

Security Economics: A Multiobjective Adversarial Risk Analysis Approach to Airport Protection

Javier Cano¹, David Ríos Insua², Alessandra Tedeschi³, Uğur Turhan⁴

¹Department of Statistics and Operations Research, Rey Juan Carlos University

²Royal Academy of Sciences, Spain

³Deep Blue Srl, Italy

⁴Anadolu University, Turkey

Abstract

We analyze the case of protecting an airport, in which there is concern with terrorist threats against the Air Traffic Control (ATC) Tower. To deter terrorist actions, airport authorities rely on various protective measures. They have considerable costs, but by deploying them, airport authorities expect to minimize the risks of terrorist actions. We aim at giving advice to the airport authorities by devising a security resource allocation plan. We use the framework of adversarial risk analysis to deal with the problem.

Keywords: Adversarial Risk Analysis, Intelligent Attacker, Critical Infrastructure, Multiattribute Expected Utility, Airport Installation, Airport/ATM Security.

1 Introduction

As cogently illustrated in [Lomborg \(2008\)](#), many of the world's biggest problems, like proliferation of weapons, armed conflicts, corruption, terrorism, drug trafficking or money laundering, are related with security, which is indeed one of the most menacing global issues.

1 By now, there is a large tradition within economics and modeling of security, including the
2 pioneering work of [Becker \(1968\)](#), who largely initiated the field with his economic theory
3 of delict, or [Cornish and Clarke \(1986\)](#), who emphasized operational aspects, like those of
4 situational crime prevention and the reasoning criminal, stressing the relevance of rational
5 choice theory within criminology.

6 Large scale terrorist attacks, like 9/11 or the Madrid train bombings, see [Haberfeld and](#)
7 [von Hassell \(2009\)](#), have entailed a renewed interest in the economics of security, given the
8 significant aftermath investments in preventive and reactive measures, which have been ques-
9 tioned by public opinion. [Merrick and Parnell \(2011\)](#) provide a review of recent approaches
10 in counterterrorism modeling, favoring adversarial risk analysis (ARA). In ARA, see [Ríos](#)
11 [Insua et al. \(2009\)](#), the aim is to support one of the participants (the Defender) who will
12 use a decision analytic approach to solve her decision making problem. For this, she needs
13 to forecast the actions of the other participants and, consequently, the outcomes which she
14 and her opponents will receive.

15 In this paper, we describe how ARA may be used to find the optimal security resource
16 allocation to protect a single site of interest to a Defender, which might be a Government
17 or a private body responsible of security, from the attacks of a terrorist organization, which
18 we designate the Attacker. From the Defender's point of view, these problems often have
19 a multiobjective nature. Although security of people and installations is always a main
20 concern for authorities, there will typically be other relevant issues that need to be taken
21 into account as e.g. the investments in preventive measures or the economic, social and/or
22 political implications of the potential damages caused by terrorists. Interestingly enough,
23 note that the Attacker might have also multiple objectives in his decision making. Thus, ARA
24 aims at providing one-sided prescriptive support to one of the opponents, the Defender, based
25 on a subjective expected (multiattribute) utility model, treating the adversary's decisions
26 as uncertainties. In order to predict the adversary's actions, we model his decision problem
27 and try to assess his probabilities and utilities. Assuming that the adversary, the Attacker,
28 is also a expected (multiattribute) utility maximizer, we can predict his actions by finding

1 the action that maximizes his expected multiattribute utility. Our uncertainty about the
2 Attacker's probabilities and utilities is propagated over to the Attacker's optimal decision
3 and incorporated in our forecasting model.

4 We focus on an airport security problems. Millions of people pass through airports every
5 day, not only passengers and their companions, but also ground and airline staff, and other
6 personnel. Such gathering of people, together with the strategic value of their installations
7 make airports a potential and prime target for terrorists. Furthermore, the possibility of
8 hijacking an airplane and using it as a lethal weapon against people and/or infrastructures,
9 as in S-11, adds an extra motivation on the terrorists' will to attack airport installations.
10 Airport authorities worldwide are deeply concerned with this type of threats. To this aim,
11 they invest annually *large amounts of money* in preventive measures, trying to minimize the
12 chances of any dangerous situation happening within airport sensitive areas. As such, airport
13 security serves several purposes in this context: (1) to protect the airport installations from
14 the terrorist threat; (2) to guarantee the safe functioning of a vital transportation means;
15 and (3) to protect a nation and its people.

16 Thus, we analyze how to support the authorities of an airport who are concerned with
17 terrorist threats against airport installations and operations. Specifically, we focus on a
18 particularly critical scenario: the unlawful access to the ATC Tower, aimed at taking hold of
19 Air Traffic Control Officers (ATCOs) before or during flight control operations. Consequences
20 of these acts have a multiattribute nature, and could be severe, including: (1) a crisis on
21 air traffic operations in the airfield and airspace; (2) flight safety very negatively affected;
22 (3) air traffic canceled or diverted to other ATC units or airfields, with important economic,
23 social (in extreme cases, even in terms of human lives) and image consequences. As a way to
24 minimize the probability of occurrence of such an attack, as well as to reduce the severity of
25 its impact, airport authorities may consider incrementing current security levels by investing
26 more in already existing human and technical resources. These preventive measures include
27 police and security guards, as well as screening and detecting devices, with non-negligible
28 costs. Besides, in the event of a successful attack within the specific country we consider, a

1 Special Police Force (SPF), linked with the Government, will be immediately called on to
2 take control of the situation, aiming at recovering from the attack as soon as possible, trying,
3 at the same time, to minimize its consequences. We assume that airport authorities do not
4 have any alternative for this decision: they will call the SPF for sure. The intervention of the
5 SPF might have drastic consequences, especially for the terrorists, whose lives will be at risk,
6 although collateral damages on persons and goods could also be suffered on the Defender's
7 side. Negotiation with the terrorists is not considered, in principle, as an acceptable option.
8 However, the presence of hostages could postpone the deployment of the SPF for a certain
9 period of time, while airport authorities try to convince the terrorists to surrender without
10 blood spilling. Nevertheless, should the terrorists not drop their attitude, threatening other
11 people and fixtures on the Defender's side, the SPF will finally intervene. The multiobjective
12 nature of the problem becomes a more delicate issue as human lives and severe consequences
13 are concerned.

14 We model the problem as a particular case of a Sequential Defend-Attack model within
15 the Adversarial Risk Analysis framework, see [Ríos and Ríos Insua \(2012\)](#), in which the
16 airport authorities would first deploy a portfolio of preventive measures to deter or mitigate
17 the actions of the terrorists. Then, the terrorists, having observed such decision, would
18 follow a strategy to perform their terrorist attacks. Should the attack be successful, an SPF
19 would be immediately deployed. We assume that the consequences for the Defender will
20 depend on the effort in implementing their preventive actions, the impacts of the attack
21 and the eventual result of the SPF action. Similarly, the consequences for the Attacker will
22 depend on the costs of deploying their terrorist actions, the impact of their attack, and the
23 final outcome of the crisis after the intervention of the SPF, which will possibly entail some
24 casualties on their side. Both the Defender and the Attacker are regarded as expected utility
25 maximizers.

26 The structure of the paper is as follows. In Section 2, we provide a detailed description of
27 the selected scenario: the unlawful access to the ATC Tower. Section 3 describes the ARA
28 model we have devised to solve the problem. We apply it to a specific case study in Section

1 4. We end up with some discussion.

2 Description of the Scenario

3 In the case of concern, the airport ATC Tower has its only access gate within the terminal
4 main hall. One can only reach this gate after passing the security checks situated at the
5 entrance of the terminal building, which are performed by the private security personnel.
6 Access to the ATC Tower is controlled by the ATCOs with the aid of a camera installed over
7 the access gate. When an authorized person needs to enter into the ATC Tower, she has to
8 ring a bell and, upon approval by the ATCOs, the door will be remotely opened.

9 An Attacker among the passengers or airport workers can plan to enter the ATC Tower
10 and take hold of the ATCOs, before or during flight control operations. We consider that
11 the Attacker is a group of between one to five terrorists. We assume that the more members
12 in the terrorist cell, the more chances they will have to be successful in their attack. After
13 passing by the first security checks, the Attackers could create an opportunity to enter into
14 the ATC Tower gate, capture the ATCOs and use telecommunications to interfere with air
15 traffic operations.

16 2.1 Multiattribute consequences of a terrorist act against the ATC 17 Tower

18 The impacts of a successful terrorist act against the ATC Tower can be potentially catas-
19 trophic, causing a crisis over air traffic operations, in the airfield and the airspace. As a
20 consequence, the safety of all flights involved would be negatively affected, and it could be
21 necessary to divert air traffic to an alternate ATC unit or airfield. Besides, during the ini-
22 tial crisis phase, pilots and/or other affected stakeholders might not be able to understand
23 the seriousness and implications of the situation, preventing them from making the most
24 appropriate decisions, something which could eventually worsen the situation. Under all
25 circumstances, pilots and ATCOs should be able to manage their flights and operations in

1 the safest manner.

2 Other collateral consequences after a successful attempt to access the ATC Tower occurs
3 could be:

4 • Besides safety and security impacts, cancelation consequences can be considerable, as
5 connected national and international flights and/or airports and airspaces could be
6 affected.

7 • Media will inform people immediately about the case. This could cause yet another
8 crisis around airport facilities, because of people trying to access/escape from it.

9 • Negative perception of security by airport users. As a result, people's image of aviation
10 industry could be affected negatively and they could opt for alternative transport
11 means, affecting the balance sheet of the operator.

12 **2.2 Countermeasures deployed by airport authorities**

13 Airport authorities are considering investing in technical resources to increase security by
14 checking passengers (through biometrics) and their baggages. They also check airport and
15 airline staff or personnel of entities providing services to the airport (construction, mainte-
16 nance, catering, etc). Besides, there are several different bodies in charge of airport security,
17 depending on the regulations of the specific country and on the size and features of the airport
18 under concern. However, we shall encompass them into two broad groups: airport police and
19 private security personnel. We outline below the main features of all these countermeasures.

20 • Cameras. They are used for biometric control, identifying people through their char-
21 acteristics or traits. They are used as a form of identification and access control, and
22 also as a way to identify individuals in groups under surveillance. In general, the more
23 cameras, the more chances to alert from suspect people entering the airport.

24 • Metal detectors. In general, the more scanning units and more operations per unit, the
25 more customers and baggages will be checked, reducing the probabilities of a terrorist

1 attack.

- 2 • X-ray devices, have a preventive role, similar to metal detectors.
- 3 • Airport police. In general, the more police, the less chances that an unauthorized
4 person will gain access to the ATC Tower.
- 5 • Airport private security. In general, the more personnel, the more customers and
6 baggages will be checked, reducing the chances that an attacker could enter and/or
7 introduce dangerous material within the airport.

8 The SPF, who will intervene in case an attack succeeds, will be considered as a recovery
9 measure. They are an elite police team, specifically trained for this kind of events, and
10 linked with the Government. As such, their hypothetical deployment would entail no finan-
11 cial consequences for the airport authorities. They will be called on in case of emergency,
12 commanding the situation. Their major concern is to recover control of the ATC Tower and
13 capture the attackers with no life cost. However, in our incumbent case, should the attackers
14 put up a bloody resistance, airport authorities would have little concern about terrorists'
15 lives. On the other hand, the presence of hostages on the Defender's side would have little
16 influence on the forcefulness of the SPF action in case the terrorists refuse to drop their
17 attitude. Furthermore, there is no quandary about their intervention: they will be deployed
18 mandatorily whenever a successful attack occurs (and, in consequence, there is actually no
19 decision associated with this event). Nevertheless, we shall include them in the model since
20 their intercession will affect substantially the final result of the attack.

21 **3 The Model**

22 We shall consider a sequential Defend-Attack model to structure the problem, see e.g. [Ríos](#)
23 [and Ríos Insua \(2012\)](#). In it, airport authorities first deploy a set of preventive measures to
24 protect, among other targets, the access to the ATC Tower. The Attacker, who observes such

1 measures, will decide on whether or not to launch an attack. The Attacker may consider dif-
 2 ferent severity options for the attack, which will be modeled through the number of terrorists
 3 taking part in the attack. Finally, should an attack be successful, airport authorities will try
 4 to recover from it and minimize its consequences by deploying additional measures, which in
 5 our case will imply calling the SPF. As mentioned before, given the peculiarities of this case
 6 study, in which human lives are involved and enormous economic, social and political conse-
 7 quences are in play, airport authorities will deploy all the available recovery resources after a
 8 successful attack, regardless of any other consideration. Therefore, we will not consider their
 9 deployment as a second defensive decision step, typical of sequential defend-attack-defend
 10 models.

11 A biagent influence diagram for the problem is shown in Figure 1, see Pearl (2005), with
 12 white nodes belonging to the Defender, dark grey nodes belonging to the Attacker and light
 13 grey nodes shared by both of them. Node “Prev. measures” corresponds to the Defender’s
 14 portfolio of preventive measures, $x \in \mathcal{D}_1$. Node “Countermeasures” is a deterministic node
 15 related with the deployment of recovery measures. There is actually no decision associated
 16 to it but, rather, an automatic response: in case of a successful attack, the SPF will be
 17 immediately called on. No additional resources will be summoned if the attack fails, since
 18 we assume, in that case, that the terrorists have been killed or detained by ordinary police
 19 and/or private security personnel or, eventually, some of them managed to escape.

20 The node “Attacker decision” represents the decision undertaken by the terrorists, once
 21 they have observed the defensive measures deployed by the Defender. The set of all possible
 22 attacks a is denoted by \mathcal{A} .

23 The only initially relevant uncertainties for this problem are: (1) the preliminary result
 24 of the attack, s_1 , represented by the node “Result”, which depends probabilistically on
 25 $(x, a) \in \mathcal{D}_1 \times \mathcal{A}$; and (2) its final outcome after the intervention of the SPF, s_2 , represented
 26 by the node “Final Result”. We denote by \mathcal{S}_1 and \mathcal{S}_2 the sets of all possible outcomes
 27 for the corresponding events. Regarding the multiple attributes of the problem, detailed
 28 later on, we assume that the consequences for the Defender, as represented by the chance

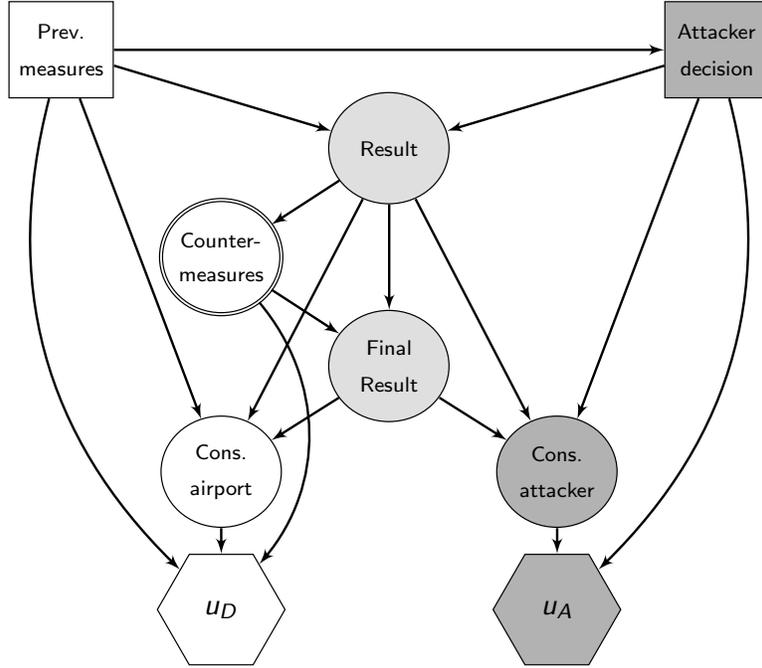


Figure 1: Influence diagram for the airport case study.

1 node “Cons. airport”, will depend on (x, s_1, s_2) , i.e., the effort spent in implementing the
 2 protective measures, the initial impact of the attack and its final result after the intervention
 3 of the SPF. Then, she will get her utility u_D . Similarly, the multiple consequences for the
 4 Attacker, summarized on the chance node “Cons. attacker”, will depend on (a, s_1, s_2) , i.e.,
 5 the effort spent in launching the attack, and the related initial and final outcomes. He will
 6 then get his utility u_A . We describe now in detail the different elements in \mathcal{D}_1 , \mathcal{A} , \mathcal{S}_1 and
 7 \mathcal{S}_2 .

- 8 • \mathcal{D}_1 . We consider all feasible portfolios $(x_1, x_2, x_3, x_4, x_5)$ of measures which, respec-
 9 tively, represent the number of additional cameras, metal detector units, X-ray devices,
 10 police and private security members deployed. They have associated per unit costs for
 11 the incumbent planning period, c_j , $j = 1, \dots, 5$, respectively. Then, if we denote by

1 B the available budget, the feasible portfolios of preventive measures would satisfy

$$2 \quad c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5 \leq B,$$

$$3 \quad x_1, x_2, x_3, x_4, x_5 \geq 0,$$

$$4 \quad x_1, x_2, x_3, x_4, x_5 \text{ integer.}$$

5

- 6 • \mathcal{A} . We model the Attacker as an organized group composed of between one and five
7 terrorists. Therefore, we shall consider the number of terrorists actually performing
8 the attack against the ATC Tower as the decision variable for the Attacker, i.e. $a =$
9 $\{0, 1, 2, 3, 4, 5\}$, including the possibility of no attack ($a = 0$).
- 10 • \mathcal{S}_1 . The possible values for s_1 are $\{0, 1, \dots, a\}$, representing how many terrorists man-
11 aged to gain access into the ATC Tower. The rest of them would have been killed or
12 detained during the attack, or might have avoided being captured, as specified later
13 on. If $s_1 = 0$, the attack fails and the problem is over. Irrespective of the result of
14 the attack, some casualties could also occur among the defenders. We will discuss this
15 issue later on, when analyzing the Defender's problem.
- 16 • Regarding \mathcal{S}_2 , we shall assume that the ATC Tower will be always recovered by the
17 SPF, since this has been historically the case in similar episodes in the past: security
18 forces take hold back of the situation sooner or later. However, we are interested in
19 how many terrorists will be killed or detained. We then define the possible values in
20 \mathcal{S}_2 as $s_2 \in \{0, 1, \dots, s_1\}$, representing the number of terrorists killed. The remaining
21 terrorists, $s_1 - s_2$, will be detained. At this stage, we explicitly rule out the possibility of
22 some terrorists getting away from the ATC Tower. Besides, additional casualties could
23 also occur among the defenders. We will give details about the entailed consequences
24 of the recovery actions for both adversaries later on.

1 3.1 The Defender's problem

2 We sketch the Defender's problem in Figure 2. As we can observe, the Attacker's decision
 3 node, is perceived by the Defender as a chance node.

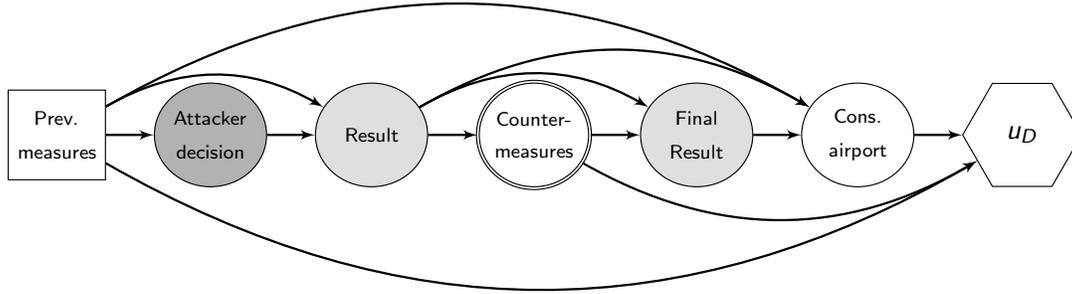


Figure 2: Influence diagram for the Defender's problem.

4 The Defender's dynamics involve the following stages:

- 5 1. She invests $(x_1, x_2, x_3, x_4, x_5)$, incurring in a cost $c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5$.
 6 Note that (x_1, x_2, x_3) serve to reduce the likelihood of any prohibited item or artefact
 7 being introduced in the airside or in security restricted areas. They also increase the
 8 probability of detecting suspect people trying to enter the ATC Tower with criminal
 9 intentions. On the other hand, (x_4, x_5) serve to deter the actions of potential attackers.
- 10 2. She observes whether an attack is launched by the terrorists. If such attack is successful,
 11 she calls on the SPF, so as to hold back control of the ATC Tower.
- 12 3. She faces the multiple consequences in relation with the possibility of a terrorist attack
 13 against the ATC Tower, and the recovery from it after the intervention of the SPF.
 14 We specify such consequences below.
- 15 4. She attains her (multiobjective) utility.

16 We provide now a detailed description of the relevant consequences for the Defender in
 17 case of a successful attack:

- 1 • Lives and injuries. When the first strike of the terrorists takes place, everybody present
2 in the scenario could be in injury and/or life danger, including the possibility of being
3 taken as hostages by the terrorists. This affects passengers and staff inside or near
4 the facilities, as well as ATCOs in the ATC Tower. Additional casualties among SPF
5 members, other involved security personnel or civilians could also happen during re-
6 covery actions. We take all this into account by defining a variable $y \in \{0, 1, \dots, m\}$,
7 representing the number of casualties or severely injured people on the Defender's side.
8 Here, m is a maximum theoretical number of possible victims. Furthermore, we assume
9 a fixed cost of a life on the Defender's side c_{life} , irrespective of their affiliation. For
10 simplicity, we assume the same consequences for a killed or badly injured person and,
11 on the other hand, we disregard the associated consequences of mildly injured people.
- 12 • Flight diversion and cancelation. In principle, this is one of the main targets for the
13 terrorists: disrupting air traffic as much as possible. Usually, the airline operator is
14 responsible for passengers' related costs in the event of a flight diversion or cancelation.
15 However, once the incident reports and investigations have been completed, airlines can
16 ask their insurance companies for partial or total compensation of entailed costs. The
17 airport could be eventually found liable to refund part of these costs to the airlines.
18 These include alternative transportation (paying the new ticket and/or refunding the
19 original one, or any other compensation mode), extra catering and/or accommodation
20 costs. We explicitly distinguish the consequences for flight diversions and cancelations.
21 When cabin crew informs about an emergency or extraordinary situation, they can
22 divert to an alternate aerodrome or fly back to the departing airport. The decision is
23 made by the cabin crew and the company, in collaboration with air traffic management.
24 Regarding flight cancelation, it can create a chain reaction, affecting connected flights,
25 resulting in additional consequences for passengers, airlines and airports. Given the dif-
26 ficulties in assessing such consequences, see e.g. [Cook et al. \(2012\)](#), we shall aggregate
27 them into a single quantity, f . It seems reasonable to assume that the consequences
28 (in terms of costs) for airport authorities will be similar, regardless of the number of

terrorists actually succeeding in their attempt to access the ATC Tower, except for the case in which only one attacker succeeds ($s_1 = 1$), for which we will assume a lesser impact. We should also take into account the inherent uncertainty on the value of f , expressed through a probability distribution $p_D(f|s_1)$.

- Image consequences. If a security incident occurs, this might essentially happen because there was a security breach. This will yield an immediate deterioration on the image of the airport as perceived by customers, even if no life or injury damage occurs. News of the crisis will be spread and amplified by the media, magnifying its impact at national or even international level. This “panic effect” is a main objective for the Attacker. We can think of different image impacts: (1) Airport security image; (2) Aircraft security and safety image; and (3) National image consequences. We shall subsume all previous effects into a single variable, g . We will use a probability distribution $p_D(g|a)$ to express our uncertainty about it, whose expected value will increase with the number a of terrorists (not only of those actually succeeding in their attempt).

We summarize all relevant impacts for the Defender in Table 1.

Concept	Impact
Investment costs	$c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5$
Cost of a life	c_{life}
Flight diversion/cancelation	f
Image	g

We use the measurable multiattribute value function concept together with the relative risk aversion concept in [Dyer and Sarin \(1979, 1982\)](#) to come out with the Defender’s utility function. First, the multiattribute value function for the Defender will be described through:

$$c_D(x, y, f, g) = \begin{cases} (c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5) + c_{\text{life}} \cdot y + f + g, & \text{if } a \geq 1, \\ c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 + c_5x_5, & \text{if } a = 0, \end{cases}$$

1 effectively monetizing consequences. We then consider that the Defender is constant risk
 2 averse with respect to c_D . Thus, her utility function is (strategically equivalent to) $u_D(c_D) =$
 3 $-\exp(k_D \cdot c_D)$, with $k_D > 0$.

4 Then, once she has assessed all the involved uncertainties, $p_D(f|s_1)$, $p_D(g|a)$, $p_{0,x}^D$, $p_{a,x}^D$
 5 and $p_{s_1,a,x}^D$, she has to compute the expected utility of each alternative, *proceeding through*
 6 *the following steps:*

7 1. Compute the random expected utility $\psi_D(x, a, s_1, y)$ when $a \geq 1$

$$8 \quad \psi_D(x, a, s_1, y) = \iint u_D \left(\sum_{j=1}^5 c_j x_j + c_{life} \cdot y + f + g \right) p_D(f|s_1) p_D(g|a) df dg.$$

9 2. Compute the random expected utility $\psi_D(x, a, s_1)$ when $a \geq 1$

$$10 \quad \psi_D(x, a, s_1) = \sum_{y=0}^m p_{y,a}^D \psi_D(x, a, s_1, y),$$

11 where

$$12 \quad p_{y,a}^D = \Pr(y \text{ casualties on Defender's side} | a \text{ terrorists attacking}).$$

13 3. Compute the random expected utility $\psi_D(x, a)$ when $a \geq 1$

$$14 \quad \psi_D(x, a) = \sum_{s_1=0}^a p_{s_1,a,x}^D \psi_D(x, a, s_1),$$

15 where $p_{s_1,a,x}^D$ models the Defender's beliefs about the number of those terrorists actually
 16 succeeding when the investment is x , and the number of terrorists is a .

17 4. Compute the random expected utility $\bar{\psi}_D(x)$ when $a \geq 1$

$$18 \quad \bar{\psi}_D(x) = \sum_{a=1}^5 p_{a,x}^D \psi_D(x, a),$$

19 where $p_{a,x}^D$ models her beliefs about the number of terrorists performing the attack when

1 3.2 The Attacker's problem

2 In order to come out with $p_{a,x}^D$, we describe now the Attacker's problem, whose influence
 3 diagram is shown in Figure 3, together with the involved random variables and their depen-
 4 dencies.

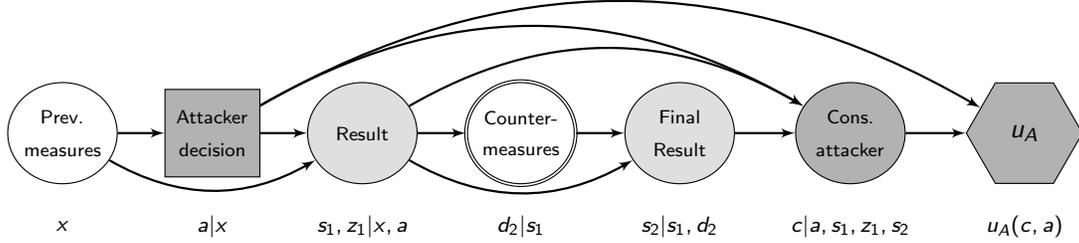


Figure 3: Influence diagram for the Attacker's problem.

5 Regarding the dynamics of the Attacker, we have that:

- 6 1. The Attacker sees the security measures deployed by the Defender $(x_1, x_2, x_3, x_4, x_5)$.
- 7 2. The Attacker decides his attack $a \in \mathcal{A}$. If he decides not to attack, the consequences
 8 are negligible for him.
- 9 3. In case of attacking, he observes the result of the attack, s_1 , and faces his operational
 10 consequences. We model this by defining two variables, z_1 and w_1 , representing the
 11 number of terrorists killed and detained in the attack, with $\{z_1, w_1\} \in \{0, 1, \dots, a - s_1\}$
 12 and $z_1 + w_1 \leq a - s_1$. The remaining terrorists, $a - s_1 - z_1 - w_1$, will manage to get away.
 13 Note that we explicitly distinguish between being killed or imprisoned (*only suicide*
 14 *terrorists will be most likely indifferent between both possibilities, but they do not seem*
 15 *to be a real threat in the political context of the incumbent country. Therefore, we shall*
 16 *not consider here such possibility*).
- 17 4. In case of a successful attack, he faces the recovery measures deployed by the Defender
 18 and its consequences. We assume that, after the intervention of the SPF, s_2 terrorists
 19 will be killed, with $s_2 \in \{0, 1, \dots, s_1\}$, and the rest, $s_1 - s_2$, are detained. Here, d_2

1 is a deterministic variable, which depends only on the outcome of the initial attack
 2 performed by the terrorists, s_1 . If $s_1 = 0$ (failed attack), the SPF is not called on, i.e.,
 3 $d_2 = 0$. Otherwise, $d_2 = 1$, meaning that the SPF will intervene.

4 5. He gets the corresponding utility.

5 The Defender considers that the relevant multiple consequences for the Attacker are:

- 6 • Preparation costs. As for many other types of terrorist attacks, preparation costs are
 7 not particularly high, especially when compared with the consequences they aim at
 8 inflicting to the Defender. We shall assume a fixed cost c_p for the whole operation per
 9 each involved terrorist.
- 10 • Whether they are able or not to take control over air traffic operations. This is the
 11 main target for terrorists. To simplify matters, we assume that the terrorists give
 12 the same value as the Defender to image and operational consequences, i.e., f and
 13 g . We shall use also probability distributions $p_A(f|s_1)$ and $p_A(g|a)$ to describe the
 14 Attacker's uncertainty about such consequences, and his belief that they will depend
 15 on the number of successful and total attackers, respectively.
- 16 • The number of terrorists killed or detained. We shall assume that the terrorists put a
 17 value c'_{life} to their lives and a value c_d to the fact of being detained.

18 As before, we consider the same approach to model the Attacker's utility function. First,
 19 we aggregate the attributes in a multiattribute value function

$$20 \quad c = \begin{cases} f + g - c_p - c'_{\text{life}} \cdot (z_1 + s_2) - c_d \cdot (w_1 + s_1 - s_2), & \text{if } a \geq 1, \\ -c_p, & \text{if } a = 0, \end{cases} \quad (2)$$

21 and, then, assume that the Attacker is risk prone in benefits. Therefore, his utility function
 22 is strategically equivalent to

$$23 \quad u_A(c) = \exp(k_A \cdot c), \quad k_A > 0.$$

1 The elements involved in solving the Attacker's problem are:

- 2 • $(s_1, z_1, w_1, a - s_1 - z_1 - w_1)$, is the initial result of the attack, in terms of the number
3 of terrorists succeeding, killed, detained or escaping. We shall consider a distribution
4 $p_{s_1, z_1, a, x}^A = p_A(s_1, z_1, w_1 | a, x)$ to model the Attacker's beliefs about the probabilities
5 over the four incumbent events, given the investments x and the number of terrorists
6 a . We assume that the more defensive resources, the less terrorists will be likely to
7 succeed in the attack or escape after it in case they fail. Regarding technological
8 measures (cameras, metal detectors and X-ray devices), they will only have influence
9 on the detention of terrorists, whereas human resources (police and private security)
10 could also cause some casualties among the attackers.
- 11 • s_2 , is the final result of the attack, after the intervention of the SPF. $p_A(s_2 | s_1)$ models
12 the Attacker's beliefs about it.

13 The steps needed to solve the Attacker's problem are:

- 14 1. We integrate out the uncertainty over c . We get the expected utility

$$15 \quad \psi_A(a, s_1, z_1, w_1, s_2) = \iint u_A(c) p_A(f | s_1) p_A(g | a) df dg,$$

16 where c is defined in (2), and $p_A(f | s_1)$ and $p_A(g | a)$ are the densities over f and g ,
17 which, in turn, induce the distribution $p_A(c | a, s_1, z_1, w_1, s_2)$.

- 18 2. We reduce the uncertainty over s_2 . We get the expected utility $\psi_A(a, s_1, z_1, w_1)$ as

$$19 \quad \psi_A(a, s_1, z_1, w_1) = \sum_{s_2 \in \mathcal{S}_2} p_A(s_2 | s_1) \psi_A(a, s_1, z_1, w_1, s_2).$$

- 20 3. We eliminate the uncertainty over s_1 . We get the expected utility $\psi_A(a, x)$ as

$$21 \quad \psi_A(a, x) = \sum_{s_1, z_1, w_1 \in \mathcal{S}_1} p_A(s_1, z_1, w_1 | a, x) \psi_A(a, s_1, z_1, w_1).$$

1 4. We find the optimal strategy for the Attacker by solving

$$2 \quad \psi_A(x) = \max_{a \in \mathcal{A}} \psi_A(a, x).$$

3 This provides $a(x) = \arg \max_a \psi_A(a, x)$, the optimal attack level when the security
4 investment is x .

5 Note, however, that we have uncertainty about $u_A(\cdot)$, $p_A(f|\cdot)$, $p_A(g|\cdot)$, $p_A(s_2|\cdot)$ and $p_A(s_1, z_1,$
6 $w_1|\cdot)$, which we model through the random utilities and probabilities $U_A(\cdot)$, $P_A(f|\cdot)$, $P_A(g|\cdot)$,
7 $P_A(s_2|\cdot)$ and $P_A(s_1, z_1, w_1|\cdot)$. Then, we propagate such uncertainty as follows, for each x :

8 1. Compute the random expected utility

$$9 \quad \Psi_A(a, s_1, z_1, w_1, s_2) = \iint U_A(c) P_A(f|s_1) P_A(g|a) df dg.$$

10 2. Compute the random expected utility

$$11 \quad \Psi_A(a, s_1, z_1, w_1) = \sum_{s_2 \in \mathcal{S}_2} P_A(s_2|s_1) \Psi_A(a, s_1, z_1, w_1, s_2).$$

12 3. Compute the random expected utility

$$13 \quad \Psi_A(a, x) = \sum_{s_1, z_1, w_1 \in \mathcal{S}_1} P_A(s_1, z_1, w_1|a, x) \Psi_A(a, s_1, z_1, w_1).$$

14 4. Compute the random optimal alternative

$$15 \quad A(x) = \arg \max_{a \in \mathcal{A}} \Psi_A(a, x).$$

16 Then, we would have that the desired distribution $p_{a,x}^D$ in (1) would be $p_{a,x}^D = \Pr(A(x) = a)$.
17 In order to estimate it, we may proceed by simulation as follows, where K is the Monte
18 Carlo sample size:

Algorithm 1: Simulating the optimal attack level

For each x

For $i = 1$ to K

Sample $U_A^i(\cdot), P_A^i(f|\cdot), P_A^i(g|\cdot), P_A^i(s_2|\cdot), P_A^i(s_1, z_1, w_1|\cdot)$.

Compute

$$\Psi_A^i(a, s_1, z_1, w_1, s_2) = \iint U_A^i(c) P_A^i(f|s_1) P_A^i(g|a) df dg.$$

Compute

$$\Psi_A^i(a, s_1, z_1, w_1) = \sum_{s_2 \in \mathcal{S}_2} P_A^i(s_2|s_1) \Psi_A^i(a, s_1, z_1, w_1, s_2).$$

Compute

$$\Psi_A^i(a, x) = \sum_{s_1, z_1, w_1 \in \mathcal{S}_1} P_A^i(s_1, z_1, w_1|a, x) \Psi_A^i(a, s_1, z_1, w_1).$$

Compute the random optimal alternative

$$A^i = \operatorname{argmax}_a \Psi_A^i(a, x).$$

Finally, we approximate $\Pr(A(x) = a) \approx \#\{1 \leq i \leq K : A^i = a\}/K$.

4 A Case Study

We consider the case of a small-size international airport. *In what follows, we shall express all the involved costs in euros, as it is the relevant currency in the incumbent case.* It has an average annual budget of 3 million euros, with around 5% of the total budget, 150,000 euros, to be invested in new security measures on top of the current ones. We first discuss issues related with the Defender's problem. Then, we give details related to the point of view of the Attacker. The assessments were made with the aid of the experts of the incumbent airports, later validated in an airport security expert workshop and checked for robustness through sensitivity analysis.

1 4.1 Defender’s assessments

2 According to the airport authorities, they are considering the maximum planned investments
 3 in security resources summarized in Table 2. We have also included the qualitative deterrent
 4 and detection rates of these measures, as assessed by the airport authorities.

Table 2: Maximum planned investments in security measures

Measure	Max	Annual cost (€)/unit	Deterrence	Detection
Cameras	4	650	Moderate-high	Moderate (persons)
Metal detectors	1	6,500	Moderate	High (material)
X-ray devices	1	90,000	Moderate	High (material)
Police	5	19,200	High	High (persons)
Private security	9	15,600	High	Moderate (persons)

5 We assessed that the number of casualties on the Defender’s side follows a binomial
 6 distribution $y \sim \text{Bin}(m, p_d)$ with a small probability p_d (*indiscriminate killing does not seem*
 7 *to be a target for terrorist in our scenario and, therefore, few casualties are to be expected*
 8 *on the Defender’s side*), which will depend, in turn, on the number of terrorists a . We use
 9 expert judgement to elicit the value of p_d . We start with $p_d = 0.005 \cdot a$. As an illustration,
 10 if we set the number of persons on the Defender’s side present at the moment of the attack
 11 to be $m = 100$, the expected number of casualties during an attack would vary between
 12 0.5 (when only one terrorist performs the attack) and 2.5 (when the cell is composed of
 13 five terrorists). As far as quantifying the value of a human life, we shall use the statistical
 14 value of life (adapted to the country in our scenario), estimating it in 2 million euros for the
 15 Defender, see [Viscusi and Aldy \(2003\)](#) for a review on the topic.

16 We specify now $p_D(f|s_1)$. We use a truncated normal distribution with a mean value μ_f
 17 dependent on the number of attackers succeeding to access the Tower. If $s_1 = 1$, we assume
 18 a smaller impact than when $s_1 \geq 2$. This seems reasonable, since if there is more than one
 19 terrorist taking hold of the ATC Tower, it will be more likely that they will be able to affect,
 20 for longer and with more severe consequences, air traffic operations than if only one of them
 21 is able to get into the ATC Tower. Besides, we also take into account different scenarios

1 for the potential damages caused by terrorists, depending on the air traffic complexity and
 2 density during the attack period. Upon discussion with experts, we considered three possible
 3 scenarios, which are representative of the usual activity at the incumbent airport:

- 4 • Low traffic level (L): one international flight and four training local flights simultane-
 5 ously.
- 6 • Medium traffic level (M): two international flights, one domestic flight and six training
 7 local flights simultaneously.
- 8 • High traffic level (H): four international flights, two domestic flights and eight training
 9 local flights simultaneously.

10 *With all these elements in mind, we assume that the flight diversion and consequences costs*
 11 *follow a truncated normal distribution*

$$12 \quad f \sim \mathcal{TN}(\mu_f | s_1, \sigma_f^2),$$

13 with different expected values depending on s_1 and on the traffic level, which have been as-
 14 sessed through expert elicitation as shown in Table 3. We have also indicated, in parentheses,
 15 the corresponding standard deviation σ_f , as assessed by our experts.

Table 3: Expected cancelation/diversion costs ($s_1 \geq 1$)

	L	M	H
$s_1 = 1$	$5 \cdot 10^4$ ($8 \cdot 10^4$)	10^5 (10^5)	$2 \cdot 10^5$ ($2 \cdot 10^5$)
$s_1 \geq 2$	10^5 (10^5)	$2 \cdot 10^5$ ($2 \cdot 10^5$)	$4 \cdot 10^5$ ($3 \cdot 10^5$)

16 *A similar reasoning can be applied to the model for image costs, which are assumed to*
 17 *follow a truncated normal distribution*

$$18 \quad g \sim \mathcal{TN}(\mu_g, \sigma_g^2 = 10^8).$$

19 However, in this case, the entailed consequences depend on the total number of terrorists

1 initially launching the attack, a , because, even if none of them succeeds in the attack, their
 2 attempt will still have some impact on the airport image. The expected costs, which have
 3 been again elicited with the aid of experts, are shown in Table 4. As we can observe,
 4 the influence of each additional successful terrorist is mitigated. The variance σ_g^2 has been
 5 considered equal for the three scenarios of concern.

Table 4: Expected image costs ($a \geq 1$)

	L	M	H
$\mu_g a$	$10^5 \cdot \sqrt{a}$	$1.5 \cdot 10^5 \cdot \sqrt{a}$	$2 \cdot 10^5 \cdot \sqrt{a}$

6 Regarding the number of terrorists succeeding, killed, detained or escaping on the first
 7 stage of the attack, we shall consider a multinomial distribution, $(s_1, z_1, w_1, a - s_1 - z_1 - w_1) \sim$
 8 $\mathcal{M}(a; \delta'_1, \delta'_2, \delta'_3, \delta'_4)$, with $\delta'_i = \delta_i / \delta_s$, $i = 1, 2, 3, 4$, being $\delta_s = \sum_{i=1}^4 \delta_i$. Using expert opinion,
 9 we adjusted the following expressions for $\delta_1, \delta_2, \delta_3, \delta_4$:

$$\begin{aligned}
 10 \quad \delta_1 &= \gamma_{1,r} \cdot \exp\left(-\sum_{j=1}^5 \gamma_{1,j} x_j\right), \\
 11 \quad \delta_2 &= \gamma_{2,r} \left[1 - \exp\left(-\gamma_{2,4} x_4 - \gamma_{2,5} x_5\right)\right], \\
 12 \quad \delta_3 &= 1 - \exp\left(-\sum_{j=1}^5 \gamma_{3,j} x_j\right), \\
 13 \quad \delta_4 &= \exp\left(-\sum_{j=1}^5 \gamma_{4,j} x_j\right),
 \end{aligned}$$

14 which account for the fact that each additional unit of $(x_1, x_2, x_3, x_4, x_5)$ is expected to reduce
 15 the number of successful and escaped terrorists, and increase the number of terrorists killed
 16 or detained.

17 We have assessed, with the aid of experts, the following values for the incumbent param-
 18 eters, based on the qualitative values shown in the last two columns of Table 2. They reflect
 19 the expected impact of each additional resource on the outcome of the attack, and have been
 20 chosen so that the δ 's are always positive:

- 21 • $\gamma_{1,1} = 0.1, \gamma_{1,2} = 0.15, \gamma_{1,3} = 0.25, \gamma_{1,4} = 0.4, \gamma_{1,5} = 0.2; \gamma_{1,r} = 0.5.$
- 22 • $\gamma_{2,4} = 0.3, \gamma_{2,5} = 0.1; \gamma_{2,r} = 0.3.$

1 • $\gamma_{3,1} = 0.1, \gamma_{3,2} = 0.2, \gamma_{3,3} = 0.25, \gamma_{3,4} = 0.4, \gamma_{3,5} = 0.25$.

2 • $\gamma_{4,1} = 0.15, \gamma_{4,2} = 0.2, \gamma_{4,3} = 0.4, \gamma_{4,4} = 0.45, \gamma_{4,5} = 0.3$.

3 *Specifically, we asked the experts about the expected deterrent effect of each countermeasure*
4 *when considered separately, fitting the expression for δ_i , $i = 1, \dots, 4$ and obtaining the*
5 *corresponding γ 's. As an example, let us consider the expression for δ_3 , assuming that the*
6 *only countermeasure available is private security, x_5 . δ_3 is the parameter of the multinomial*
7 *distribution related with the number of detained terrorists after the first attack. When $x_5 = 0$,*
8 *i.e., if there is no investment, we cannot expect more arrests ($\delta_3 = 0$). On the other hand,*
9 *the experts considered that hiring one security guard is expected to imply the detention of*
10 *one terrorist (for a terrorist cell of five members)¹. With this value, we fitted $\gamma_{35} = 0.25$.*
11 *We checked for consistency of the assessment, asking the experts about the expected increase*
12 *in the detention rate if more than one security guard were to be hired, obtaining consistent*
13 *results. Similar reasonings were used to assess the rest of the involved parameters. The*
14 *value of $\gamma_{1,r}$ expresses the operator's belief that the number of successful terrorists is expected*
15 *to be approximately half the number of those being able to escape when no resources are*
16 *deployed. A similar interpretation holds for $\gamma_{2,r}$, in that the number of killed terrorists is*
17 *expected to be approximately one third of the number of those being detained if all the*
18 *available resources were deployed. To further illustrate these values, let us consider the*
19 *number of police members, x_4 , as if they were the only available preventive measure for the*
20 *Defender. Using the values of the $\gamma_{\cdot,4}$'s, $\gamma_{1,r}$ and $\gamma_{2,r}$ stated above, and assuming that $a = 5$,*
21 *the expected number of succeeding, killed, detained or escaping terrorists for the different*
22 *values of x_4 are shown in Table 5. As we can observe, the contribution of each additional*
23 *police member is mitigated.*

24 Finally, we have assessed, with the aid of experts, a value $k_D = 0.02$ for the risk aversion
25 parameter. We have performed a sensitivity analysis for k_D , suggesting robustness.

¹Recall that the expected values of a multinomial distribution $(n_1, \dots, n_k) \sim \mathcal{M}(N; \delta_1, \dots, \delta_k)$ are $E[n_i] = N \cdot \delta_i$, $i = 1, \dots, k$.

Table 5: Influence of the number of police in the expected outcome of the attack

x_4	0	1	2	3	4	5
Successful	1.67	1.21	0.85	0.59	0.40	0.27
Killed	0.00	0.28	0.51	0.69	0.82	0.92
Detained	0.00	1.19	2.09	2.72	3.13	3.40
Escaped	3.33	2.31	1.54	1.01	0.65	0.41

4.2 Attacker’s assessments

Regarding the probability distribution that the Attacker shall use to describe his uncertainty about $f|s_1$, we also use a truncated normal distribution with the same expected value than the Defender, although with a variance ten times higher. Similarly, we assume that the probability distribution that the Attacker uses to describe his uncertainty about $g|a$ is a truncated normal distribution with the same expected value as the Defender, and a variance ten times higher.

We shall also assume a binomial distribution for the number of terrorists killed after the intervention of the SPF, which will depend on the number of successful terrorists on the first attack, s_1 , provided that $s_1 \geq 1$,

$$s_2 \sim \text{Bin}(s_1, p_t).$$

Since the deployment of the SPF is mandatory, its influence on the number of terrorists killed at this second stage will be similar regardless of any other consideration (defensive measures initially deployed by the Defender, number of terrorists attacking, etc). According to experts’ opinion, there is a probability of 10% that at least one terrorist will be killed during the recovery action, irrespective of the actual number of them occupying the ATC Tower. This corresponds to an approximate value of $p_t \simeq 0.05$. This estimation is subject to uncertainty, although we shall neglect it, since it will not affect significantly the final results.

Regarding the value of a terrorist life, we estimate at about 200,000 euros, whereas we use a value of 100,000 euros if the terrorist is imprisoned. These values seem reasonable since terrorists usually assess their lives at a much less value than those people on the Defender’s side, see e.g. [Viscusi \(2009\)](#). However, unless they are suicide terrorists (which is not the

1 case in our problem), they will still prefer to be imprisoned rather than killed in case of a
 2 failed attack. Nevertheless, the expectation of a long prison term in case they are captured
 3 implies little differences between the two values.

4 Regarding the preparation costs for the Attacker, we assume a fixed cost of 20,000 euros
 5 per involved terrorist, which may account for the need of being armed with weapons and/or
 6 trained as ATCOs, as well as for the time spent on gathering the necessary intelligence in
 7 order to launch a successful attack. Note that we do not take into account uncertainty over
 8 such costs. Finally, we assume a random utility model for the Attacker

$$9 \quad U_A(c) = \exp(k_A \cdot c), \quad k_A \sim \mathcal{U}(0, K_A).$$

10 The Defender thinks that the parameter k_A that determines the Attacker's utility function,
 11 takes a maximum value $K_A = 5$.

12 4.3 Results

13 Based on Table 2, we have 495 feasible portfolios. We use $K = 10000$ in Algorithm 1, for
 14 each of these portfolios. We have first chosen the scenario in which the traffic level is low.
 15 As discussed, for each portfolio x , we have obtained as a result an empirical distribution of
 16 the probability that the Attacker would choose an attack $a \in \mathcal{A}$. Once with the estimation
 17 of $p_{a,x}^D$ for each x , we have solved the Defender's problem, finding the optimal portfolio of
 18 preventive measures which maximizes the Defender's expected utility.

19 Figure 4 shows the Defender's estimated expected utility for all possible portfolios x .
 20 From left to right, the portfolios on the horizontal axis begin with $x = (0, 0, 0, 0, 0)$, $x =$
 21 $(0, 0, 0, 0, 1)$ and so on, sequentially increasing the values in x_5 , x_4 , x_3 , x_2 and x_1 , and
 22 finishing with $x = (4, 1, 1, 2, 0)$. The optimal portfolio $(4, 1, 0, 5, 1)$ is highlighted with a
 23 vertical dashed line.

24 We show in Table 6 the estimated probabilities $p_{a,x}^D$ for some representative portfolios,
 25 together with their corresponding investments. In the first row, we have included the optimal

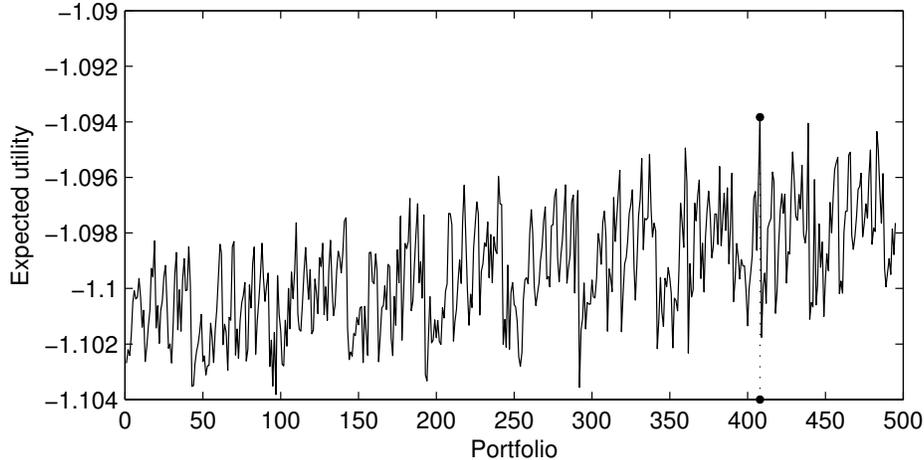


Figure 4: Estimated expected utility for the Defender.

1 portfolio, for which the Defender attains her maximum expected utility, as we comment
 2 below. Besides, we have also included those portfolios in which just one of the preventive
 3 measures attains its maximum allowable value, with no investment in the other measures. For
 4 instance, the second row of Table 6 corresponds to a portfolio in which airport authorities
 5 would have only invested in cameras, acquiring the maximum allowable number of them
 6 (4). Finally, to complete our analysis, we have also considered the five portfolios which
 7 entailed the highest investments. With this, we aim at investigating whether the highest
 8 investments are necessarily the most effective ones, in terms of the Defender’s multiattribute
 9 value function.

10 The optimal portfolio for the Defender corresponds to four cameras, one metal detector, five
 11 policemen and one security member, with an associated investment of 120,700 euros. The
 12 estimated probabilities $p_{a,x}^D$ for this portfolio were (0.61, 0.25, 0.07, 0.04, 0.02, 0.01), which
 13 have the following interpretation. Should the operator choose this optimal portfolio, it would
 14 be highly likely that the terrorists decide not to attack (61%), or that they just launch a
 15 low-profile attack, with only one terrorist (25%). Attacking with two or more terrorists is
 16 not regarded as such a worthy option for the Attacker. Note that the optimal portfolio does
 17 not exhaust the available budget. In this sense, we should mention that the optimal portfolio
 18 implies maximum investments in three of the five resources: cameras, metal detector and

Table 6: Estimated probabilities for some representative portfolios

x	Investment	$P_{a,x}$					
		0	1	2	3	4	5
(4, 1, 0, 5, 1)	120700	0.61	0.25	0.07	0.04	0.02	0.01
(4, 0, 0, 0, 0)	2600	0	0.13	0.26	0.18	0.31	0.12
(0, 1, 0, 0, 0)	6500	0.01	0.06	0.20	0.21	0.21	0.31
(0, 0, 1, 0, 0)	90000	0.01	0.13	0.17	0.21	0.21	0.27
(0, 0, 0, 5, 0)	96000	0.45	0.27	0.11	0.10	0.05	0.02
(0, 0, 0, 0, 9)	140400	0.48	0.29	0.08	0.09	0.05	0.01
(4, 1, 1, 1, 2)	149500	0.30	0.36	0.13	0.09	0.08	0.04
(4, 1, 0, 0, 9)	149500	0.41	0.36	0.11	0.07	0.03	0.02
(3, 0, 1, 3, 0)	149550	0.35	0.30	0.16	0.12	0.06	0.01
(3, 0, 0, 2, 7)	149550	0.54	0.31	0.08	0.03	0.03	0.01
(1, 1, 0, 5, 3)	149950	0.48	0.36	0.07	0.07	0.01	0.01

1 police. On the contrary, there would be no investment in the most expensive resource, the
2 X-ray device. This seems reasonable, since its higher efficiency, relative to the other related
3 resources (e.g. metal detectors; compare the values of $\gamma_{,2}$'s and $\gamma_{,3}$'s), is beaten by its
4 comparatively much higher costs. A similar reasoning holds for the investment in private
5 security: only one of the maximum nine allowable units would be hired. Although their
6 salaries are lower than those of a police member, this is not compensated by the fact that
7 they are less efficient than the police (compare the values of $\gamma_{,4}$'s and $\gamma_{,5}$'s).

8 With regards to the other portfolios displayed in Table 6, it is interesting to note that
9 those including high numbers of police and/or private security members imply higher prob-
10 abilities of not being attacked by the terrorists. On the other hand, investing mainly in
11 technological resources does not seem to bring such good results. The most extreme cases
12 are portfolios (4, 0, 0, 0, 0), (0, 1, 0, 0, 0) and (0, 0, 1, 0, 0), for which terrorists would be prone
13 to attack with several members. This is especially symptomatic in the case when the oper-
14 ator would only invest in the X-ray device: in spite of the high costs, the deterrent effect
15 seems quite limited.

16 The above results are sensitive to changes in the estimation of the entailed consequences to
17 the airport in case of a successful attack. In this regard, we have repeated our calculations

1 considering the two other scenarios regarding the traffic level. For the high traffic level
2 scenario, the optimal portfolio was $(4, 1, 0, 4, 4)$, corresponding to four cameras, one metal
3 detector, four policemen and four security members. It has an associated investment of
4 148,300 euros, and an estimated probability $p_{a,x}^D = (0.09, 0.47, 0.17, 0.13, 0.09, 0.05)$ for $a =$
5 $, 0, 1, \dots, 5$. As we can observe, under this new scenario of higher expected losses, the
6 operator would opt for a more expensive portfolio, exhausting almost entirely the available
7 budget. Again, it becomes clear that it is worthier for the operator to invest in human
8 resources than in expensive technological measures.

9 Finally, we briefly comment the case of medium traffic level. The optimal portfolio
10 was $(4, 1, 0, 5, 2)$, corresponding to four cameras, one metal detector, five policemen and
11 two security members. It has an associated investment of 136,300 euros, and an estimated
12 probability $p_{a,x}^D = (0.48, 0.36, 0.08, 0.02, 0.04, 0.01)$ for $a = , 0, 1, \dots, 5$.

13 However, our aim is to provide airport authorities with a unique security plan, which
14 should be adequate for all day periods. Analyzing the three proposed scenarios and their
15 associates optimal portfolios, we conclude that, in order to protect the airport in the best
16 manner throughout the whole day, the optimal alternative would be to implement the optimal
17 portfolio for the medium traffic level scenario, i.e., $x = (4, 1, 0, 5, 2)$, which entails a moderate
18 investment.

19 Summarizing, we have observed the following trends in the Attacker's behavior after
20 performing our analysis. Under the scenario of an airport which will incur in big losses if
21 a terrorist attack occurs, the terrorists would behave in the following manner: (1) They
22 tend to be cautious when they see that the defensive measures are too intense, typically
23 choosing attacking with, at most, only one terrorist; (2) Otherwise, if they feel that the ATC
24 Tower is vulnerable, they would launch the most powerful attack they can; and (3) Only in
25 case of doubt, when they do not perceive with clarity any of the situations mentioned above,
26 they would opt for an intermediate strategy, sending between two to four attackers. However,
27 should the terrorists feel that the damages inflicted to the airport will not be so considerable,
28 their strategy would change radically. Although they are considered as risk seekers, they also

1 put a certain value to their lives and, therefore, they will not put themselves in unnecessary
2 risk if the chances of causing spread and costly damages to airport authorities are reduced.

3 In the light of our analysis, it is clear that not always the most expensive measures are
4 the most appropriate ones for a given situation. Furthermore, it is also important to remark
5 that experts' opinion should be always taken into account when devising security plans.

6 **5 Discussion**

7 We have analyzed the case study of an airport, threatened by the possibility of a terrorist
8 attack aimed at taking control over the ATC Tower. The operator has a set of feasible
9 portfolios of preventive measures she could invest in. The Attacker would decide to attack
10 or not with a given power depending on the preventive measures deployed by the operator.
11 In case of a successful attack, the operator would call on a Special Police Force, who will be
12 in charge of the situation, trying to recover the ATC Tower as soon as possible. In devising
13 a suitable model for this problem, we have taken into account all relevant consequences for
14 the operator, in terms of lives lost and operations and image consequences, incorporating
15 also the inherent uncertainty. In a similar way, we have assessed the consequences for the
16 Attacker, in terms of preparation costs, lives lost or possibility of being imprisoned, and
17 the revenue they aim at obtaining: disrupting air traffic and bringing about, as much as
18 possible, economical and political damage to airport authorities and governments. We have
19 also taken into account uncertainty on these quantities. We have addressed the problem as
20 a particular case of a Sequential Defend-Attack model within the Adversarial Risk Analysis
21 framework. The final aim of the model was to give advise to the Defender for devising a
22 security plan. In this regard, we have highlighted the need of assessing in a precise way the
23 efficiency of all available resources before making a decision on where to invest.

24 The proposed methodology may be used for other cases related to airport security, as
25 e.g. unlawful interference with apron, airside and/or security checks, cyber-attacks to the
26 ATC or bioterrorism, among others. It could be also adapted to deal with similar security

1 problems involving critical infrastructures, or alternative transportation means. We have
2 only considered a single site to protect, but the extension to multiple site protection is
3 relevant in applications. In this case, additional constraints should be placed on the available
4 portfolios of countermeasures, since some of them might have to be shared among the
5 different sites.

6 **Acknowledgements**

7 Work supported by the Spanish Ministry of Economy and Innovation program MTM2011-
8 28983-C03-01, the Government of Madrid RIESGOS-CM program S2009/ESP-1685 and the
9 EU-FP7 program SECONOMICS, grant number 285223. We are grateful to airport experts
10 and stakeholders for fruitful discussion about modeling issues.

11 **References**

- 12 G. S. Becker. Crime and punishment: An economic approach. *Journal of Political Economy*,
13 76(2):169–217, 1968.
- 14 A. Cook, G. Tanner, and A. Lawes. The hidden cost of airline unpunctuality. *Journal of*
15 *Transport Economics and Policy*, 46(2):157–173, 2012.
- 16 D. B. Cornish and R. V. Clarke. *The Reasoning Criminal: Rational Choice Perspectives on*
17 *Offending. Reprint 2011*. Research in Criminology. Springer, London, 1986.
- 18 J. S. Dyer and R. K. Sarin. Measurable multiattribute value functions. *Operations Research*,
19 27(4):810–822, 1979.
- 20 J. S. Dyer and R. K. Sarin. Relative risk aversion. *Management Science*, 28(8):875–886,
21 1982.
- 22 M. R. Haberfeld and A. von Hassell. *A New Understanding of Terrorism: Case Studies,*
23 *Trajectories and Lessons Learned*. Humanities, Social Sciences and Law. Springer, 2009.

- 1 J. P. C. Kleijnen and R. G. Sargent. A methodology for fitting and validating metamodels
2 in simulation. *European Journal of Operational Research*, 120(1):14–29, 2000.
- 3 B. Lomborg. *Solutions for the World’s Biggest Problems. Costs and Benefits*. Cambridge
4 University Press, 2008.
- 5 J. Merrick and G. S. Parnell. A comparative analysis of PRA and intelligent adversary
6 methods for counterterrorism risk management. *Risk Analysis*, 31(9):1488–1510, 2011.
- 7 J. Pearl. Influence diagrams—Historical and personal perspectives. *Decision Analysis*, 2(4):
8 232–234, 2005.
- 9 J. Ríos and D. Ríos Insua. Adversarial risk analysis for counterterrorism modeling. *Risk*
10 *Analysis*, 32(5):894–915, 2012.
- 11 D. Ríos Insua, J. Ríos, and D. Banks. Adversarial risk analysis. *Journal of the American*
12 *Statistical Association*, 104(486):841–854, 2009.
- 13 W. K. Viscusi. Valuing risks of death from terrorism and natural disasters. *Journal of Risk*
14 *and Uncertainty*, 38(3):191–213, 2009.
- 15 W. K. Viscusi and J. E. Aldy. The value of a statistical life: a critical review of market
16 estimates throughout the world. *Journal of Risk and Uncertainty*, 27(1):5–76, 2003.