05455	0.4525413	-17
$P(0)$	22.66085	8.00012	193	1012.49	0.04531443	0.308
t_{support}	5.32197	2.399035	219	2943.568	0.0532197	2.19
γ	1.352601	0.09922564	44	45.28314	-0.2705202	-8.8

idea of the rate of variation in the outputs relative to the inputs. The average speeds are shown in the 5-th and 6-th columns of Table 6.

4.5.2. Variation analysis. In this subsection, we establish a connection between the numerical results of Table 6 and their interpretations in reality. Figure 9 shows that, when we vary t_{inter}, $T(0)$ or λ, the amplitude of the interval of the number of victims reaches high values. The intervals vary with amplitudes of 337.6689, 333.15 and 338.98 (Table 6).

We conclude that the initial number of terrorists $T(0)$, their capability of inflicting severe damage on their targets (λ), and the time needed for the first response to the attack (t_{inter}) are the criteria that have a major impact on the final victim numbers VP(t_{final}). As shown in Fig. 9, a fast response to terrorist attacks saves lives and allows us to control the situation and limit material damage. For that reason, modifying t_{inter} greatly affects the numbers of victims. In the case of the Bardo attack, a slow and delayed response led to a total loss of a civilian population targeted by terrorists. This hypothesis is the wide amplitude of the victim range that reaches 337.6689.

The duration of the mission t_{final}, in the second column of Table 6, is highly influenced by changing t_{inter} and $T(0)$. These two inputs have maintained their influential weight. In addition, although the effect of the size of the periodic support β is limited after the intervention of government forces, we note that its impact on t_{final} is interesting. We also find that the size supporting forces β and the debit of their support during the mission t_{support} highly influence the mission duration, whereas they have negligible influence on the number of victims. We notice that the size of the support forces β and the reduction of their support t_{support} during the mission highly influence the mission duration, while being negligible on the numbers of casualties. Thus, we assume that those parameters also impact the numbers of government forces and terrorists.

Figure 9 shows that β has a wider range of variation in the scenario duration than t_{support} (320 and 219, respectively). However, the average speed of this variation is higher for t_{support} in Table 6, which means that the size of supporting forces has a impact than their supporting debit.

4.5.3. Variance analysis. We have already explained the meaning of variance in the description of our sensitivity analysis. We visualize that the casualty count has a high variance (13374.08) with a high average speed (67.794) when we vary λ. We conclude that it rapidly increases when λ increases.

Table 6 shows that the variance of the number of victims is also high when we vary t_{inter} and $T(0)$ (11592.51 and 3294.16, respectively). Otherwise, their average speed is low (0.67 and 0.66, respectively). We conclude that the number of victims increases until a certain threshold is reached. At this threshold, the increase in the input has no effect on the casualty count.

We highlight that the variance of the scenario duration is important for variations for all inputs except for parameter N. The effect of N is stable since an increase in the degree of the training of terrorists can only lead to a weighted increase in their efficiency, which implies a similar effect on the duration of the mission.

4.5.4. Average speed variation analysis. By analyzing the variation in the average speed, we gain insight into two issues. The first small variation regards the average sensitivity of the outputs to the

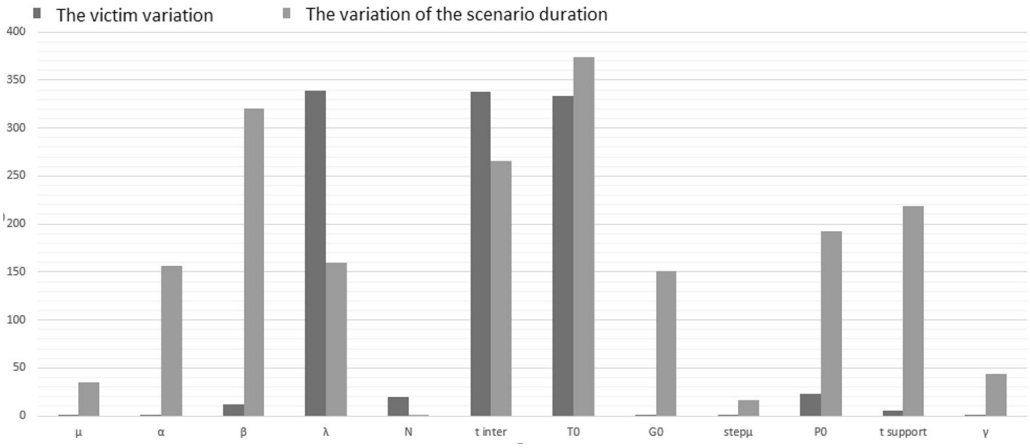

Fig. 9. Variations the number of victims and the scenario duration (BA).

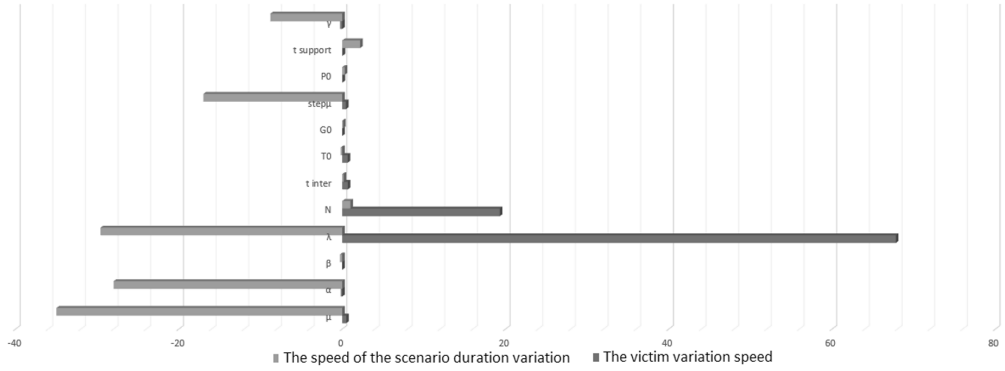

Fig. 10. Average speed of the variation in the number of victims and the scenario duration (BA).

input throughout the interval. We notice that if the interval of the output parameter variation is important and the average speed of this variation tends toward approximately zero, then the value of the output varies exponentially. Yet, if the average speed is also important, then the output value varies linearly. The second issue is about the direction of variation in the outputs. If we have a positive speed, this means that an increase in the values of the inputs implies an increase in the values of the outputs, and vice versa.

As shown in Fig. 10, the rate at which terrorists inflict casualties on a civilian population λ has the highest positive average speed among the number of victims and a high range of the number of victims, presented in Fig. 9. We conclude that a small variation in λ involves a constant increase in the number of victims throughout the input range. Actually, even if there is a high variation in the output intervals for t_{inter}, the average speed for those variations is positive and around zero.

We conclude, also, that a small variation in t_{inter} involves an exponential modification of the number of victims and the duration of the event. Besides, we note that β and t_{support} have an opposite effect on our output criteria because their average speeds have opposite signs. Finally, once we analyzed the sensitivity of our model, we noted that it is coherent when we vary the input parameters over all their ranges, and that some input parameters have greater impacts than others.

5. Conclusion

The goal of designing ATiPreTA lies in being able to predict the size of actors during a terrorist attack taking into account different parameters. This model allows decision makers to estimate the number of victims and predict scenarios to begin their own planning. We note that our work could be a cornerstone for a future active DSS that produces real-time solutions for decision makers during terrorist attacks.

We first reviewed several related research works and noted that most mathematical methods are static. Therefore, ATiPreTA blended mathematical equations

with a dynamic aspect. The actors' relations are described by the proposed equations of interaction analysis. The courses of action in these dynamic scenarios are based on our military knowledge. Therefore, ATiPreTA provides a mechanism which follows military planning concepts and rules.

Finally, we analyzed the sensitivity of ATiPreTA to variants of the input parameters. We conclude that the most influential factors in a terrorist attack scenario are the initial size of terrorist forces, their effectiveness, and the time elapsed till a first government force reaction. In addition, we found that the effectiveness of terrorists depends on their force size and level of training. For that reason, a small number of terrorists could severely damage their adversary's lines. Similarly, the effect of other parameters could not be ignored due to the importance of human lives.

The results extracted from ATiPreTA are reasonable for all inputs modified within their prescribed ranges in Table 1. Hence, the use of ATiPreTA to support decision making for predicting 650 terrorism events is an adequate alternative for some types of terrorist attacks.

In future work, we plan to integrate other parameters that handle irregular conflicts. Furthermore, we aim to integrate ATiPreTA, as an intelligence agent, in a multi-agent model for countering terrorism (Kebir *et al.*, 2020a). This agent predicts the casualty count in different cases and compares it with the results obtained from the multi-agent model to refine the process.

References

Army, U.S. (2006). *Field Manual 4-02.51: Combat and Operational Stress Control*, Department of the Army, Washington DC.

Aylwin-Foster, N.R.F (2005). Changing the army for counterinsurgency operations, *Military Review*: 27–40.

Benesty, J., Chen, J., Huang, Y. and Cohen, I. (2009). Pearson correlation coefficient, *in* J. Cohen *et al.* (Eds), *Noise Reduction in Speech Processing*, Springer, Berlin/Heidelberg, pp. 1–4.

Bongers, A. and Torres, J.L. (2019). A bottleneck combat model: An application to the Battle of Thermopylae, *Operational Research* **21**: 2859–2877, DOI: 10.1007/s12351-019-00513-0.

Chabir, K., Rhouma, T., Keller, J.Y. and Sauter, D. (2018). State filtering for networked control systems subject to switching disturbances, *International Journal of Applied Mathematics and Computer Science* **28**(3): 473–482, DOI: 10.2478/amcs-2018-0036.

Chai, T. and Draxler, R.R. (2014). Root mean square error (RMSE) or mean absolute error (MAE), *Geoscientific Model Development Discussions* **7**(1): 1525–1534.

Chmielewski, M., Kukie, M., Fr, D., Kukiełka, M., Frąszczak, D. and Bugajewski, D. (2018). Military and crisis management decision support tools for situation awareness development using sensor data fusion, *in* J. Świątek *et al.* (Eds), *Information Systems Architecture and Technology: Proceedings of the 38th International Conference on Information Systems Architecture and Technology, ISAT 2017*, Springer, Cham, pp. 189–199.

Coulson, S.G. (2018). Lanchester modelling of intelligence in combat, *IMA Journal of Management Mathematics* (2): 149–164.

Deitchman, S.J. (1962). A Lanchester model of guerrilla warfare, *Operations Research* **10**(6): 818–827.

El-Douh, A.A.-R., Lu, S.F., Elkouny, A.A. and Amein, A. (2022). Hybrid cryptography with a one-time stamp to secure contact tracing for COVID-19 infection, *International Journal of Applied Mathematics and Computer Science* **32**(1): 139–146, DOI: 10.34768/amcs-2022-0011.

Gambo, A. (2020). Mathematical modeling of dynamics behavior of terrorism and control, *Caspian Journal of Mathematical Sciences* **9**(1): 68–85.

Hu, X., Lai, F., Chen, G., Zou, R. and Feng, Q. (2019). Quantitative research on global terrorist attacks and terrorist attack classification, *Sustainability* **11**(5): 1487.

Janis, I.L. and Mann, L. (1977). Emergency decision making: A theoretical analysis of responses to disaster warnings, *Journal of Human Stress* **3**(2): 35–48.

Junosza-Szaniawski, K., Nogalski, D. and Rzążewski, P. (2022). Exact and approximation algorithms for sensor placement against DDoS attacks, *International Journal of Applied Mathematics and Computer Science* **32**(1): 35–49, DOI: 10.34768/amcs-2022-0004.

Kebir, O., Nouaouri, I., Belhadj, M. and Ben Said, L. (2020a). A multi-agent model for countering terrorism, *in* H. Fujita *et al.* (Eds), *Knowledge Innovation Through Intelligent Software Methodologies, Tools and Techniques: Proceedings of the 19th International Conference on New Trends in Intelligent Software Methodologies, Tools and Techniques (SoMeT_20)*, IOS Press, Amsterdam, p. 260.

Kebir, O., Nouaouri, I., Belhadj, M. and Bensaid, L. (2020b). A multi-agent model for countering terrorism, *Proceedings of the 33rd International Conference on Industrial, Engineering & Other Applications of Applied Intelligent Systems (IEA/AIE_20), Kitakyushu, Japan*, pp. 1–8.

Kebir, O., Nouaouri, I., Belhaj, M., Ben Said, L. and Akrout, K. (2020c). A multi-agent architecture for modeling organizational planning against terrorist attacks in urban areas, *2020 International Multi-Conference on Organization of Knowledge and Advanced Technologies (OCTA), Tunis, Tunisia*, pp. 1–8.

Kebir, O., Nouaouri, I., Belhaj, M., Said, L.B. and Akrout, K. (2020d). MAMCTA—Multi-agent model for counter terrorism actions, *Revue de l'Information Scientifique et Technique* **25**(1): 76–90.

Kebir, O., Nouaouri, I., Rejeb, L. and Said, L.B. (2022). Simulating actors' behaviors within terrorist attacks scenarios based on a multi-agent system, *Proceedings*

of the 12th International Defence and Homeland Security Simulation Worskhop (DHSS 2022), Rome, Italy, pp. 12–20.

Kebir, O., Nouaouri, I., Rejeb, L. and Said, L.B. (2021). Conceptual terrorist attacks classification: Pre-processing for artificial intelligence-based classification, *Proceedings of the 11th International Defence and Homeland Security Simulation Workshop (DHSS 2021), Kraków, Poland*, pp. 16–24.

Kress, M., Caulkins, J.P., Feichtinger, G., Grass, D. and Seidl, A. (2018). Lanchester model for three-way combat, *European Journal of Operational Research* **264**(1): 46–54, DOI: 10.1016/j.ejor.2017.07.026.

Kress, M. and Szechtman, R. (2009). Why defeating insurgencies is hard: The effect of intelligence in counter-insurgency operations—A best-case scenario, *Operations Research* **57**(3): 578–585.

Lanchester, F.W. (1916). *Aircraft in Warfare: The Dawn of the Fourth Arm*, Constable, London.

Lee, H.-K. and Zo, H. (2017). Assimilation of military group decision support systems in Korea: The mediating role of structural appropriation, *Information Development* **33**(1): 14–28.

Lucas, T.W. and McGunnigle, J.E. (2003). When is model complexity too much? Illustrating the benefits of simple models with Hughes' salvo equations, *Naval Research Logistics* **50**(3): 197–217.

Maureen, A. (2017). Military mission combat efficiency, *Journal of Defense Resources Management* **8**(1 (14)): 63–76.

Okoye, C., Collins, O. and Mbah, G. (2020). Mathematical approach to the analysis of terrorism dynamics, *Security Journal* **33**: 427–438, DOI: 10.1057/s41284-020-00235-5.

Oladejo, M., Udoh, I. and Abam, A. (2020). Optimizing the community's supports in counter-terrorism operations: A sticks–carrots game theoretic model, *Journal of Applied Science and Technology* **39**(47): 45–67.

Osoba, O.A. and Kosko, B. (2017). Fuzzy cognitive maps of public support for insurgency and terrorism, *Journal of Defense Modeling and Simulation* **14**(1): 17–32.

Pagán, J.V. (2010). Improving the classification of terrorist attacks: A study on data pre-processing for mining the Global Terrorism Database, *ICSTE 2010—2nd International Conference on Software Technology and Engineering, Puerto Rico, USA*, Vol. 1, pp. 104–110.

Pechenkina, A.O. and Bennett, D.S. (2017). Violent and non-violent strategies of counterinsurgency, *Journal of Artificial Societies and Social Simulation* **20**(4): 11.

Saltelli, A. and Annoni, P. (2010). How to avoid a perfunctory sensitivity analysis, *Environmental Modelling & Software* **25**(12): 1508–1517.

Sandler, T. (2018). *Terrorism: What Everyone Needs to Know*, Oxford University Press, Oxford.

Seehuus, R.A., Rise, Ø.R., Hannay, J.E., Wold, R. and Matlary, P. (2020). Cloud-based decision support system for planning military operations, *Technical report*, Norwegian Military Academy, Oslo.

Sumithra, S. and Vadivel, R. (2021). An optimal innovation based adaptive estimation Kalman filter for accurate positioning in a vehicular ad-hoc network, *International Journal of Applied Mathematics and Computer Science* **31**(1): 45–57, DOI: 10.34768/amcs-2021-0004.

Surdu, J.R. and Kittka, K. (2008). The deep green concept, *Proceedings of the 2008 Spring Simulation Multiconference, Ottawa, Canada*, pp. 623–631.

Udoh, I. and Oladejo, M. (2019). Optimal human resources allocation in counter-terrorism (CT) operation: A mathematical deterministic model, *International Journal of Advances in Scientific Research and Engineering* **5**(1): 96–115.

Şuşnea, E. (2012). Decision support systems in military actions: Necessity, possibilities and constraints, *Journal of Defense Resources Management* **3**(2): 131–140.

Vilanova, A., Telea, A., Scheuermann, G. and Möller, T. (2008). Investigative visual analysis of global terrorism, *Eurographics, Crete, Greece*, Vol. 27, p. 2008.

Willis, H.H., Morral, A., Kelly, T. and Medby, J. (2005). *Estimating Terrorism Risk*, RAND Corporation, Santa Monica.

Oussama Kebir is a weapon systems engineer from the Military Academy of Fondok (2015), a doctoral candidate in artificial intelligence at the Tunis Higher Institute of Management, and a master student of human rights and international humanitarian law at the Faculty of Legal, Political and Social Sciences, Carthage University. He participates in and leads different counter-terrorism missions in sensitive areas in Tunisia. He has had some publications in local and international conferences.

Issam Nouaouri is an associate professor at the University of Artois–Lille Nord de France and the LGI2A Laboratory. He holds a PhD in industrial and logistic engineering from the University of Artois–Lille Nord de France and is an engineer in industrial engineering from the National Engineering School of Tunis. He is currently focusing on logistics and operational research in health care.

Lilia Rejeb obtained her PhD in computer science from the University of Reims Champagne–Ardennes, France, in 2005. She is an associate professor of higher education at the Tunis Higher Institute of Management, University of Tunis, and a member of the SMART Laboratory.

Lamjed Ben Said obtained his PhD in computer science from the University of Paris VI, France, in 2003. Now, he is a full professor of higher education and the head of the Tunis Higher Institute of Management, University of Tunis, where he also holds the position of the head of the SMART Laboratory.

Received: 3 September 2021
Revised: 25 January 2022
Accepted: 27 January 2022