D5.1 - Basic Models for Security Risk Analysis

Document author(s) and Company – D. Ríos, J. Cano (URJC), W. Shim, F. Massacci (UNITN), A.Schmitz (Fraunhofer ISST)

Pending of approval from the Research Executive Agency - EC

Document Number	D5.1
Document Title	Basic Models for Security Risk Analysis
Version	3.0
Status	Final
Work Package	WP 5
Deliverable Type	Report
Contractual Date of Delivery	31.01.2013
Actual Date of Delivery	31.01.2013
Responsible Unit	URJC
Contributors	UNITN, Fraunhofer ISST
Keyword List	Adversarial risk; security risk; game theory; decision analysis
Dissemination level	PU

SECONOMICS Consortium

SECONOMICS "Socio-Economics meets Security" (Contract No. 285223) is a Collaborative project) within the 7th Framework Programme, theme SEC-2011.6.4-1 SEC-2011.7.5-2 ICT. The consortium members are:

1	UNIVERSITÀ DEGLI STUDI DI TRENTO	Università Degli Studi di Trento (UNITN) 38100 Trento, Italy http://www.unitn.it	Project Manager: Prof. Fabio Massacci Fabio.Massacci@unitn.it
2	DEEPBLUE	DEEP BLUE Srl (DBL) 00193 Roma, Italy http://www.dblue.it	Contact: Alessandra Tedeschi Alessandra.tedeschi@dblue.it
3	Fraunhofer ISST	Fraunhofer Institute for Software and Systems Engineering ISST Emil-Figge-Straße 91 44227 Dortmund, Germany http://www.isst.fraunhofer.de/en/	Contact: Prof. Jan Jürjens jan.juerjens@isst.fraunhofer.de
4	Universidad Rey Juan Carlos	UNIVERSIDAD REY JUAN CARLOS, Calle Tulipán s/n, 28933, Móstoles (Madrid), Spain. http://www.urjc.es	Contact: Prof. David Ríos Insua david.rios@urjc.es
5	UNIVERSITY OF ABERDEEN	THE UNIVERSITY COURT OF THE UNIVERSITY OF ABERDEEN, King's College Regent Walk, AB24 3FX, Aberdeen, United Kingdom http://www.abdn.ac.uk/	Contact: Prof. Julian Williams julian.williams@abdn.ac.uk
6	TMB Transports Metropolitans de Barcelona	FERROCARRIL METROPOLITÀ DE BARCELONA S.A., Carrer 60 Zona Franca, 21-23, 08040, Barcelona, Spain http://www.tmb.cat/ca/home	Contact: Michael Pellot mpellot@tmb.cat
7	Atos	ATOS ORIGIN SOCIEDAD ANÓNIMA ESPAÑOLA, Calle Albarracín, 25, 28037, Madrid, Spain http://es.atos.net/es-es/	Contact: Silvia Castellvi Català silvia.castellvi@atosresearch.eu
8	SECURENOK	SECURE-NOK AS, Professor Olav Hanssensvei, 7A, 4021, Stavanger , Norway Postadress: P.O. Box 8034, 4068, Stavanger, Norway http://www.securenok.com/	Contact: Siv Houmb sivhoumb@securenok.com
9	SOU Institute of Sociology AS CR	INSTITUTE OF SOCIOLOGY OF THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC PUBLIC RESEARCH INSTITUTION, Jilska 1, 11000, Praha 1, Czech Republic http://www.soc.cas.cz/	Contact: Dr. Zdenka Mansfeldová zdenka.mansfeldova@soc.cas.cz
10	nationalgrid THE POWER OF ACTION	NATIONAL GRID ELECTRICITY TRANSMISSION PLC, The Strand, 1-3, WC2N 5EH, London, United Kingdom http://www.nationalgrid.com/uk/	Contact: Dr. Raminder Ruprai Raminder.Ruprai@uk.ngrid.com
11	ANADOLU ÜNİVERSİTESİ	ANADOLU UNIVERSITY, SCHOOL OF CIVIL AVIATION Iki Eylul Kampusu, 26470, Eskisehir, Turkey http://www.anadolu.edu.tr/akademik/yo_svlhvc/	Contact: Nalan Ergun nergun@anadolu.edu.tr

Document change record

Version	Date	Status	Author (Unit)	Description
0.1	12/09/2012	Draft	D. Ríos, J. Cano (URJC)	First draft
0.2	12/11/2012	Draft	D. Ríos, J. Cano (URJC)	First version
0.3	13/12/2012	Draft	W. Shim, F. Massacci (UNITN)	Scientific revision
0.4	15/12/2012	Draft	W. Shim, F. Massacci (UNITN)	Adaption of paper by W. Shim, L. Allodi and F. Massacci (UNITN) added as Annex 6 in the deliverable
0.5	17/12/2012	Draft	E. Chiarani (UNITN)	Quality check completed. Minor changes requested
0.6	20/12/2012	Draft	A.Schmitz (Fraunhofer ISST)	Algorithmic improvements
1.0	30/12/2012	First version	D. Ríos, J. Cano (URJC)	Rewrite with all suggestions and minor modification
1.1	10/01/2013	First version	W. Shim, F. Massacci (UNITN)	Scientific review
1.2	22/01/2013	First version	M. Angeli (UNITN)	Quality check
1.3	24/01/2013	First version	J. Williams (UA)	Final scientific review
2.0	25/01/2013	Final	D Ríos, J. Cano (URJC)	Finalized version ready to be submitted
3.0	15/11/2013	Final	D Ríos, J. Cano (URJC)	Response to Project Officer comments

Index

Executive summary

This report provides several template models aimed at devising strategies for the protection of critical infrastructures or, more generally, at supporting security policy making. The template models are based on the adversarial risk analysis framework. While risk analysis provides a methodology to mitigate the effects of threats that may harm the performance of a system, adversarial risk analysis expands the methodology focusing on threats coming from intelligent intentional adversaries. Specifically, we have developed five different models to support a Defender in facing the actions of an Attacker. The models differ from each other in the way and order in which the possible attacks and defences take place within the sequence of events. Thus, we have given the models self-explanatory names: (a) **Simultaneous Defend-Attack**, in which a defender and an attacker decide their defence and attack, respectively, without knowing the action chosen by each other; (b) **Sequential Defend-Attack**, in which the defender first chooses a defence and, then, having observed it, the attacker chooses an attack; (c) **Sequential Attack-Defend**, in which the attacker first performs an attack and, then, having suffered it, the defender chooses a defence; (d) **Sequential Defend-Attack-Defend**, in which the defender first deploys defensive resources. Then, the attacker, having observed such decision, performs an attack and, finally, the defender tries to recover from the attack as best as she can; and (e) **Sequential Defend-Attack with Private Information**, similar to the Sequential Defend-Attack, but with some information that the defender does not want the attacker to know.

These five models may be seen as basic building blocks for general risk analysis problems related with the protection of critical infrastructures. For each model, we provide the following information: (1) A general description of the model, emphasising its most relevant features; (2) A simple motivating example, dealing with some related problem regarding the protection of critical infrastructure; (3) The standard game theoretic solution. This is a classic approach, overcome by the adversarial risk analysis methodology, although some of its concepts are useful as a starting point to understand our template models; (4) The approach from the view of adversarial risk analysis. This is the main part of our document, dealing with all the theoretical and modelling aspects of our models; and (5) A basic numerical illustration in a stylised problem. This case study will complete in full detail the ideas sketched in the introductory example. For the sake of clarity, all examples will be placed at the end of this document, on a separate annex.

We also illustrate how the templates may be adapted in more realistic problems, specifically in a security resource allocation problem within a spacial setting, i.e. when assets and values are distributed among various nodes (cells). This may be viewed essentially as a set of adversarial risk analysis models, one for each cell, with models coordinated by resource constraints and value aggregation across each cell for both the Defender and the Attacker. We end up discussing issues in opponent modelling, in which our aim is to provide models for the decision making of all the participants.

1. Introduction

Game theory and other group decision making paradigms have long been considered of little relevance for practical risk management decision-making, see Bier and Cox Jr (2007). This viewpoint has recently become less dogmatic because:

- High-profile terrorist attacks have demanded significant national investment in protective responses, and there is public concern that not all of these investments are prudent and/or effective, see Parnell et al. (2008).
- Key business sectors (especially finance, e-commerce, and software) have become much more mathematically sophisticated, and are now using this expertise to shape corporate strategy for auction bidding, lobbying efforts, and other decisions, see McAfee and McMillan (1987) or Rothkopf (2007).
- Regulatory legislation must balance competing interests (for growth, environmental impact, safety) in a way that is credible and transparent, see Heyes (2000).
- The on-going arms race in cybersecurity means that the financial penalties for myopic protection are large and random, see Killourhy et al. (2004).

The involved challenges cross many fields (Statistics, Economics, Operations Research, Engineering, Sociology, Political Science, etc.) and are characterised by the fact that there are two or more intelligent opponents who make decisions for which the outcome is uncertain. Collectively, we call this problem area Adversarial Risk Analysis (ARA).

Traditional statistical risk analysis grew in the context of nuclear reactor safety, insurance, and other applications in which loss was governed by chance rather than the malicious (or self-interested) actions of intelligent actors. But in ARA, one needs to have some model for the decision-making of all the participants. This model might be classically game-theoretic, with (non-cooperative) Nash equilibria as core concept, see Myerson (1997), or it might be more psychological, reflecting either a decision analytic formulation, see Kadane and Larkey (1982), or empirical studies of game behaviour, see Camerer (2003).

Specifically regarding counterterrorism, appropriate responses to security represent one of the key challenges for states in this century, see English (2010) or Lomborg (2007). Indeed, after recent large-scale terrorist attacks, multi-billion euro investments are being made to increase safety and security. This has stirred public debate about the convenience of such measures. In turn, this has motivated a great deal of interest in modelling issues in relation with counterterrorism, with varied techniques and tools from fields such as reliability analysis, data mining, or complex dynamic systems. Recent accounts of various techniques and applications may be seen in Ezell et al. (2010), Gutfraind (2009) or Wein (2009). Parnell et al. (2008) and Enders and Sandler (2011) provide overviews on strategies, models, and research issues in terrorism risk analysis. As mentioned, the key feature of these problems is the presence of intelligent opponents whose decision outcomes are uncertain and interdependent. Thus, it is no wonder that much of this research has reminiscent game-theoretic and risk analytic flavors. Parnell et al. (2008) provided an in-depth review for the US National Academy of Sciences on bioterrorist assessment models, with important conclusions, including the inadequacy of traditional risk analysis tools, like fault trees, for not accounting for intentionality; the critical common knowledge assumption of game theoretic based

approaches; and, finally, the problems of decision analytic based approaches in forecasting adversarial actions. The role of standard risk analysis in the management of terrorism risks has been discussed in Deisler Jr (2002). Also, Garrick (2002) points out some of the challenges associated with extending standard risk assessment methods for the analysis of threats from terrorist acts. Dillon et al. (2009) describe a decision making framework based on risk analysis principles for allocating anti-terrorism resources using risk scores. Ezell et al. (2010) defend the use of traditional probabilistic risk assessment methods like event trees to estimate terrorism risks.

These approaches, based on the direct application of conventional risk analysis methods to terrorism risk management, have been criticised by Cox Jr (2009a) and Brown and Cox Jr (2011), who warn about the inappropriateness of modelling the actions from terrorists in essentially the same way as random adverse events in natural or engineered systems. On the other hand, there is a rich literature in political sciences and economics regarding game theory and terrorism, though it places little emphasis on risk analysis aspects, see Siqueira and Sandler (2006), Arce and Sandler (2007) or Powell (2007). Recent relevant references with a game-theoretic flavour include various papers by Brown et al. (2005, 2006, 2008) who present bilevel (max-min, minmax) and trilevel (min-max-min) optimization models for three stylised counterterrorism models such as defender-attacker, attacker-defender, and defender-attacker-defender problems. Kardes and Hall (2005) survey various approaches to strategic decision making in the presence of adversaries, arguing for the use of robust stochastic games to deal with counterterrorism, pointing out to the difficulty in assessing what the adversary aims at doing in this context. The book edited by Bier and Azaiez (2009) contain many papers on the attacker-defender model and several variants and applications. Insights combining risk analysis and game theory can be found in Hausken (2002) and Cox Jr (2009b).

A thread in the above game-theoretic approaches is the common knowledge assumption, criticised, for example, in Raiffa et al. (2002). Most versions of game theory assume that the opponents not only know their own payoffs, preferences, beliefs, and possible actions, but also those of their opponents. Moreover, when there is uncertainty in the game, it is assumed that players have common probabilities over the uncertain variables. This strong common knowledge assumption allows a symmetric joint normative analysis in which players try to maximise their expected utilities (and expect the other players to do the same). Therefore, their decisions can be anticipated and are predated by Nash equilibria concepts. However, in counterterrorism contexts, players will not typically have full knowledge of their opponent's objectives, beliefs, and possible moves. This is aggravated as participants try to conceal information.

The other mainstream literature in the field has a decision analytic flavor. Among others, Pinker (2007) uses qualitative influence diagrams to assess short and long-term deployment of countermeasures; Merrick and McLay (2010) use decision trees and influence diagrams from the point of view of the defender to model the decision of installing radiation sensors to screen cargo containers against terrorist radiological threats; and Parnell et al. (2010) describe canonical terrorist multiobjective decision trees and influence diagrams to evaluate bioterrorist threats. Their recurrent issue is the difficulty in assessing the probabilities over the actions of the adversaries, which is the key objection, see Harsanyi (1982), to the Bayesian approach to games, introduced by Kadane and Larkey (1982), Raiffa et al. (2002) and Raiffa (1982). Banks and Anderson (2006) provide a numerical comparison of classi-

cal and Bayesian approaches to games within a smallpox attack problem. Paté-Cornell and Guikema (2002) present an interesting perspective, suggesting to address the problem of assessing the probabilities of possible attacks by modelling the attacker's problem from the point of view of the defender, based on point estimates of the attacker's probabilities and utilities. Then, they assess the expected utilities of the attacker's actions and estimate the probabilities of these actions as proportional to the attacker's perceived expected utilities. This approach does not take proper account of the fact that the (idealised) attacker is an expected utility maximiser and, thus, would certainly choose the optimal action. Another possibility would be to undertake a sensitivity analysis approach, see Ríos Insua and Ruggeri (2000), taking into account our imprecision about the likely actions of our adversary. This is the venue adopted by von Winterfeldt and O'Sullivan (2006) within a simple decision tree to evaluate man-portable air defence systems countermeasures. This may be too involved computationally in complex problems.

Many of those models previously commented combine risk analysis, decision analysis and game theory, as reviewed in Merrick and Parnell (2011) who comment favorably about Adversarial Risk Analysis (ARA), introduced in Ríos Insua et al. (2009). In supporting one of the participants, ARA views the security resource allocation problem as a decision analytic one, but procedures which employ the game theoretical structure, and other information available, are used to estimate the probabilities of the opponents' actions.

Summarising, ARA aims at providing one-sided prescriptive support to one of the intervening agents, the defender, based on a subjective expected utility model, treating the adversary's decisions as uncertainties. In order to predict the adversary's actions, we model his decision problem and try to assess his probabilities and utilities. Assuming that the adversary is an expected utility maximiser, we can predict the adversary's actions by finding his maximum expected utility action. Our uncertainty about the adversary's probabilities and utilities is propagated over to the adversary's decision. Sometimes, such assessment may lead to a hierarchy of nested decision problems, as described in Ríos Insua et al. (2009), close to the concept of k-level thinking, see Stahl and Wilson (1995).

In this deliverable we provide in Section 2 an initial motivation of how Risk Analysis has derived into Adversarial Risk Analysis over the last few years. We then apply the ARA framework to five prototypical models relevant in security risk analysis in Section 3. Two of them (specifically, the Sequential Defend-Attack and the Simultaneous Defend-Attack models) will be analysed in detail, whereas the three others (the Sequential Attack-Defend, the Sequential Defend-Attack-Defend and the Sequential Defend-Attack with Private Information) will be addressed in detail in corresponding annexes. These basic models may be used as templates for general security risk models. Finally, in Section 4 we will describe how the previous templates can be adapted for the incumbent problems to take into account the problem topology, possible constraints over resources and other complicating features.

We include six annexes at the end of this document. The first three describe in more detail the Sequential Attack-Defend Model, the Sequential Defend-Attack-Defend Model, and the Sequential Defend-Attack with Private Information Model. The fourth annex contains detailed examples of the models above, illustrating real world scenarios. The fifth annex outlines how the Sequential Defend-Attack-Defend can be adapted for spacial settings. Finally, in the last annex we present a study of strategies for mitigating attacker's malicious activities, which uses a simple game-theoretic Attack-Defend model. This would help one understand better about how to design effective strategies relevant to security problems.

For all the models, we first provide a thorough description of them, using influence diagrams and decision trees as well as a simple example. We then analyse the models from a game theoretical perspective, and, after criticising such approach, we provide the ARA solution and illustrate the corresponding model with an example. We shall assume two participants, the Attacker (He), and the Defender (She). We aim at supporting the Defender in making her decisions. Our agents' decisions will be termed, generically, as defences and attacks. Depending on the context (strategic, tactical, operational), these may be viewed as security policies, security policy levels, security resource allocations or security plans, among others. Unless stated otherwise, we shall assume discrete sets of alternatives for both the Attacker and the Defender.

The relevance of this document in relation with the other deliverables of WP5, *D5.2 - Case Studies in Security Risk Analysis*, and *D5.3 - Describing a General Methodology for Critical Infrastructure Protection Risk Analysis*, is evident. According to the DoW, D5.1 will lead the development of template risk analysis models for application in the case studies. Taking D5.1 as a starting point, D5.2 will explore the modification of the template models after application and start the development of the general methodology in D5.3. Moreover, based on the results obtained in D5.1 and D5.2, D5.3 will provide information and documentation to the WP8 leader to facilitate tool development.

This latter aspect makes reference to the interaction of this deliverable with WP8. But there are actually relationships with all other WPs within the SECONOMICS project. Regarding WP1–WP3, we have fed our models with information coming from experts and stakeholders of the corresponding Wps. We shall further explore and adapt the templates to the cases proposed in such WPs in D5.2 (and D5.3). On the other hand, WP4 has provided us with ideas about what to model within the relevant utility functions to be further used when solving the case studies. The collaboration with WP6 has been also very fruitful, since our aim is to combine our models with those in WP6. Therefore, intense conversations have taken place in order to start with the integration of both methodologies. Finally, WP7 has given constant advice in determining which of the models presented here may be relevant in general security problems and how they may be used in other application areas.

2. From Risk Analysis to Adversarial Risk Analysis

This section reviews a schematic framework that formalises standard risk analysis, assessment, and management methods as in Haimes (2004) or Bedford and Cooke (2001), adapted to the classic proposal of Kaplan and Garrick (1981). Influence diagrams are used to structure problems. For simplicity, we assume that losses can be monetised as costs associated with interventions. All the participating agents are assumed to be expected utility maximisers, see French and Ríos Insua (2000).

Figure 1 shows an *influence diagram*, see Pearl (2005), that displays the simplest version of a non-adversarial risk management problem. An influence diagram is a directed acyclic graph with three kinds of nodes: decision nodes, shown as rectangles; uncertainty nodes, shown as ovals; and value nodes, shown as hexagons. A *functional arrow* ends in a value node, and indicates that the utility function depends on the immediately preceding nodes. A *conditional arrow* ends at an uncertainty node, indicating that the probabilities at the head depend on the values of the nodes at its tail. An *informational arrow* ends at a decision node, indicating that, when the decision is made, the values of the preceding node are known.

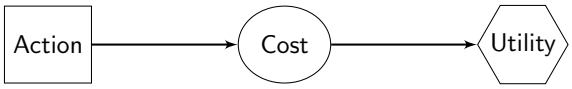


Figure 1: Basic influence diagram

In Figure 1, the rectangle represents the set $\mathcal{A}$ of possible decisions or actions, the oval represents the costs associated with the decisions, and the hexagon represents the net consequences in terms of the decision-maker's utility function. It corresponds to a problem in which an organization has to make a decision a from a set $\mathcal{A}$ of choices. The cost c that results from each decision is uncertain and is modelled through the density $\pi(c|a)$. The utility $u(c)$ of the cost is decreasing and typically non-linear: costs are bad, and catastrophic costs are disproportionately bad. One should seek the decision that maximises the expected utility

$$\psi = \max_{a \in \mathcal{A}} \left[\psi(a) = \int u(c)\pi(c|a)dc \right]. \tag{1}$$

In practice, the cost for a particular action is complex and conditional; it includes fixed and random summands. The organization will typically perform a risk assessment to:

1. identify disruptive events $E_1, E_2, \ldots, E_k$ (these may be assumed to be mutually exclusive);
2. assess their probabilities of occurrence, $P(E_i|a) = q_i(a)$; and,
3. assess the cost c_i conditional on the occurrence of E_i and decision a (these costs are typically random).

It is convenient to let E_0 be the event that there are no disruptions, with probability $q_0(a)$. Figure 2 shows the influence diagram that extends the previous formulation to include risk assessment.

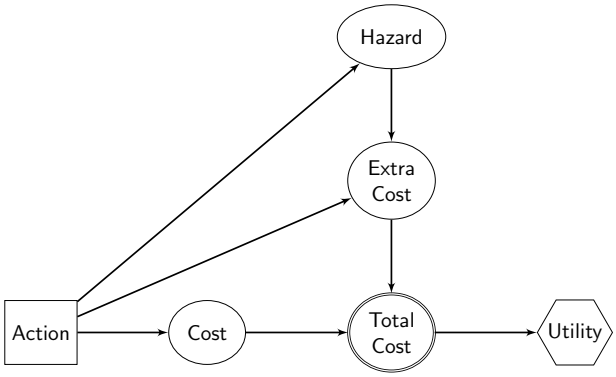


Figure 2: Influence diagram with risk assessment

Let $\boldsymbol{q}(a)$ be the vector of probabilities corresponding to decision a and let $\pi_i(c|a)$ be the cost density for decision a, if event E_i occurs. Then, the density of the cost for decision a is the mixture $\sum_{i=0}^{k} q_i(a)\ \pi_i(c|a)$. Once the risk assessment is performed, the organization wants the maximum expected utility decision, which is found by solving:

$$\psi_r = \max_a \left[\psi_r(a) = \sum_{i=0}^{k} q_i(a) \int u(c)\pi_i(c|a)\, dc \right].$$

In some cases, the probabilities $q_i(a)$ are themselves uncertain, e.g., if one is combining assessments from multiple experts. In that case, one can describe that uncertainty through a distribution $g(\boldsymbol{q}(a))$ on the unit simplex S in $\mathbb{R}^{k+1}$ and solve:

$$\psi_r = \max_a \left[\psi_r(a) = \int_S g(\boldsymbol{q}(a)) \left(\sum_{i=0}^{k} q_i(a) \int u(c)\pi_i(c|a)\, dc \right) d\boldsymbol{q}(a) \right]. \tag{2}$$

Note that this maximises the utility with respect to uncertainty from two different sources—the randomness in the costs and the imprecise knowledge about the disruption probabilities.

Consider the difference $\psi - \psi_r$. This is non-negative, as ψ describes a decision problem without including the costs associated to disruptive events, whereas ψ_r relies upon risk assessment and is more realistic. To reduce this difference, organizations often undertake a risk management strategy. This introduces an additional set of choices $\mathcal{M}$, e.g., contingency plans or insurance policies; these tend to lower the costs associated with particular disruptions and/or lower the chance of disruption.

As an example, imagine that a country is deploying security forces to defend some particular critical installations within its territory. The country considers three possible deployment strategies, these being the decisions in $\mathcal{A}$. But the risk assessment indicates the possibility of security threats against different installations or staff from those initially expected by the country officers. The country therefore considers sending more security personnel (which would protect against the costs associated with both hazards), or investing in building deterrent infrastructures around the perimeter of the installations (at more expense, but with less chance of suffering sabotages or attacks) or doing neither. These choices are the elements in $\mathcal{M}$.

In principle, one could take the cross product of sets $\mathcal{A}$ and $\mathcal{M}$ and then solve for ψ_r over this extended set. But in practice, it is often helpful for managers to keep these distinct. The risk management solution remains the same,

$$\psi_m = \max_{(a,m)\in\mathcal{A}\times\mathcal{M}} \psi_r(a,m) \tag{3}$$

where, in an obvious extension of the previous notation,

$$\psi_r(a,m) = \sum_i q_i(a,m) \int u(c)\pi_i(c|a,m)\,dc.$$

As before, a slightly more complicated formula applies when there is uncertainty in the $q_i(a,m)$ probabilities. Figure 3 shows the influence diagram for a risk management problem.

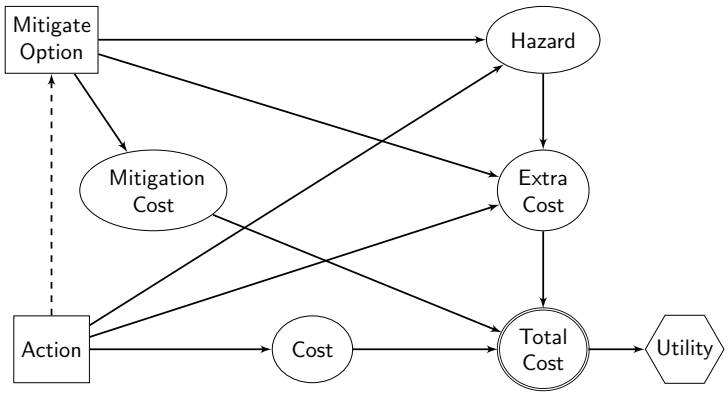


Figure 3: Influence diagram with risk management

Since risk management extends the set of choices, $\psi_m \geq \psi_r$, but both are still less than ψ. The solution of (3) requires dynamic programming. The choice sets may be discrete (as implied in our notation) or continuous (e.g., if the country officers can choose among defensive investment measures with infinitely divisible costs). Clearly, additional complexity arises if there is sequential investment, if one allocates risk management resources according to a portfolio analysis, and if there are multiattribute utility functions.

2.1 Adversarial Risks: Modelling

We now consider the situation in which there are adversaries whose actions affect each other's risks. Assume that there are just two opponents (the Attacker and the Defender). Their decision problems are structurally similar: both can take actions that affect the costs of the other, and both seek to maximise their expected utilities. The sets of actions for the Attacker and the Defender are, respectively, denoted by $\mathcal{A}$ and $\mathcal{D}$; their utility functions are $u_A(\cdot)$ and $u_D(\cdot)$; and their collection of probabilities about outcomes are $\mathcal{P}_A$ and $\mathcal{P}_D$.

In this kind of situations, the Attacker and the Defender may have different utility functions and different probability assessments of the costs. Each player may know his own payoffs

but the other's payoffs and beliefs may be unknown. One example is that of urban security resource allocation to protect urban spaces. A defender is protecting a certain place from the threats of an attacker. Such place will have a certain value for the defender and the attacker; neither part knows what utility the other puts upon it. Furthermore, contenders may also be uncertain about their own place valuation. Similarly, a situation with different probability assessments might arise in counterterrorism, where both parties could have intelligence that leads to very different estimates for the probability of successful attack under different Attacker/Defender choices.

To illustrate these cases we modify in Figure 4 the usual influence diagram to show the interaction between the decisions of the Attacker and the Defender. Specifically, to simplify our discussion, we essentially consider symmetric diagrams for the Attacker and the Defender, with interventions aimed at increasing the adversarial risks, impacting the likelihood and extra costs of the hazards. We expect this symmetry to be typical of corporate adversarial decisions whereas in counterterrorism scenarios we shall expect more asymmetries.

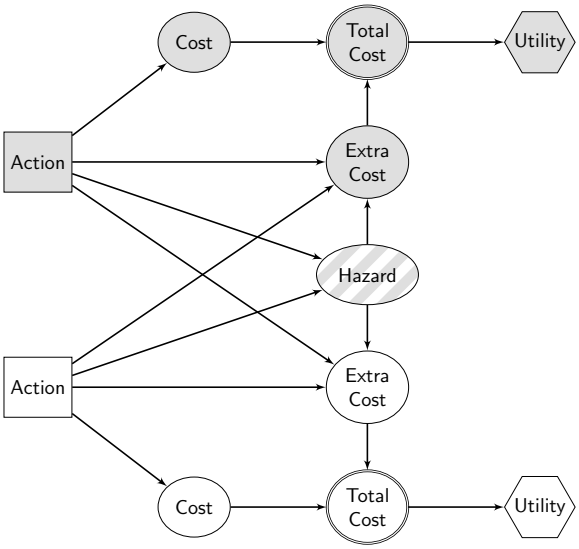


Figure 4: Symmetric adversarial risk influence diagram

For the ARA case, the expected utilities of the Attacker and the Defender depend upon the actions of both. Specifically, extending (1), the utility that the Attacker expects from choosing action $a \in \mathcal{A}$ when the Defender makes decision $d \in \mathcal{D}$ is

$$\psi_A(a,d) = \int u_A(c)\pi_A(c|a,d)dc$$

where $\pi_A(c|a,d) \in \mathcal{P}_A$ represents the Attacker's beliefs about the distribution of his costs for the decision pair (a,d). As in (2), the Attacker can identify events $E_1,\ldots,E_k$ that affect his costs and include their impact explicitly:

$$\psi_A(a,d) = \int_S g_A(\boldsymbol{q}(a,d)) \left(\sum_i q_i(a,d) \int u_A(c)\pi_A(c|a,d,E_i)\,dc \right) d\boldsymbol{q}(a,d) \qquad (4)$$

where $g_A(\cdot)$, $\boldsymbol{q}_A(a,d)$, $\pi_A(c|a,d,E_i) \in \mathcal{P}_A$. The expected utility $\psi_D(a,d)$ for the Defender is analogous. In this framework, the key remaining problem is to determine how the Attacker and the Defender make their decisions.

As written, this description of ARA applies to normal form games, in which players make simultaneous decisions. But it also applies to extensive form games, such as Stackelberg games in which the Leader and Follower alternate their moves, or games in which agents act asynchronously. Here the risk analysis must condition on the choices that have already been made when calculating expected utilities. Such sequential analysis can become cumbersome; often the tree of unmade decisions that drives the risk calculation becomes elaborate, and simplifying assumptions are needed. A special case of this concerns the expression in (3), where $\mathcal{M}$ was used to denote a set of decisions that were made separately. Additionally, in realistic applications there are usually more than two actors, requiring an even more complex analysis.

As we have already mentioned, ARA aims at providing one-sided prescriptive support to the defender, based on a subjective expected utility model, treating the adversary's decisions as uncertainties. In order to predict the adversary's actions, we model his decision problem and try to assess his probabilities and utilities. Assuming that the adversary is an expected utility maximiser, we can predict the adversary's actions by finding his action of maximum expected utility. Our uncertainty about the adversary's probabilities and utilities is propagated over to the adversary's decision.

In the following section, we illustrate the use of ARA through the description of five relevant models related with security risk issues, which can be used as templates to deal with many real contexts, as the ones described in WP1, WP2 and WP3.

3. ARA Templates for Security

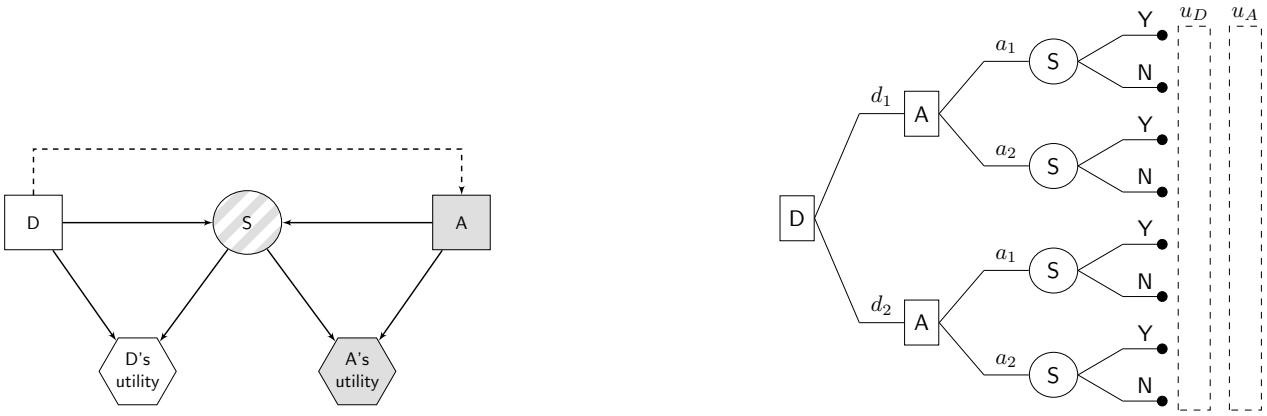
In this section, we present five template models that may be used to model cases in which two subjects (typically, an attacker and a defender) confront themselves. We use them to support one of them, the defender, to make appropriate decisions. We analyse in detail the first two and introduce the other three, which are dealt with in detail in the annexes. Illustrative examples of all models are gathered in ANNEX4. The initial model is introduced first as it does not include strategic elements, therefore facilitating a smoother introduction. The second is the simplest one requiring strategic considerations and allows the simplest illustration of the hierarchical approach in ARA and its relations with k-level thinking.

3.1 Sequential Defend-Attack Model

We start by considering the Sequential Defend-Attack model. The Defender first chooses a defence. Then, having observed it, the Attacker chooses an attack. To simplify our discussion, we shall assume that the Defender (she) has a discrete set of possible defences $\mathcal{D} = \{d_1, d_2, \ldots, d_m\}$ from which she must choose one. Similarly, the Attacker (he) has his set of possible attacks $\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$ to choose one from. As earlier stated, the set $\mathcal{D}$ could refer to possible defence policies, or possible policy levels, or defensive resource allocations or plans, among others, and, similarly, for $\mathcal{A}$.

We shall also simplify the problem by assuming that the only uncertainty deemed relevant is a binary outcome $S \in \{0, 1\}$ representing the failure or success of the attack. Finally, for both adversaries, the consequences depend on the success of this attack and their own action. A typical example would be a Government deciding how to allocate defensive resources around some transport infrastructures and, then, a terrorist organisation, having observed how such resources are deployed, performing an attack to one, or more, of such infrastructures.

Figure 5 depicts the problem graphically. On one hand it shows a coupled influence diagram (an influence diagram for each participant with a shared uncertain node and a linking arrow).



(a) Influence diagram

(b) Game tree ($m = n = 2$)

Figure 5: The Sequential Defend-Attack model

The influence diagram shows explicitly that the uncertainty associated with the success of an attack S is probabilistically dependent on the actions of both the Attacker and the Defender: $S|d,a$. Recall that arcs into a utility node represent functional dependence, see Shachter (1986). Thus, the utility functions over the consequences for the Defender and the Attacker are, respectively, $u_D(d,S)$ and $u_A(a,S)$. The arc in the influence diagram from the Defender's decision node to the Attacker's reflects that the Defender's choice is observed by the Attacker. We also show a game tree (with only two actions per adversary: $m = n = 2$) for the problem, reflecting the sequential nature. Note that there are two utility values, for the Attacker and the Defender, at the tree terminal nodes.

3.1.1 A Game Theoretic Analysis

We briefly describe first how standard game theory solves the Sequential Defend-Attack problem, which is an example of a Stackelberg game, see Aliprantis and Chakrabarti (2000). The game-theoretic approach requires the probability assessment over S, conditional on (d,a). As the Defender and the Attacker may have different assessments for the success S, these will be represented by $p_D(S = 1|d,a)$ and $p_A(S = 1|d,a)$, respectively. The solution does not require the Attacker to know the Defender's probabilities and utilities, since he observes the Defender's actions, but the Defender needs to know the Attacker's.

To solve the problem, we need the expected utilities of players at node (S) of the tree in Figure 5. The expected utility that the Attacker obtains when the decisions are $(d,a) \in \mathcal{D} \times \mathcal{A}$ is

$$\psi_A(d,a) = p_A(S = 0|d,a)\, u_A(a, S = 0) \; + \; p_A(S = 1|d,a)\, u_A(a, S = 1). \tag{5}$$

We compute $\psi_D(d,a)$ symmetrically for the Defender. Then, the Attacker's best attack against the defence d is

$$a^*(d) = \arg\max_{a \in \mathcal{A}} \psi_A(d,a), \forall d \in \mathcal{D}. \tag{6}$$

Under the assumption that the Defender knows how the Attacker will solve his problem, the Defender's best defence is

$$d^* = \arg\max_{d \in \mathcal{D}} \psi_D(d, a_*^{(2)}(d)).$$

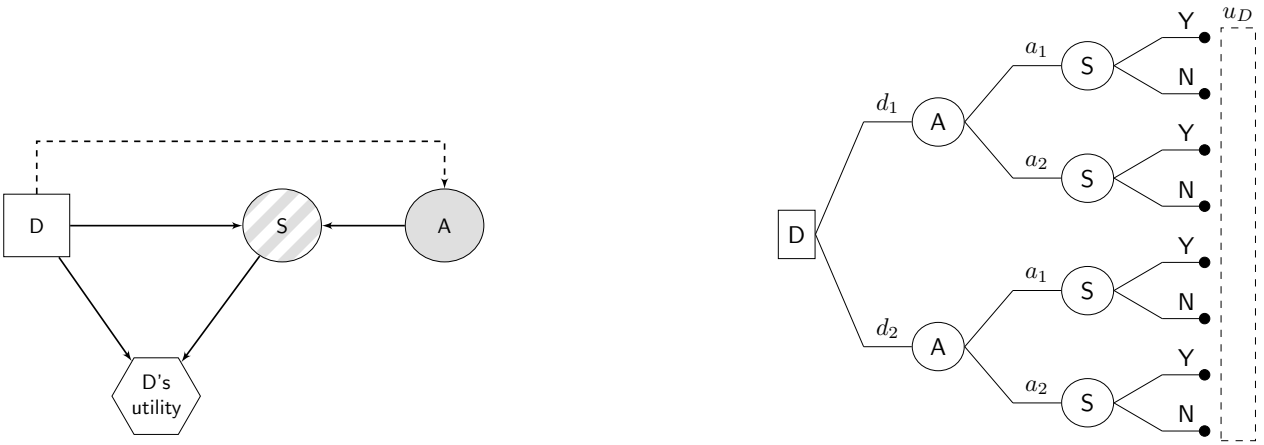
The solution $(d^*, a^*(d^*))$ is a Nash equilibrium.

Under the above assumptions that the Defender accurately knows the Attacker's true p_A and u_A, the Defender has an advantage: she is the first to move and, *ceteris paribus*, has larger expected utility than in the analogous simultaneous game. Bier (2007) discusses this in detail, pointing out that sometimes disclosing information about one's defences against terrorism can have deterrent effects. However, the assumption that the Defender knows the Attacker's preferences and probabilistic assessments is far from realistic most of the times in the kind of problems relevant to SECONOMICS.

3.1.2 The ARA Analysis

We now weaken the above common knowledge assumption: the Defender does not actually know (p_A, u_A). We thus consider the Defender's problem as a standard decision analysis

problem: the Defender's influence diagram in Figure 6, no longer has the hexagonal utility node with the Attacker's information and his decision node is perceived as random variable. Similarly, her decision tree denotes uncertainty about the Attacker's decision by replacing A with (A) and including a reference only to the Defender's utility function. However, as we shall see, she may have beliefs about (p_A, u_A), which will be relevant in our analysis.



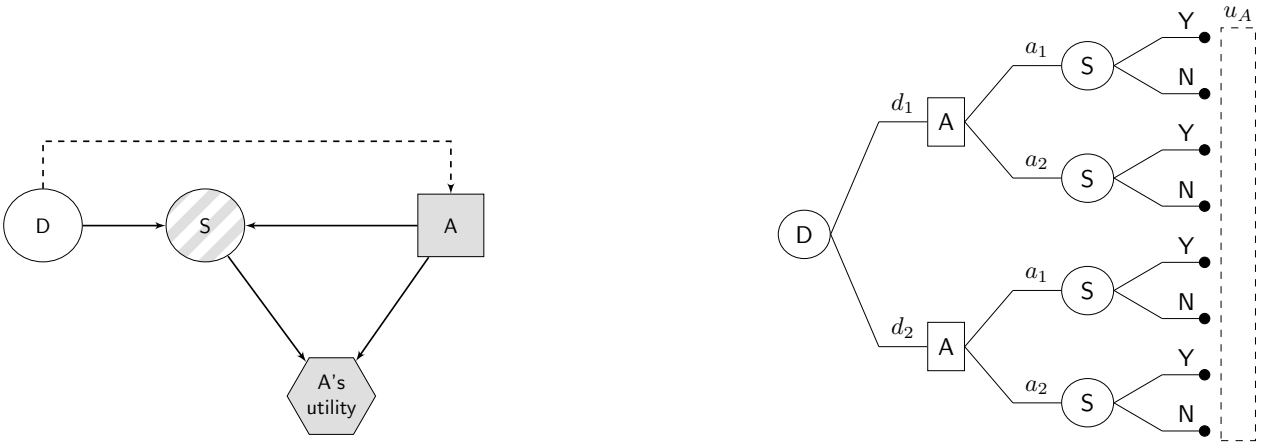
(a) Influence diagram

(b) Decision tree ($m = n = 2$)

Figure 6: The Defender's decision problem

By observing the influence diagram, note that in order to solve her decision problem, the Defender has already assessed $p_D(S|d, a)$ and $u_D(d, S)$, but she also needs $p_D(A|d)$, which is her assessment of the probability that the Attacker will choose attack a, after having observed that the Defender has chosen defence d. This assessment requires the Defender to analyse the problem from the Attacker's perspective, possibly as we describe.

First, the Defender must place herself in the Attacker's shoes, and consider his decision problem. Figure 7 represents the Attacker's problem, as seen by the Defender.



(a) Influence diagram

(b) Decision tree ($m = n = 2$)

Figure 7: The Defender's analysis of the Attacker's problem

We assume that the Defender analyses the Attacker's problem considering that he is an expected utility maximiser. Thus, she will use all the information and judgment available she can about the Attacker's utilities and probabilities. To find $p_D(A|d)$, she should first estimate the Attacker's utility function and his probabilities about success S, conditional on (d, a), and consequently compute the required probability. However, instead of using point estimates for p_A and u_A to find the Attacker's optimal decision $a^*(d)$ as in (6), the Defender's uncertainty about the Attacker's decision should derive from her uncertainty about the Attacker's (p_A, u_A), which we describe through a distribution $F = (P_A, U_A)$. This, in turn, will induce a distribution on the Attacker's expected utility $\psi_A(a, d)$ defined in (5). Thus, assuming the Attacker is an expected utility maximiser, the Defender's distribution about the Attacker's choice, given her defence choice d, is

$$p_D(A = a|d) = \mathbb{P}_F[a = \arg\max_{x \in \mathcal{A}} \Psi_A(d, x)], \quad \forall a \in \mathcal{A},$$

where

$$\Psi_A(d, a) = P_A(S = 0|d, a)\ U_A(a, S = 0)\ +\ P_A(S = 1|d, a)\ U_A(a, S = 1).$$

She can use Monte Carlo simulation to approximate the probabilities $p_D(A|d)$ by drawing N samples $\left\{\left(p_A^k, u_A^k\right)\right\}_{k=1}^N$ from F, which produce $\{\psi_A^k\}_{k=1}^N \sim \Psi_A$, and approximating $p_D(A = a|d)$ by

$$\hat{p}_D(A = a|d) = \frac{\#\{a = \arg\max_{x \in \mathcal{A}} \psi_A^k(d, x)\}}{N}, \quad \forall a \in \mathcal{A}. \tag{7}$$

Once the Defender has completed these assessments, she can solve her problem. Her expected utilities at node (S) in Figure 6 for each $(d, a) \in \mathcal{D} \times \mathcal{A}$ are

$$\psi_D(d, a) = p_D(S = 0|d, a)\ u_D(d, S = 0) + p_D(S = 1|d, a)\ u_D(d, S = 1).$$

Then, her estimated expected utilities at node (A) for each $d \in \mathcal{D}$ are

$$\hat{\psi}_D(d) = \sum_{j=1}^{n} \psi_D(d, a_j)\ \hat{p}_D(A = a_j|d).$$

Finally, her optimal decision is $d^* = \arg\max_{d \in \mathcal{D}} \hat{\psi}_D(d)$.

Note that in terms of classic game theory, the solution d^* for the sequential game need not correspond to a Nash equilibrium. Assume there would be a third party who knows the Defender's true (p_D, u_D) and her beliefs F about the Attacker's utilities and probabilities, as well as the Attacker's true (p_A, u_A) and his beliefs G about the Defender's. That party would then be able to predict the game, identifying the decisions chosen by each player. However, this omniscient prediction would not be the Nash equilibrium computed based on the true (p_D, u_D) and (p_A, u_A). Since the players lack full and common knowledge, their choices are unlikely to coincide with those made in the traditional game theory formulation.

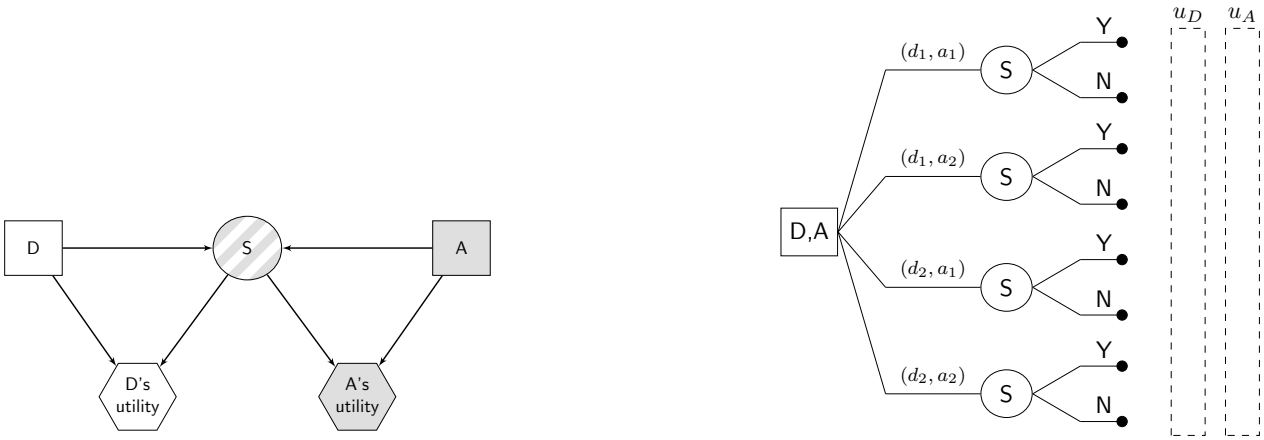
ANNEX4 includes an example of this type of model.

3.2 Simultaneous Defend-Attack Model

We discuss now the Simultaneous Defend-Attack model: a Defender (She, D) and an Attacker (He, A) decide their defence and attack, respectively, without knowing the action chosen by each other. See Zhuang and Bier (2007) for a related discussion. As an example,

imagine a case in which the authorities of a given airport decide whether to introduce undercover marshals in the airport installations, which might, or not, be attacked by terrorists.

We shall assume again that the adversaries have discrete alternative sets $\mathcal{D} = \{d_1, d_2, \ldots, d_m\}$ and $\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$ of defences and attacks, respectively. We shall also assume that the only relevant uncertainty is S, denoting the success ($S = 1$) or failure ($S = 0$) of an attack. Each decision maker assesses differently the probability of the result of an attack, which depend on the defence and attack adopted: $p_D(S = s|d, a)$ and $p_A(S = s|d, a)$. The utility function of the Defender $u_D(d, s)$ depends on her chosen defence and the result of the attack. Similarly, the Attacker's utility function is $u_A(a, s)$. This situation can be represented by two coupled influence diagrams (one for the Defender, one for the Attacker) with a shared uncertainty node associated with the attack success, as in Figure 8. We also show a game tree for this problem, with just two possible attacks and defences, to simplify the figure.



(a) Influence diagram

(b) Game tree ($m = n = 2$)

Figure 8: The Simultaneous Defend-Attack model

3.2.1 A Game Theoretic Analysis

Under the common knowledge assumption, preferences and beliefs from both the Defender and the Attacker, (u_D, p_D) and (u_A, p_A) respectively, are disclosed. Therefore, each adversary knows the expected utility that each pair $(d, a) \in \mathcal{D} \times \mathcal{A}$ would provide to both of them, computed through

$$\psi_D(d, a) = p_D(S = 0|d, a)\, u_D(d, S = 0) + p_D(S = 1|d, a)\, u_D(d, S = 1),$$

and, similarly,

$$\psi_A(d, a) = p_A(S = 0|d, a)\, u_A(a, S = 0) + p_A(S = 1|d, a)\, u_A(a, S = 1).$$

A Nash equilibrium (d^*, a^*) for this game would satisfy

$$\psi_D(d^*, a^*) \geq \psi_D(d, a^*)\ \ \forall d \in \mathcal{D} \quad \text{and} \quad \psi_A(d^*, a^*) \geq \psi_A(d^*, a)\ \ \forall a \in \mathcal{A}.$$

Finding Nash equilibria may require the use of randomised strategies Gibbons (1992). There could be several equilibria with no unambiguous criteria to further discern among them Raiffa et al. (2002).

If utilities and probabilities are not common knowledge among the adversaries, a game-theoretic approach proceeds by modelling the game as one with incomplete information Harsanyi (1967), introducing the notion of player types: each player will be of a certain type which is known to him but not to his opponent. Thus, a player's type represents the private information he may have. The Defender's type $\tau_D \in T_D$ determines her utility $u_D(d, s, \tau_D)$ and probability $p_D(S = s|d, a, \tau_D)$. Similarly, for the Attacker's types $\tau_A \in T_A$. Harsanyi (1967) proposes the Bayes-Nash equilibrium as a solution concept, under a still strong common knowledge assumption: the adversaries' beliefs about the opponent's types are common knowledge and modelled through a common prior distribution $\pi(\tau_D, \tau_A)$. Moreover, it is assumed that the players' beliefs about other uncertainties in the problem are also common knowledge. Then, the solution is computed as follows.

Define, first, the notion of strategy functions for the participants. These associate a decision with each type, $d : \tau_D \to d(\tau_D) \in \mathcal{D}$ and $a : \tau_A \to a(\tau_A) \in \mathcal{A}$. The Defender's expected utility associated with a pair of strategy functions, given any of her privately known types $\tau_D \in T_D$, is

$$\psi_D(d(\tau_D), a, \tau_D) = \int \left[\sum_{s \in S} u_D(d(\tau_D), s, \tau_D) p_D(S = s|d(\tau_D), a(\tau_A), \tau_D) \right] \pi(\tau_A|\tau_D) \, \mathrm{d}\tau_A.$$

Similarly, we can compute the Attacker's expected utility $\psi_A\big(d, a(\tau_A), \tau_A\big)$ for a pair of strategy functions (d, a), given any of his privately known types $\tau_A \in T_A$. Then, a Bayes-Nash equilibrium is a pair of strategy functions (d^*, a^*) for the Defender and the Attacker satisfying

$$\psi_D(d^*(\tau_D), a^*, \tau_D) \geq \psi_D(d(\tau_D), a^*, \tau_D), \ \forall \tau_D \quad \text{and} \quad \psi_A(d^*, a^*(\tau_A), \tau_A) \geq \psi_A(d^*, a(\tau_A), \tau_A), \ \forall \tau_A$$

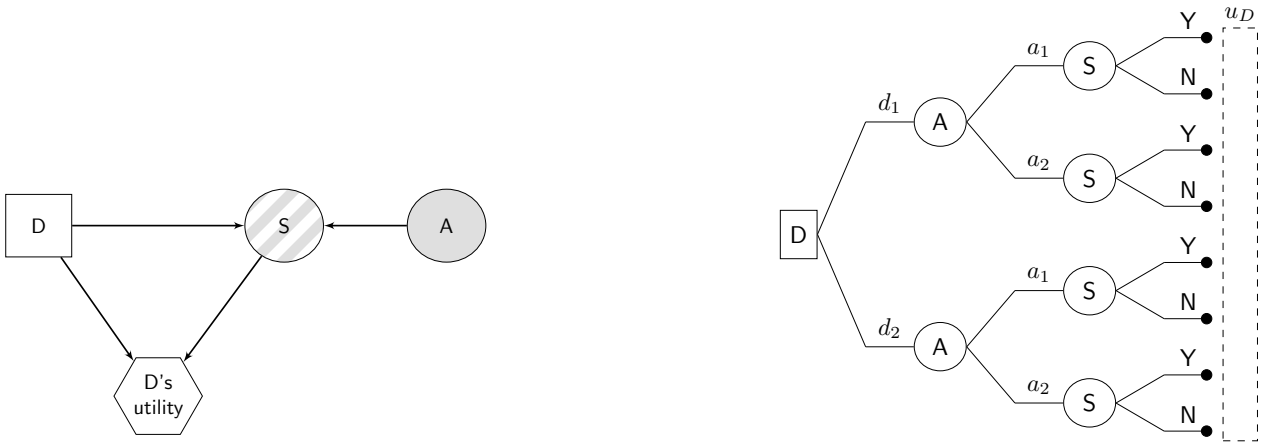
for every d and every a, respectively. Again, randomised strategies might be required to possibly find an equilibria.

We believe that the underlying common (prior) knowledge assumption is still counter-intuitive and unrealistic, specially in the context of security: it implies that players need to disclose, *inter alia*, their true beliefs about their opponent's type, as well as their private probabilistic assessments in order to be able to compute a Bayes-Nash equilibrium.

3.2.2 The ARA Approach

More realistically, we weaken the common (prior) knowledge assumption. We assume that we support the Defender in solving the Simultaneous Defend-Attack model. As reflected in Figure 9, the Defender has to choose a defence $d \in \mathcal{D}$, whose consequences depend on the success of an attack $a \in \mathcal{A}$ simultaneously chosen by the Attacker, which is, therefore, uncertain for the Defender at the time she makes her decision.

By standard decision theory, the Defender should maximise her expected utility, see French and Ríos Insua (2000). She knows her utility function $u_D(d, s)$ and her probability assessment p_D over S, conditional on (d, a). However, she does not know the Attacker's decision a at node A. She expresses her uncertainty through a probability distribution $\pi_D(A = a)$.



(a) Influence diagram

(b) Decision tree ($m = n = 2$)

Figure 9: The Defender's decision analysis

Then, the optimization problem she should solve is

$$d^* = \arg\max_{d\in\mathcal{D}} \sum_{a\in\mathcal{A}} \left[\sum_{s\in\{0,1\}} u_D(d,s)\, p_D(S=s|d,a) \right] \pi_D(A=a). \tag{8}$$

The Defender thus needs to assess $\pi_D(A)$. To do so, suppose she thinks that the Attacker is an expected utility maximiser who tries to solve the decision problem shown in Figure 10. The Attacker would look for the attack $a \in \mathcal{A}$ providing him maximum expected utility:

$$a^* = \arg\max_{a\in\mathcal{A}} \sum_{d\in\mathcal{D}} \left[\sum_{s\in\{0,1\}} u_A(a,s)\, p_A(S=s|d,a) \right] \pi_A(D=d). \tag{9}$$

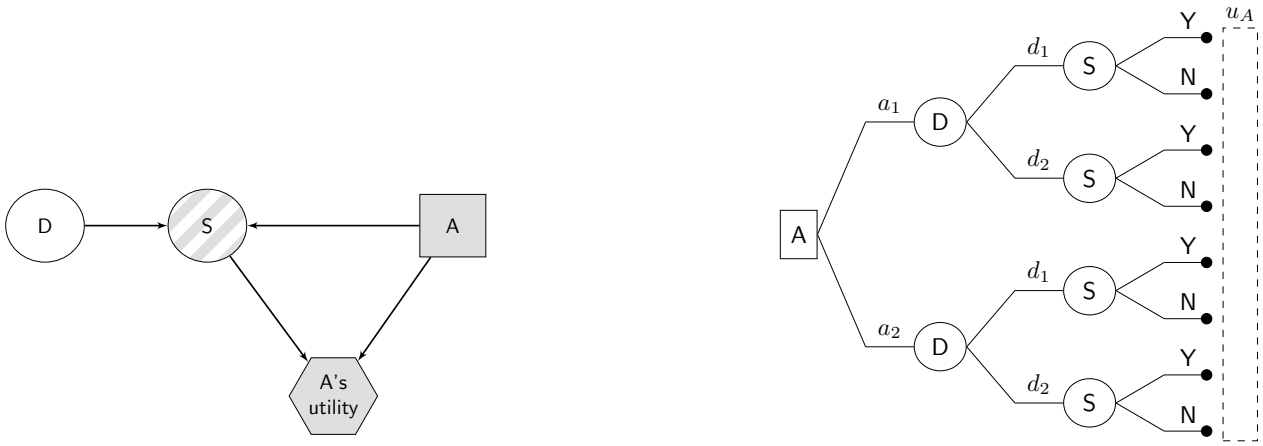
In general, the Defender will be uncertain about the Attacker's utility function and probabilities (u_A, p_A, π_A) required to solve such problem.

Suppose that we model all information available to the Defender about (u_A, p_A, π_A) through a probability distribution (U_A, P_A, Π_A). Then, and this will aid us in assessing $\pi_D(A)$, mimicking the argument in (9), we propagate such uncertainty to compute the probability distribution

$$A|D \sim \arg\max_{a\in\mathcal{A}} \sum_{d\in\mathcal{D}} \left[\sum_{s\in\{0,1\}} U_A(a,s)\, P_A(S=s|d,a) \right] \Pi_A(D=d). \tag{10}$$

Note that (U_A, P_A) could be directly elicited from the Defender. However, eliciting $\Pi_A(D)$ may require further analysis, leading to the next level of recursive thinking: the Defender would need to think about how the Attacker analyses her problem. This is why we condition in (10) by (the distribution of) D. Note that $\Pi_A(D)$ incorporates two sources of uncertainty:

- the Attacker's uncertainty about the Defender's choice, represented through his beliefs $\pi_A(D)$, and
- the Defender's uncertainty about the probabilistic model π_A used by the Attacker to predict what the Defender will choose, assessed from her perspective through $\pi_A \sim \Pi_A$.



(a) Influence diagram

(b) Decision tree ($m = n = 2$)

Figure 10: The Attacker's decision analysis, as seen by the Defender

In the above, the Defender presumes that the Attacker thinks she is an expected utility maximiser trying to solve a decision problem like the one described in Figure 9. Therefore, in order for the Defender to assess the distribution (10), she will elicit $(U_A, P_A) \sim F$ from her viewpoint, and assess $\Pi_A(D)$ through the analysis of her decision problem, as thought by the Attacker, mimicking the resolution of problem (8) from the Attacker's perspective. This reduces the assessment of $\Pi_A(D)$ to the computation of the distribution

$$D|A^1 \sim \arg\max_{d\in\mathcal{D}} \sum_{a\in\mathcal{A}} \left[\sum_{s\in\{0,1\}} U_D(d,s)\, P_D(S=s|d,a) \right] \Pi_D(A^1=a), \tag{11}$$

assuming the Defender is able to assess $\Pi_D(A^1)$, where A^1 represents the Attacker's decision within the Defender's second level of recursive thinking: the nested decision model used by the Defender to predict the Attacker's analysis of her decision problem. To assess the distribution (11), the Defender needs to elicit $(U_D, P_D) \sim G$, representing her probabilistic knowledge about how the Attacker may estimate her utility function $u_D(d,a)$ and her probability p_D over $S|d,a$, when she analyses how the Attacker thinks about her decision problem. Again, the elicitation of $\Pi_D(A^1)$ might require further recursive thinking from the Defender. This would lead to the recursive assessments:

Defender's elicitation of $\Pi_{\mathtt{D}}(\mathtt{A}^1)$

Repeat

- Find $\Pi_{\mathtt{D}^{k-1}}(\mathtt{A}^k)$ by solving
- $\mathtt{A}^k|\mathtt{D}^k \sim \arg\max_{\mathtt{a}\in\mathcal{A}} \sum_{\mathtt{d}\in\mathcal{D}} \left[\sum_{\mathtt{s}\in\{0,1\}} \mathtt{U}_{\mathtt{A}}^k(\mathtt{a},\mathtt{s})\ \ \mathtt{P}_{\mathtt{A}}^k(\mathtt{S}=\mathtt{s}|\mathtt{d},\mathtt{a})\right] \Pi_{\mathtt{A}^k}(\mathtt{D}^k=\mathtt{d})$
  - with $(\mathtt{U}_{\mathtt{A}}^k, \mathtt{P}_{\mathtt{A}}^k) \sim \mathtt{F}^k$
- Find $\Pi_{\mathtt{A}^k}(\mathtt{D}^k)$ by solving
- $\mathtt{D}^k|\mathtt{A}^{k+1} \sim \arg\max_{\mathtt{d}\in\mathcal{D}} \sum_{\mathtt{a}\in\mathcal{A}} \left[\sum_{\mathtt{s}\in\{0,1\}} \mathtt{U}_{\mathtt{D}}^k(\mathtt{d},\mathtt{s})\ \ \mathtt{P}_{\mathtt{D}}^k(\mathtt{S}=\mathtt{s}|\mathtt{d},\mathtt{a})\right] \Pi_{\mathtt{D}^k}(\mathtt{A}^{k+1}=\mathtt{a})$
  - with $(\mathtt{U}_{\mathtt{D}}^k, \mathtt{P}_{\mathtt{D}}^k) \sim \mathtt{G}^k$
- $\mathtt{k} = \mathtt{k} + 1$

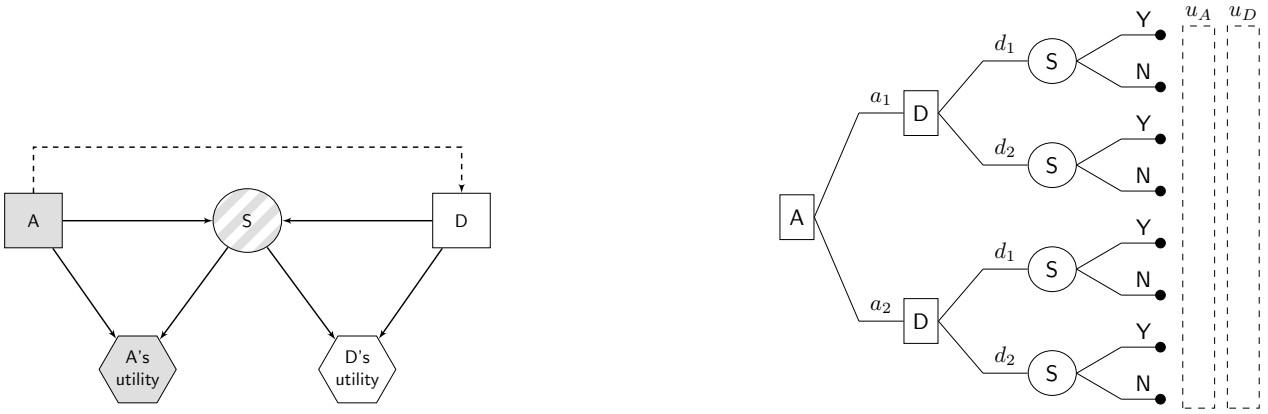
To simplify the discussion, we have assumed that the recursive decision models used to assess A^i and D^i are a reflection of each other and have the same structure as in Figures 10 and 9, respectively. Moreover, the choice sets for the Defender and the Attacker are the same in all the recursive models: $\mathcal{D}$ and $\mathcal{A}$, respectively.

This hierarchy of nested models would stop at a level in which the Defender lacks the information necessary to assess the distribution F^i or G^i associated with the decision analysis of A^i and D^i, respectively. At this point, the Defender would holistically assign an unconditional probability distribution over A^i or D^i, respectively, without going deeper in the hierarchy, summarising all remaining information she might have through the direct assessment of $\Pi_{D^{i-1}}(A^i)$ or $\Pi_{A^i}(D^i)$, as might correspond. Of course, should she feel that she has no information available to do so, she could assign a noninformative distribution, see French and Ríos Insua (2000). Note that this proposal is clearly connected with k-level thinking as in Stahl and Wilson (1995) or Rothschild et al. (2012), who provide a related approach in which a level k is first agreed on and, then, a uniform distribution is propagated.

We illustrate the ARA approach to this model with a simple numerical example in ANNEX4.

3.3 Sequential Attack-Defend

We consider now the Sequential Attack-Defend model. The Attacker first performs an attack. Then, having suffered it, the Defender chooses a defence. Again, we shall assume that the sets of possible attacks and defences $\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$ and $\mathcal{D} = \{d_1, d_2, \ldots, d_m\}$ are discrete. We shall also simplify the problem by assuming that the only uncertainty deemed relevant is a binary outcome $S \in \{0, 1\}$ representing the final failure or success of the attack. Finally, for both adversaries, the consequences depend on the success of this attack and their own action. As an example, consider that under a given defence resource allocation for protecting national critical installations, we consider possible attacks of a terrorist organisation and the corresponding recovery plans. Thus, we are devising a security contingency plan. Figure 11 depicts the problem graphically.



(a) Influence diagram

(b) Game tree ($m = n = 2$)

Figure 11: The Sequential Attack-Defend model

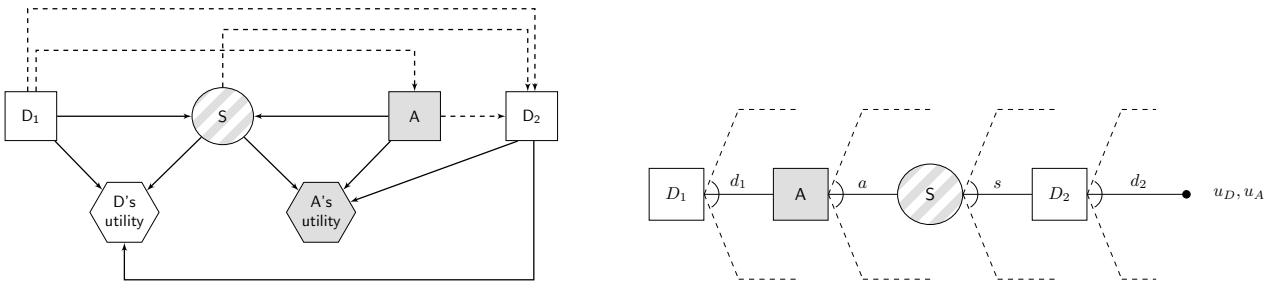
On one hand it shows a coupled influence diagram (an influence diagram for each participant with a shared uncertain node and a linking arrow). The influence diagram shows explicitly that the uncertainty associated with the success of an attack S is probabilistically dependent on the actions of both the Attacker and the Defender: $S|a,d$. Thus, the utility functions over the consequences for the Attacker and the Defender are, respectively, $u_A(a,S)$ and $u_D(d,S)$. The arc in the influence diagram from the Attacker's decision node to the Defender's reflects that the Attacker's choice is observed by the Defender. We also show a game tree (with only two actions per adversary: $m = n = 2$) for the problem, reflecting its sequential nature. Note that there are two utility values, for the Attacker and the Defender, at the tree terminal nodes.

In ANNEX1 we address the standard game theory analysis of this model, criticising the main limitations of such approach, and formulate an alternative Adversarial Risk Analysis, which we illustrate with an example in ANNEX4.

3.4 Sequential Defend-Attack-Defend

We proceed now with the Sequential Defend-Attack-Defend model, see Brown et al. (2006) or Parnell et al. (2010) for various examples.

In this model, the Defender first deploys defensive resources. Then, the Attacker, having observed such decision, performs an attack. Finally, the Defender tries to recover from the attack as best as she can. Figure 12 shows coupled influence diagrams, with a shared uncertainty node S, and a game tree representing this model. Nodes D_1 and D_2 correspond to the Defender's first and second decisions, respectively, and node A represents the Attacker's decision. The respective choices will be $d_1 \in \mathcal{D}_1$, $a \in \mathcal{A}$ and $d_2 \in \mathcal{D}_2$, which we shall assume continuous. Again, we shall assume that the only relevant uncertainty is the success level S of the attack, which depends probabilistically on $(d_1, a) \in \mathcal{D}_1 \times \mathcal{A}$. We shall assume that the consequences for the Defender and the Attacker will depend, respectively, on (d_1, s, d_2), the effort in implementing her protective and recovery actions and the mitigated result of the attack, and on (a, s, d_2), the effort in implementing his attack and the result of the attack, mitigated by the recovery action of the Defender.



(a) Influence diagram

(b) Game tree ($m = n = 2$)

Figure 12: The Defend-Attack-Defend model

As an example, consider a case in which a Government decides how to allocate security resources to an airport installations; then, the terrorists, having observed them, perform an attack. Finally, the Government tries to recover as best as possible from such attack.

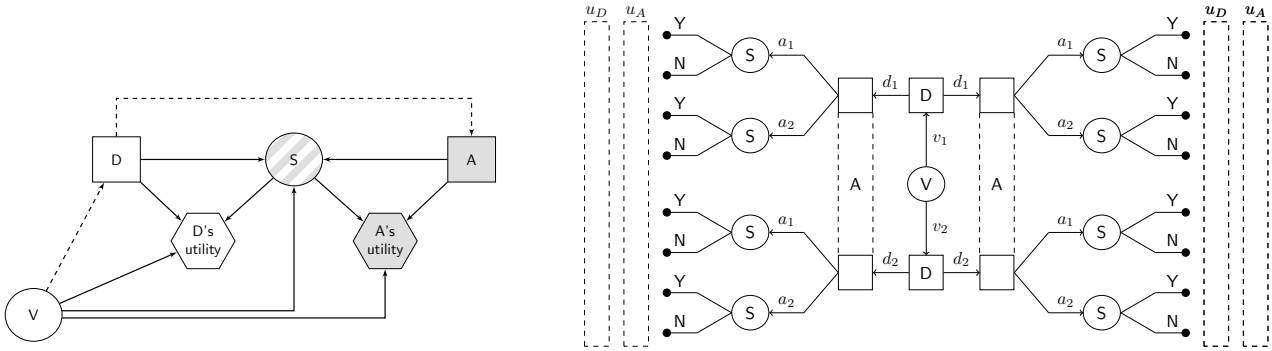
In ANNEX2, we provide a full description of the Defend-Attack-Defend model through

both a game theoretic analysis and the ARA approach. ANNEX4 contains a detailed example.

3.5 Sequential Defend-Attack with Private Information

Our final basic model will be the Sequential Defend-Attack model with Defender's private information, i.e. information that she does not want the Attacker to know. This is the case when e.g. the Defender wants to keep secrecy about vulnerabilities of sites she is trying to protect, as this information can be used by the Attacker to increase the chances of success and the expected impact of an attack. In this model, the Defender moves first by choosing a defence and, then, having observed it, the Attacker moves by choosing an attack. An example of this situation is given by an Attacker who gets to observe how the Defender allocates her resources among the critical installations she wants to protect before deciding his attack. Note that the Defender's decision allocating resources to protect different critical installations might signal to the Attacker about the sites' vulnerability and importance for the Defender, which is the type of information she wants to keep secret. This kind of applications, with the corresponding game theoretic analysis, has been considered e.g. by Powell (2007), Zhuang et al. (2010), and Zhuang and Bier (2010, 2011).

Assume that the Defender and the Attacker have, respectively, sets $\mathcal{D}$ and $\mathcal{A}$ of possible defences and attacks. We shall also assume that the success level S of an attack is uncertain. The private information (e.g., vulnerabilities) is represented by V, whose value is known by the Defender, but not by the Attacker. This affects the chances of success of an attack, as well as its impact. Finally, for both adversaries, the consequences depend, in addition, on the success of this attack and their own action.



(a) Influence diagram

(b) Game tree ($m = n = 2$)

Figure 13: The Sequential Defend-Attack model with Defender's private information

Figure 13 depicts the problem graphically. The coupled influence diagrams show explicitly that the uncertainty associated with the success of an attack S is probabilistically dependent on the actions of both the Attacker and the Defender, as well as on v. For example, if v represents a site's vulnerability, this probability will be higher as vulnerability gets higher, the rest of factors remaining fixed. The utility functions over the consequences for the Defender and the Attacker are, respectively, $u_D(d, s, v)$ and $u_A(a, s, v)$, reflecting that the consequences depend also on $V = v$. The arc in the influence diagram from the Defender's decision node

to the Attacker's reflects that the Defender's choice is observed by the Attacker. The arc from (V) to [D] reflects that v is known by the Defender at the time she makes her decision. The lack of arc from (V) to [A] indicates that v is not known by the Attacker at the time he makes his decision.

We also show the corresponding game tree. To simplify the figure, we only show two actions per adversary: $\mathcal{D} = \{d_1, d_2\}$ and $\mathcal{A} = \{a_1, a_2\}$; two possible outcomes (failure or success) of an attack: $S \in \{N, Y\}$; and two possible values for $V \in \{v_1, v_2\}$. The game tree reflects the sequential nature of the problem, as well as the asymmetric information. The fact that the Attacker does not know what is the value v at the time he must move is displayed using information sets (drawn as dashed lines), a standard element of games with imperfect information Harrington (2008).

In ANNEX3 we describe in more detail the basic features of this model. ANNEX4 includes a detailed numerical example.

4. Adapting the Templates

In this section, we illustrate how the basic templates may be adapted to take into account the complexities in real SECONOMICS case studies as reflected on those in WP1, WP2, WP3. The above models should be seen as such: templates reflecting basic dynamics between an attacker and a defender. Some of the simplifications include restrictions to discrete decisions, just one uncertainty node,.... Going through the case studies will allow us to revise and propose more complex models that cater for further realism. Here we shall illustrate how these basic models may be compounded to provide a security resource allocation model in a spacial setting.

Assume that we are supporting an agent (She, the Defender) in protecting some kind of critical or transport infrastructure from the attacks of another agent (He, the Attacker). We assume that both agents operate monolithically. The infrastructures have a value, as specified below. The Defender aims at preserving such value; the Attacker aims at obtaining as much value as possible.

The infrastructures can be divided into adjacent cells (i,j), representing e.g. metro stations, or transformers within a major national electric infrastructure. Each cell has a value v_{ij} which aggregates all assets (information, human resources, money,...) available at this cell. At the start, the Defender has resources R_D^1 to protect the installations under concern. This might include policemen, vehicles, cameras, arms, money and others. For our proposal, we shall assume that there is just one type of resource, which is discrete, but this might not always be the case. They allocate resources $d_{ij}^1 \geq 0$ to cell (i,j), fulfilling the constraint

$$\sum_{ij} d_{ij}^1 \leq R_D^1.$$

The Attacker has also attack resources R_A (human resources, arms, vehicles, money and others) that he will use to deploy different types of attacks. Again, we assume that there is just one type of resource, which is discrete. They allocate attack resources $a_{ij} \geq 0$ to cell (i,j), satisfying the constraint

$$\sum_{ij} a_{ij} \leq R_A.$$

Based on the initial resource allocation and the type of attacks, the Defender will have available R_D^2 resources after the attacks take place. They will deploy resources $d_{ij}^2 \geq 0$ to cell (i,j) to recover from the attacks satisfying the constraint

$$\sum_{ij} d_{ij}^2 \leq R_D^2.$$

Recovery resources will typically be related, but not necessarily coincide, with the initially deployed resources. For example, security staff who are too far away will not be able to be displaced for recovery in time.

We shall assume that the dynamics of the Defender and the Attacker can be described with a Sequential Defend-Attack-Defend model, represented in Figure 14 as a coupled influence diagram. At a first stage, the Defender makes its initial resource allocation $d^1 = \{d_{ij}^1\}$ for each cell (i,j) within the infrastructure. The Attacker observes these and launches his

attacks by allocating resources $a = \{a_{ij}\}$ to each cell (i, j). The success of these attacks is represented through $s_1 = \{s_1^{ij}\}$. Depending on the results of these attacks, the Defender makes his recovery decisions $d^2 = \{d_{ij}^2\}$, which lead to the final level of Attacker success $s_2 = \{s_2^{ij}\}$ for each cell within the installations. The utility obtained by the Defender depends on how the attack levels of success s_2 after the recovery stage affect the installations assets at each cell $v = \{v_{ij}\}$ as well as its defensive investments d^1 and d^2 at the first and second stages, respectively; the utility obtained by the Attacker depends on the attack levels of success s_2 at the last stage and its offensive resource investments a. The set of feasible actions for both the Defender and the Attacker are subject to the above resource constraints.

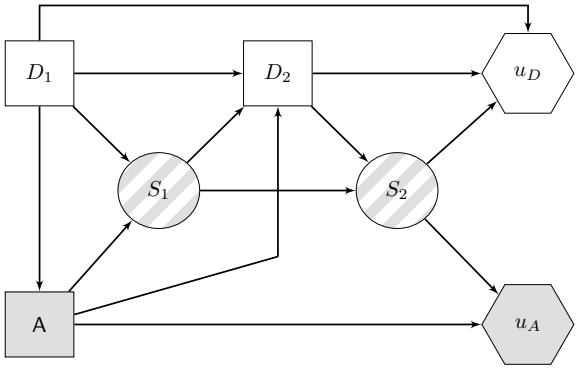


Figure 14: Coupled influence diagrams for the security resource allocation problem

Globally, we may view that each cell is assigned a Sequential Defend-Attack-Defend model, with all models coordinated by resource constraints and value aggregation for both agents.

We illustrate this model in detail in ANNEX5, showing how to solve it through ARA.

5. Conclusions

In this deliverable, we have provided the analysis of five template models aimed at devising strategies for the protection of critical infrastructures or, more generally, at supporting security policy making. The templates are based on the adversarial risk analysis framework, which aims at providing models for the decision making of Defender when facing the decisions of the Attacker, the two agents involved in the problem. The models differ from each other in the way and order in which the possible attacks and defences take place within the sequence of events: Simultaneous Defend-Attack; Sequential Defend-Attack; Sequential Attack-Defend; Sequential Defend-Attack-Defend and Sequential Defend-Attack with Private Information.

We have started describing how these templates may be adapted to realistic problems, providing in each case a security example. We have discussed for all the models the standard game theoretic solution as a starting point to discuss our methodology, based on adversarial risk analysis. We have also illustrated how the templates may be adapted in more realistic problems, specifically in a security resource allocation problem within a spacial setting. Finally, we have also discussed issues regarding opponent modelling.

We shall further explore and adapt the templates to the cases proposed in WP1–WP3. WP4 will provide ideas about what to model within the relevant utility functions. We aim also at combining the models here proposed with those in WP6. On the other hand, WP7 will determine which of these models may be relevant in general security problems, which would be then implemented in the SECONOMICS tool delivered by WP8.

BIBLIOGRAPHY

G.A. Akerlof. The market for “lemons”: Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics*, 84(3):488–500, 1970.

C.D. Aliprantis and S.K. Chakrabarti. *Games and Decision Making*. Oxford University Press, 2000.

R. Anderson and T. Moore. The economics of information security. *Science, New Series*, 314(5799):610–613, 2006.

R. Anderson, C. Barton, R. Böhme, R. Clayton, M. van Eeten, M. Levi, T. Moore, and S. Savage. Measuring the cost of cybercrime. In *11th Workshop on the Economics of Information Security*, 2012.

D.G. Arce and T. Sandler. Terrorist signalling and the value of intelligence. *British Journal of Political Science*, 37(4):573–586, 2007.

W. Baker, M. Howard, A. Hutton, and C.D. Hylender. *2012 Data Breach Investigation Report*. Technical report, 2012.

J. Baltazar. *More traffic, more money: Koobface draws more blood*. Technical report, TrendLabs, 2011.

D. Banks and S. Anderson. Game theory and risk analysis in the context of the smallpox threat. In G. Wilson A. Wilson and D. Olwell, editors, *Statistical Methods in Counterterrorism*, pages 9–22. Springer, 2006.

D. Banks, F. Petralia, and S. Wang. Adversarial risk analysis: Borel games. *Applied Stochastic Models in Business and Industry*, 27(2):72–86, 2011.

T. Bedford and R.M. Cooke. *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge University Press, 2001.

C. Bielza, P. Müller, and D. Ríos Insua. Decision analysis by augmented probability simulation. *Management Science*, 45(7):995–1007, 1999.

V.M. Bier. Choosing what to protect. *Risk Analysis*, 27(3):607–620, 2007.

V.M. Bier and M.N. Azaiez. *Game Theoretic Risk Analysis of Security Threats*. Springer, 2009.

V.M. Bier and L.A. Cox Jr. Probabilistic risk analysis for engineered systems. In W. Edwards, R.F. Miles Jr., and D. von Winterfeldt, editors, *Advances in Decision Analysis: from Foundations to Applications*, pages 279–301. Cambridge University Press, 2007.

R. Broadhurst. Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, 29:408–433, 2006.

G. Brown, M. Carlyle, J. Salmeron, and K. Wood. Analyzing the vulnerability of critical infrastructure to attack and planning defenses. *INFORMS Tutorials in Operations Research*, pages 102–123, 2005.

G. Brown, M. Carlyle, J. Salmerón, and K. Wood. Defending critical infrastructure. *Interfaces*, 36(6):530–544, 2006.

G. Brown, W.M. Carlyle, and R. Wood. *Optimizing Department of Homeland Security Defense Investments: Applying Defender-Attacker(-Defender) Optimization to Terror Risk Assessment and Mitigation*. National Academies Press, Appendix E, 2008.

G.G. Brown and L.A.T. Cox Jr. How probabilistic risk assessment can mislead terrorism risk analysts. *Risk Analysis*, 31(2):196–204, 2011.

C. Camerer. *Behavioral Game Theory: Experiments in Strategic Interaction*. Princeton University Press, 2003.

S. Carney, S. Eggertsson, and M. Doret. Cutthroat capitalism: An economic analysis of the somali pirate business model. *Wired Magazine*, 17(07), 2009.

B.R. Cobb and A. Basuchoudhary. A decision analysis approach to solving the signaling game. *Decision Analysis*, 6(4):239–255, 2009.

D.B. Cornish and R.V. Clarke. Understanding crime displacement: An application of rational choice theory. *Criminology*, 25(4):933–948, 1987.

L.A. Cox Jr. Improving risk-based decision making for terrorism applications. *Risk Analysis*, 29(3):336–341, 2009a.

L.A.T. Cox Jr. Game theory and risk analysis. *Risk Analysis*, 29(8):1062–1068, 2009b.

P.F. Deisler Jr. A perspective: Risk analysis as a tool for reducing the risks of terrorism. *Risk Analysis*, 22(3):405–413, 2002.

R.L. Dillon, R.M. Liebe, and T. Bestafka. Risk-based decision making for terrorism applications. *Risk Analysis*, 29(3):321–335, 2009.

A.K. Dixit, S. Skeath, and D.H. Reiley. *Games of Strategy*. WW Norton New York, 1999.

W. Enders and T. Sandler. *The Political Economy of Terrorism, 2nd edition*. Cambridge University Press, 2011.

R. English. *Terrorism: How to Respond*. Oxford University Press, 2010.

B.C. Ezell, S.P. Bennett, D. von Winterfeldt, J. Sokolowski, and A.J. Collins. Probabilistic risk analysis and terrorism risk. *Risk Analysis*, 30(4):575–589, 2010.

J. Franklin, V. Paxson, A. Perrig, and S. Savage. An inquiry into the nature and causes of the wealth of Internet miscreants. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pages 375–388, 2007.

S. French and D. Ríos Insua. *Statistical Decision Theory*. 2000.

B.J. Garrick. Perspectives on the use of risk assessment to address terrorism. *Risk Analysis*, 22(3):421–423, 2002.

R. Gibbons. *A Primer in Game Theory*. Pearson Education Ltd., 1992.

C. Grier, L. Ballard, J. Caballero, N. Chachra, C.J. Dietrich, K. Levchenko, P. Mavrommatis, D. McCoy, A. Nappa, A. Pitsillidis, N. Provos, M.Z. Rafique, M.A. Rajab, C Rossow, K. Thomas, V. Paxson, S. Savage, and G.M. Voelker. Manufacturing compromise: the emergence of exploit-as-a-service. In *Proceedings of the 2012 ACM Conference on Computer Communications Security*, pages 821–832. ACM, 2012.

Group IB. *State and Trends of the Russian digital crime market*. Technical report, Group IB, 2011.

A. Gutfraind. Terrorism as a mathematical problem. *SIAM News*, 42(8), 2009.

Y.Y. Haimes. *Risk Modeling, Assessment, and Management*. Wiley, 2004.

J.E. Harrington. *Games, Strategies, and Decision Making*. Worth Publishers, 2008.

J.C. Harsanyi. Games with Incomplete Information Played by “Bayesian” Players, I-III. Part I. The Basic Model. *Management Science*, 14(3):159–182, 1967.

J.C. Harsanyi. Subjective Probability and the Theory of Games: Comments on Kadane and Larkey’s Paper. *Management Science*, 28(2):120–124, 1982.

K. Hausken. Probabilistic risk analysis and game theory. *Risk Analysis*, 22(1):17–27, 2002.

T. Hennig-Thurau and G. Walsh. Electronic Word-of-Mouth: Motives for and Consequences of Reading Customer Articulations on the Internet. *International Journal of Electronic Commerce*, 8:51–74, 2003.

C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Workshop on New Security Paradigms Workshop (NSPW)*, pages 133–144, 2009.

C. Herley. Why do Nigerian Scammers Say They are from Nigeria? In *Proceedings of the Workshop on the Economics of Information Security*, 2012.

C. Herley and D. Florêncio. Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. In Tyler Moore, David Pym, and Christos Ioannidis, editors, *Economics of Information Security and Privacy*, pages 33–53. Springer US, 2010.

A. Heyes. Implementing environmental regulation: Enforcement and compliance. *Journal of Regulatory Economics*, 17(2):107–129, 2000.

J.B. Kadane. Adversarial risk analysis: what’s new, what isn’t?: discussion of adversarial risk analysis: Borel games. *Applied Stochastic Models in Business and Industry*, 27(2): 87–88, 2011.

J.B. Kadane and P.D. Larkey. Subjective probability and the theory of games. *Management Science*, 28(2):113–120, 1982.

C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G.M. Voelker, V. Paxson, and S. Savage. Spamalytics: An empirical analysis of spam marketing conversion. In *Proceedings of the 15th ACM Conference on Computer and Communications Security*, pages 3–14, 2008.

C. Kanich, N. Chachra, D. McCoy, C. Grier, D.Y. Wang, M. Motoyama, K. Levchenko, S. Savage, and G.M. Voelker. No plan survives contact: experience with cybercrime measurement. In *Proceedings of the 4th Conference on Cyber Security Experimentation and Test*, 2011.

S. Kaplan and B.J. Garrick. On the quantitative definition of risk. *Risk Analysis*, 1(1):11–27, 1981.

E. Kardes and R. Hall. Robust stochastic games and applications to counter-terrorism strategies. Technical report, 2005.

K.S. Killourhy, R.A. Maxion, and K.M.C. Tan. A defense-centric taxonomy based on attack manifestations. In *Proceedings of the International Conference on Dependable Systems & Networks*, pages 102–111. IEEE Computer Society Press, 2004.

C. P. Krebs, M. Costelloe, and D. Jenks. Drug control policy and smuggling innovation: a game-theoretic analysis. *Journal of Drug Issues*, 33(1):133–160, 2003.

J.S.H. Kwok and S. Gao. Knowledge sharing community in p2p network: a study of motivational perspective. *Journal of Knowledge Management*, 8:94–102, 2004.

J.D. Lipton. What blogging might teach about cybernorms. *Akron Intellectual Property Journal*, 4:239, 2010.

S.H. Liu, H.L. Liao, and Y.T. Zeng. Why people blog: an expectancy theory analysis. *Issues in Information Systems*, 8(2):232–237, 2007.

B. Lomborg. *Solutions for the World's Biggest Problems: Costs and Benefits*. Cambridge University Press, 2007.

J.E. Martínez Pérez and I. Méndez Martínez. ¿ Qué podemos saber sobre el valor estadístico de la vida en España utilizando datos laborales? *Hacienda Pública Española*, 3(191): 73–93, 2009.

R.P. McAfee and J. McMillan. Auctions and bidding. *Journal of Economic Literature*, 25(2): 699–738, 1987.

J. Merrick and G.S. Parnell. A Comparative Analysis of PRA and Intelligent Adversary Methods for Counterterrorism Risk Management. *Risk Analysis*, 31(9):1488–1510, 2011.

J.R.W. Merrick and L.A. McLay. Is screening cargo containers for smuggled nuclear threats worthwhile? *Decision Analysis*, 7(2):155–171, 2010.

B.B. Mesquita and L.E. Cohen. Self-interest, equity, and crime controls: A game-theoretic analysis of criminal decision making. *Criminology*, 33(4):483–518, 1995.

C. Miller. The legitimate vulnerability market: Inside the secretive world of 0-day exploit sales. In *Workshop on the Economics of Information Security (WEIS)*, pages 7–8, 2007.

M. Motoyama, D. McCoy, S. Savage, and G.M. Voelker. An analysis of underground forums. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement*, pages 71–80, 2011.

R.B. Myerson. *Game Theory: Analysis of Conflict*. Harvard University Press, 1997.

G. Parnell, D. Banks, L. Borio, G. Brown, L.A. Cox, J. Gannon, E. Harvill, H. Kunreuther, S. Morse, M. Pappaioanou, Pollack S., Singpurwalla N., and Wilson A. *Report on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis*. National Academies Press, 2008.

G.S. Parnell, C.M. Smith, and F.I. Moxley. Intelligent adversary risk analysis: A bioterrorism risk management model. *Risk Analysis*, 30(1):32–48, 2010.

E. Paté-Cornell and S. Guikema. Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures. *Military Operations Research*, 7(4):5–23, 2002.

J. Pearl. Influence diagrams—historical and personal perspectives. *Decision Analysis*, 2(4): 232–234, 2005.

E.J. Pinker. An analysis of short-term responses to threats of terrorism. *Management Science*, 53(6):865–880, 2007.

R. Powell. Allocating defensive resources with private information about vulnerability. *American Political Science Review*, 101(4):799–809, 2007.

N. Provos, P. Mavrommatis, M.A. Rajab, and F. Monrose. All your iframes point to us. In *Proceedings of the 17th USENIX Security Symposium*, pages 1–15, 2008.

H. Raiffa. *The Art and Science of Negotiation*. Harvard University Press, 1982.

H. Raiffa, J. Richardson, and D. Metcalfe. *Negotiation Analysis: the Science and Art of Collaborative Decision Making*. Harvard University Press, 2002.

I. Rezek, D.S. Leslie, S. Reece, S.J. Roberts, A. Rogers, R.K. Dash, and N.R. Jennings. On similarities between inference in game theory and machine learning. *Journal of Artificial Intelligence Research*, 33(1):259–283, 2008.

A. Riera Font, A. Ripoll Penalva, and J. Mateu Sbert. Estimación del valor estadístico de la vida en España: Una aplicación del método de salarios hedónicos. *Hacienda Pública Española*, 2(181):29–48, 2007.

J. Ríos and D. Ríos Insua. Supporting negotiations over influence diagrams. *Decision Analysis*, 6(3):153–171, 2009.

J. Ríos and D. Ríos Insua. Adversarial risk analysis for counterterrorism modeling. *Risk Analysis*, 32(5):894–915, 2012.

D. Ríos Insua and F. Ruggeri. *Robust Bayesian Analysis*. Springer, 2000.

D. Ríos Insua, J. Ríos, and D. Banks. Adversarial risk analysis. *Journal of the American Statistical Association*, 104(486):841–854, 2009.

M.H. Rothkopf. Decision analysis: The right tool for auctions. *Decision Analysis*, 4(3):167–172, 2007.

C. Rothschild, L. McLay, and S. Guikema. Adversarial risk analysis with incomplete information: A level-k approach. *Risk Analysis*, 32(7):1219–1231, 2012.

J.C. Sevillano, D. Ríos Insua, and J. Ríos. Adversarial Risk Analysis: The Somali Pirates Case. *Decision Analysis*, 9(2):86–95, 2012.

R.D. Shachter. Evaluating influence diagrams. *Operations Research*, 34(6):871–882, 1986.

K. Siqueira and T. Sandler. Terrorists versus the government strategic interaction, support, and sponsorship. *Journal of Conflict Resolution*, 50(6):878–898, 2006.

D.O. Stahl and P.W. Wilson. On players' models of other players: Theory and experimental evidence. *Games and Economic Behavior*, 10(1):218–254, 1995.

Symantec. *Analysis of Malicious Web Activity by Attack Toolkits*. Symantec, Available on the web at http://www.symantec.com/threatreport/topic.jsp?id=threat_activity_trends&aid=analysis_of_malicious_web_activity, online edition, 2011. Accessed on June 2012.

P.A. Taylor. *Hackers: crime in the digital sublime*. Psychology Press, 1999.

O. Turgeman-Goldschmidt. Hackers' accounts hacking as a social entertainment. *Social Science Computer Review*, 23(1):8–23, 2005.

M. van Eeten and J. Bauer. *Economics of Malware: Security Decisions, Incentives and Externalities*. Technical report, OECD, 2008.

M. van Eeten, J. Bauer, H. Asghari, S. Tabatabaie, and D. Rand. *The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data*. Technical report, OECD STI Working Paper, 2010.

D. von Winterfeldt and T.M. O'Sullivan. Should we protect commercial airplanes against surface-to-air missile attacks by terrorists. *Decision Analysis*, 3(2):63–75, 2006.

X. Wang, H.H. Teo, and K.K. Wei. What Mobilizes Information Contribution to Electronic Word-of-Mouth System? Explanations from a Dual-Process Goal Pursuit Model. In *Workshop Association for Informational Systems, Oklahoma*, 2009.

L.M. Wein. OR Forum — Homeland Security: From Mathematical Models to Policy Implementation. *Operations Research*, 57(4):801–811, 2009.

J. Zhuang and V.M. Bier. Balancing terrorism and natural disasters — defensive strategy with endogenous attacker effort. *Operations Research*, 55(5):976–991, 2007.

J. Zhuang and V.M. Bier. Reasons for secrecy and deception in homeland-security resource allocation. *Risk Analysis*, 30(12):1737–1743, 2010.

J. Zhuang and V.M. Bier. Secrecy and deception at equilibrium, with applications to anti-terrorism resource allocation. *Defence and Peace Economics*, 22(1):43–61, 2011.

J. Zhuang, V.M. Bier, and O. Alagoz. Modeling secrecy and deception in a multiple-period attacker-defender signaling game. *European Journal of Operational Research*, 203(2): 409–418, 2010.

ANNEX1. Sequential Attack-Defend Model

We describe now in more detail the Sequential Attack-Defend Model, introduced in Section 3.3, starting with the standard game theory analysis. We then provide the adversarial risk analysis of such model, pointing out the advantages of such approach with respect to the game theoretical one.

A Game Theoretic Analysis

We briefly describe first how standard game theory solves the Sequential Attack-Defend decision problem. The game-theoretic approach requires the probability assessment over S, conditional on (a, d). As the Attacker and the Defender may have different assessments for the success S, these will be represented by $p_A(S = 1|a, d)$ and $p_D(S = 1|a, d)$, respectively. The solution does not require the Defender to know the Attacker's probabilities and utilities, since she observes the Attacker's actions, but the Attacker needs to know the Defender's.

To solve the problem, we need the expected utilities of players at node (S) of the tree in Figure 11. The expected utility that the Defender obtains when the decisions are $(a, d) \in \mathcal{A} \times \mathcal{D}$ is

$$\psi_D(a, d) = p_D(S = 0|a, d)\, u_D(d, S = 0) \; + \; p_D(S = 1|a, d)\, u_D(d, S = 1).$$

We compute $\psi_A(a, d)$ symmetrically for the Attacker. Then, the Defender's best defence against the attack a is

$$d^*(a) = \arg\max_{d \in \mathcal{D}} \psi_D(a, d), \forall a \in \mathcal{A}. \tag{12}$$

Under the assumption that the Attacker knows how the Defender will solve her problem, the Attacker's best attack is

$$a^* = \arg\max_{a \in \mathcal{A}} \psi_A(a, d^*(a)).$$

The solution $(a^*, d^*(a^*))$ is a Nash equilibrium.

Since it is unrealistic that the Attacker knows the defender beliefs and preferences, we perform an ARA analysis.

The ARA Analysis

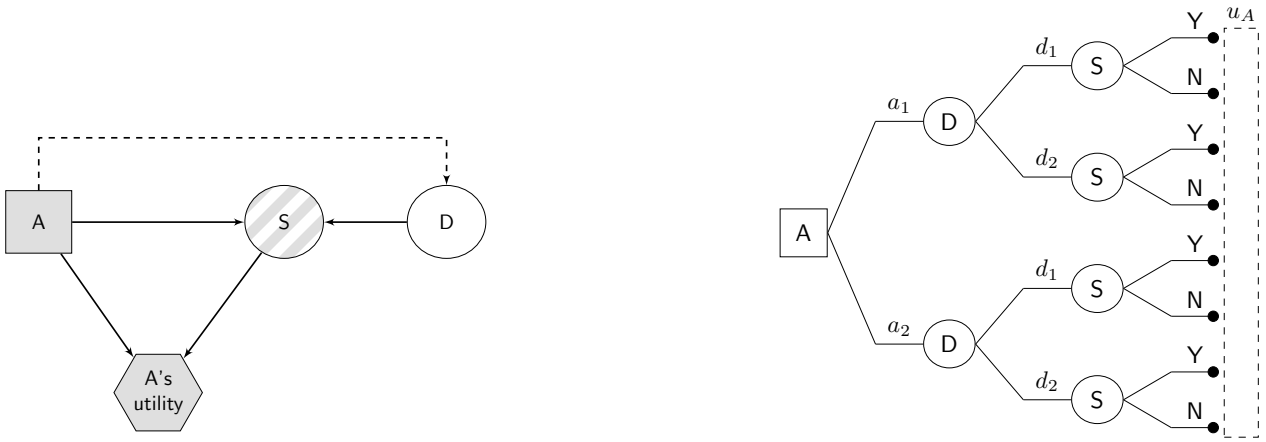
In principle, in the ARA approach the Defender sees the Attacker's attack a and then she can only reply with her best defence by computing $d^*(a)$ as in (12). The vector $(a_j, d^*(a_j))_{j=1}^n$ may be viewed as a contingency plan.

The ARA approach may help us in evaluating preparedness by thinking about the problem faced by the Attacker, whose aspect is described in the tree in Figure 15, in which the Defender decision is presented as an uncertainty. To solve his problem, the Attacker would need $\{p_A(d|a), p_A(s|a, d), u_A(a, s)\}$. Then, he would compute the expected utility of each attack through

$$\psi_A(a) = \sum_{d \in \mathcal{D}} p_A(d|a) \left[\sum_{s \in \mathcal{S}} p_A(s|a, d) u_A(a, s) \right],$$

where $\mathcal{S} = \{0, 1\}$, and find the optimal attack a^* maximising $\psi_A(a)$. Since we do not know u_A and the p_A's, we assume uncertainty about them through

$$F = \big(P_A(d|a), P_A(s|a,d), U_A(a,s)\big).$$



(a) Influence diagram

(b) Game tree ($m = n = 2$)

Figure 15: The Attacker decision problem

We, then, compute the random expected utility through

$$\Psi_A(a) = \sum_{d \in \mathcal{D}} P_A(d|a) \left[\sum_{s \in \mathcal{S}} P_A(s|a,d) U_A(a,s) \right],$$

building the distribution $P_D(A = a)$, defining the beliefs of the Defender about the eventual attacks. $P_D(A = a)$ will be approximated through

$$\hat{P}_D(A = a) = \frac{\#\{a = \arg\max_{x \in \mathcal{A}} \psi_A^k(x)\}}{N}, \ \forall a \in \mathcal{A},$$

where $\{\psi_A^k(a)\}_{k=1}^N$ is a suitable sample from $\Psi_A(a)$.

As in other cases, we proceed by simulation through

Simulation for the Sequential Attack-Defend problem

For $k = 1$ to N
  For $j = 1$ to n
    Generate $\{p_A^k(d|a_j), p_A^k(s|a_j, d), u_A^k(a_j, s)\} \sim F$
    Compute $\psi_A^k(a_j) = \sum_{d \in \mathcal{D}} p_A^k(d|a_j) \left[\sum_{s \in \mathcal{S}} p_A^k(s|a_j, d) u_A^k(a_j, s) \right]$
  Compute $a^* = \arg\max_{x \in \mathcal{A}} \psi_A^k(x)$
  $\hat{p}_D(a^*) = \hat{p}_D(a^*) + 1$
$\hat{p}_D(a_j) = \hat{p}_D(a_j)/N, \ \forall j$

$\hat{p}_D(a)$ may serve to evaluate preparedness, by telling us the most likely attack of the Attacker.

Note that, of all the three elements in F, $P_A(s|a,d)$ and $U_A(a,s)$ may be reasonably guessed through intelligence. However, $P_A(d|a)$ requires considering strategic elements and may lead to recursions of the type considered in Section 3.2.

An example is included in ANNEX4.

ANNEX2. Sequential Defend-Attack-Defend Model

We describe now how we may solve the Sequential Defend-Attack-Defend introduced in Section 3.4.

A Game Theoretic Analysis

A game-theoretic approach requires the Defender to know the Attacker's utilities and probabilities, the Attacker to know the Defender's, and, furthermore, that all this is common knowledge. Let these utility functions be $u_D(d_1, s, d_2)$ and $u_A(a, s, d_2)$, respectively, and their probability assessments about the success of attack be $p_D(S = s|d_1, a)$ and $p_A(S = s|d_1, a)$. Then, we may compute a solution using backward induction as follows.

At node D_2 of the game tree in Figure 12, the Defender's best response after each observed $(d_1, s) \in \mathcal{D}_1 \times S$ is

$$d_2^*(d_1, s) = \arg\max_{d_2 \in \mathcal{D}_2} u_D(d_1, s, d_2). \tag{13}$$

Under the common knowledge assumption, the Defender's behaviour at D_2 can be anticipated by the Attacker. Thus, at node S, the Defender's expected utility associated with each $(d_1, a) \in \mathcal{D}_1 \times A$,

$$\psi_D(d_1, a) = \int u_D(d_1, s, d_2^*(d_1, s))\, p_D(S = s|d_1, a)\, \mathrm{d}s, \tag{14}$$

and the Attacker's,

$$\psi_A(d_1, a) = \int u_A(a, s, d_2^*(d_1, s))\, p_A(S = s|d_1, a)\, \mathrm{d}s,$$

are known to both of them. Then, the Attacker can find his optimal attack decision at node A, after observing the Defender's first move $d_1 \in \mathcal{D}_1$, by solving

$$a^*(d_1) = \arg\max_{a \in \mathcal{A}} \psi_A(d_1, a).$$

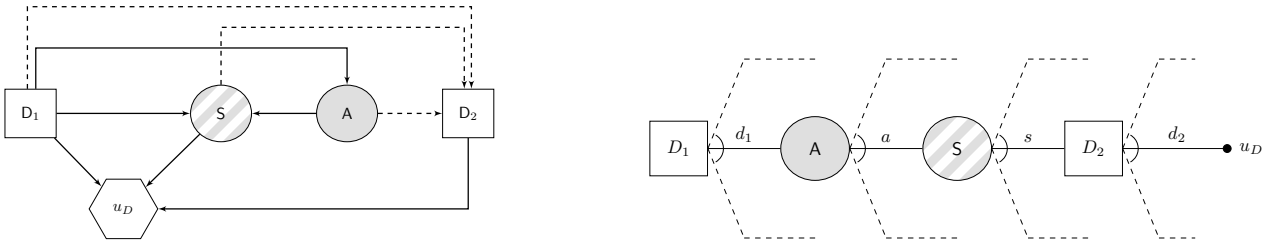
Knowing this, the Defender can find her maximum expected utility decision at node D_1 through

$$d_1^* = \arg\max_{d_1 \in \mathcal{D}_1} \psi_D(d_1, a^*(d_1)).$$

Therefore, under common knowledge, game theory predicts that the Defender will choose $d_1^* \in \mathcal{D}_1$ at node D_1; then, the Attacker will respond by choosing attack $a^*(d_1^*) \in \mathcal{A}$ at node A; and, finally, the Defender, after observing $s \in S$, will choose $d_2^*(d_1^*, s) \in \mathcal{D}_2$ at node D_2.

The ARA Approach

We now give up the strong common knowledge assumption and provide an ARA analysis to support the Defender. For this, we treat the Attacker's decision at node A as uncertain from the Defender's viewpoint and model such uncertainty. This is reflected in the influence



(a) Influence diagram

(b) Decision tree ($m = n = 2$)

Figure 16: The Defender's decision problem

diagram and the decision tree in Figure 16, where the Attacker's decision node has been converted into a chance node, by replacing A with (A). The Defender needs to assess $p_D(A|d_1)$, her predictive distribution about what attack the Attacker will choose at node A against each $d_1 \in \mathcal{D}_1$, besides the (more standard) assessments $u_D(d_1, s, d_2)$ and $p_D(S|d_1, a)$.

Given these, the Defender can solve her decision problem working backwards the tree in Figure 16. At node D_2, she can compute her maximum utility action $d_2^*(d_1, s)$ for each $(d_1, s) \in \mathcal{D}_1 \times S$, as in (13). Afterwards, she will obtain at node S her expected utility $\psi_D(d_1, a)$ for each $(d_1, a) \in \mathcal{D}_1 \times A$, as in (14). At this point, she will use her probabilistic assessment about what the Attacker will do, $p_D(A|d_1)$, to compute her expected utility at node A for each $d_1 \in \mathcal{D}_1$,

$$\psi_D(d_1) = \int \psi_D(d_1, a)\, p_D(A = a|d_1)\, \mathrm{d}a.$$

Finally, she can find her maximum expected utility decision at node D_1

$$d_1^* = \arg\max_{d_1 \in \mathcal{D}_1} \psi_D(d_1).$$

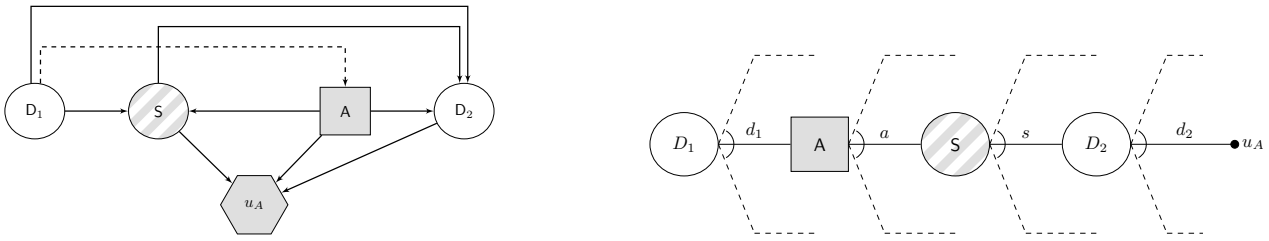
Based on this approach, the Defender's best strategy is to choose first d_1^* at node D_1, and later, after observing $s \in S$, choose $d_2^*(d_1^*, s)$ at node D_2.

Let us discuss now the assessment of $p_D(A|d_1)$. Alternatively to the standard risk analysis approach as in Ezell et al. (2010), we propose ARA to model the Defender's uncertainty about the Attacker's decision assuming he is an expected utility maximiser and taking into account that the Defender's uncertainty stems from her uncertainty about the Attacker's probabilities and utilities associated with his decision problem. The analysis of the Attacker's decision problem, as seen by the Defender, is shown in Figure 17, where the Attacker's probabilities and utilities need to be assessed from the Defender's perspective, based on all the information available to her. Again, should this kind of information not be available to the Defender, she could use a noninformative distribution to describe $p_D(A|d_1)$.

Therefore, to elicit $p_D(A|d_1)$, the Defender needs to assess $u_A(a, s, d_2)$ and $p_A(S|d_1, a)$, as well as $p_A(D_2|d_1, a, s)$. In general, she will not know these quantities, but she may acknowledge her uncertainty about them through a probability distribution $F = (U_A(a, s, d_2), P_A(S|d_1, a), P_A(D_2|d_1, a, s))$ and solve the perceived Attacker's decision problem using backward induction over the decision tree in Figure 17 as follows, propagating the uncertainty in F to get the random variable $A^*(d_1)$ for each d_1:

- At chance node D_2, compute

$$(d_1, a, s) \to \Psi_A(d_1, a, s) = \int U_A(a, s, d_2)\, P_A(D_2 = d_2|d_1, a, s)\, \mathrm{d}d_2.$$



(a) Influence diagram (b) Decision tree ($m = n = 2$)

Figure 17: The Defender's view of the Attacker's decision problem

- At chance node S, compute

$$(d_1, a) \to \Psi_A(d_1, a) = \int \Psi_A(d_1, a, s)\, P_A(S = s|d_1, a)\, \mathrm{d}s.$$

- At decision node A, compute

$$d_1 \to A^*(d_1) = \arg\max_{a \in \mathcal{A}} \Psi_A(d_1, a).$$

Then, the Defender's predictive density $p_D(A|d_1)$ over attacks, conditional on her first defence decision d_1, is given by

$$\int_0^a p_D(A = x|d_1)\mathrm{d}x = \Pr(A^*(d_1) \leq a).$$

This distribution could be approximated by Monte Carlo as follows

Monte Carlo approximation of Defender's predictive density $\mathrm{p_D(A|d_1)}$

1. For each $\mathrm{d_1}$
   For $\mathrm{k = 1}$ to N
   Draw $\left(\mathrm{u_A^k(a, s, d_2), p_A^k(S|d_1, a), p_A^k(D_2|d_1, a, s)}\right) \sim \mathrm{F}$
   At chance node $\mathrm{D_2}$, compute

$$(\mathrm{d_1, a, s}) \to \psi_{\mathrm{A}}^{\mathrm{k}}(\mathrm{d_1, a, s}) = \int \mathrm{u_A^k(a, s, d_2)\ p_A^k(D_2 = d_2|d_1, a, s)\ dd_2}$$

   At chance node S, compute

$$(\mathrm{d_1, a}) \to \psi_{\mathrm{A}}^{\mathrm{k}}(\mathrm{d_1, a}) = \int \psi_{\mathrm{A}}^{\mathrm{k}}(\mathrm{d_1, a, s})\ \mathrm{p_A^k(S = s|d_1, a)\ ds}$$

   At decision node A, compute

$$\mathrm{d_1} \to \mathrm{a_i^*(d_1)} = \arg\max_{\mathrm{a} \in \mathcal{A}} \psi_{\mathrm{A}}^{\mathrm{k}}(\mathrm{d_1, a})$$

2. For any a
   Approximate $\int_0^{\mathrm{a}} \mathrm{p_D(A = x|d_1)\ dx}$ through $\#\{1 \leq \mathrm{k} \leq \mathrm{N} : \mathrm{a_i^*(d_1)} \leq \mathrm{a}\}/\mathrm{N}$.

We have seen how the assessment of $p_D(A|d_1)$ is straightforward after the Defender's elicitation of F. However, the assessment of $P_A(D_2|d_1, a, s)$ within F could be problematic,

as the Defender may want to exploit information available to her about how the Attacker analyses her decision problem. Of course, if there is no information that the Defender can use, she will put a noninformative distribution over $P_A(D_2|d_1, a, s)$. The Defender may continue this recursive analysis, until eventually she has no more information to analyse the next level of the hierarchy of recursive decision models, much as described in Section 3.2.2. The recursive analysis will always stop at some point, perhaps after some simplifications leading to an heuristic distribution to model an adversary's thinking at some step of the recursive analysis, as illustrated in Ríos Insua et al. (2009) for an auction problem.

We provide an example in ANNEX4.

ANNEX3. Sequential Defend-Attack with Private Information Model

We describe now how to solve the model presented in Section 3.5.

The game theoretic approach to games with private information is to model them as games with imperfect information, in which Nature chooses first a possible instance of the Defender's private information and this move from Nature is observed by her, but not by the Attacker.

A Game Theoretic Analysis

We briefly describe how standard game theory solves this model with private and asymmetric information. This is an example of a signaling game, see Aliprantis and Chakrabarti (2000); Cobb and Basuchoudhary (2009). The game-theoretic approach requires the probability assessment of S, conditional on (d, a, v). As the Defender and the Attacker may have different assessments, these will be represented by $p_D(S|d, a, v)$ and $p_A(S|d, a, v)$. The Attacker's prior beliefs about the Defender's private information V are represented through the probability distribution $\pi_A(v)$. All these probabilities, and the utilities $u_D(d, s, v)$ and $u_A(a, s, v)$, are common knowledge. A solution proceeds, then, as follows.

First, we define strategy functions for each player. As the Defender knows the value of V, her strategy function is of the form $v \to d(v) \in \mathcal{D}$. As the Attacker makes his decision knowing the Defender's, his strategy function is of the form $d \to a(d) \in \mathcal{A}$. We compute the expected utilities of both players at node (S) of the tree in Figure 13, for any pair of decisions $(d, a) \in \mathcal{D} \times \mathcal{A}$ and value of private information $V = v$:

$$\psi_D(d, a, v) = \int u_D(d, s, v)\, p_D(S = s|d, a, v)\, ds, \tag{15}$$

$$\psi_A(d, a, v) = \int u_A(a, s, v)\, p_A(S = s|d, a, v)\, ds. \tag{16}$$

The Attacker's best response against a defence d is

$$a^*(d) = \arg\max_{a \in \mathcal{A}} \int \psi_A(d, a, v)\, \pi_A(V = v|d)\, dv, \tag{17}$$

where $\pi_A(V|d)$ represents the Attacker's updated beliefs about the Defender's private information, after having observed her defence action. We show how to determine $\pi_A(V|d)$ below. For now, we shall assume it is known. Under the assumption that the Defender knows how the Attacker will solve his decision problem for any $d \in \mathcal{D}$, the Defender's maximum expected utility decision, given that she knows the value of $V = v$, would be

$$d^*(v) = \arg\max_{d \in \mathcal{D}} \psi_D(d, a^*(d), v).$$

As commonly accepted in game theory, we allow for randomised strategies. Assuming that $\mathcal{D}$ and $\mathcal{A}$ are continuous, we define

$$\Pi_{\mathcal{D}} = \left\{ \pi : \ \pi(d) \geq 0 \ \forall d \in \mathcal{D} \text{ and } \int_{\mathcal{D}} \pi(d) dd = 1 \right\}$$

and

$$\Pi_{\mathcal{A}} = \left\{ \pi : \ \pi(a) \geq 0 \ \forall a \in \mathcal{A} \text{ and } \int_{\mathcal{A}} \pi(a)\mathrm{d}a = 1 \right\}$$

as their associated sets of randomised strategies. Hence, $d^*(v)$ and $a^*(d)$ have associated probability distributions $\pi_{d^*(v)}(d|v) \in \Pi_{\mathcal{D}}$ and $\pi_{a^*(d)}(a|d) \in \Pi_{\mathcal{A}}$, respectively.

We now show how the probability distribution $\pi_{d^*(v)}(d|v)$ is related with $\pi_A(V = v|d)$. Under the assumption that the Attacker knows how the Defender will solve her problem for any $v \in V$, he can update his prior knowledge about V after observing a defence d, through Bayes' rule:

$$\pi_A(V = v|d) \propto \pi_A(V = v)\ \pi_{d^*(v)}(D = d|v),$$

which is the probability distribution needed to compute (17).

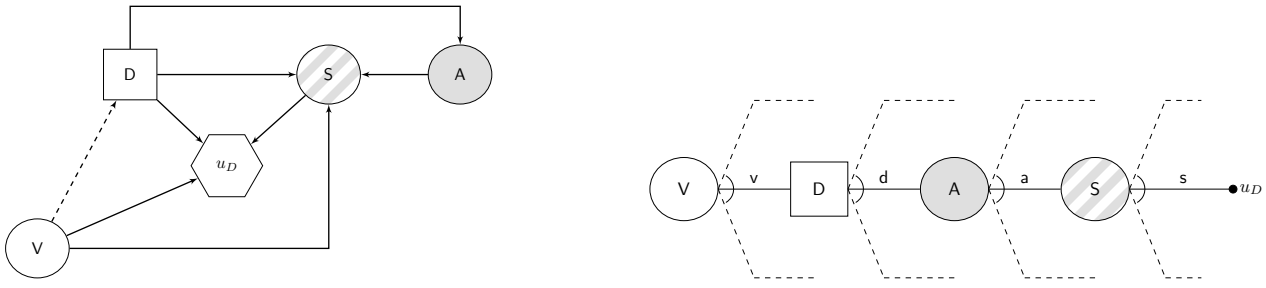
A game theoretic solution can be determined, then, by finding a pair of strategies ($\pi_{d^*(v)}$, $\pi_{a^*(d)}$) which are a fixed point solution of the equations

$$\begin{cases} \pi_{d^*(v)} = \arg\max_{\pi \in \Pi_{\mathcal{D}}} \int_{\mathcal{D}} \left[\int_{\mathcal{A}} \psi_D(d, a, v)\pi_{a^*(d)}(a|d)\,\mathrm{d}a \right] \pi(d)\mathrm{d}d, \ \forall v \in V, \\ \pi_{a^*(d)} = \arg\max_{\pi \in \Pi_{\mathcal{A}}} \int_{\mathcal{A}} \left[\int_{V} \psi_A(d, a, v)\pi_A(v)\pi_{d^*(v)}(d|v)\mathrm{d}v \right] \pi(a)\mathrm{d}a, \ \forall d \in \mathcal{D}. \end{cases} \tag{18}$$

Note that a fixed point solution of the equations in (18) is a Nash equilibrium. In addition, we have assumed that the Attacker's learning behaviour follows Bayes' rule.

The ARA Approach

For a more realistic approach, we weaken the common knowledge assumption. We consider the Defender's decision problem as a standard decision analysis problem, illustrated in Figure 18, with the Attacker's decision node perceived now as a random variable. Similarly, her decision tree shows uncertainty about the Attacker's decision by replacing A with (A).



(a)Influence diagram (b)Decision tree

Figure 18: The Defender's decision problem

Assume, the Defender has already assessed $p_D(S|d, a, v)$ and $u_D(d, s, v)$. She also needs $p_D(A|d)$, which is her assessment of the probability that the Attacker will choose attack $A = a$, after observing that she has chosen defence d. Obtaining this will require that the Defender analyses the problem from the Attacker's perspective. Assume for a moment that

she has assessed $p_D(A|d)$. Then, the Defender can obtain her maximum expected utility defence by solving the tree in Figure 18 using backwards induction as follows:

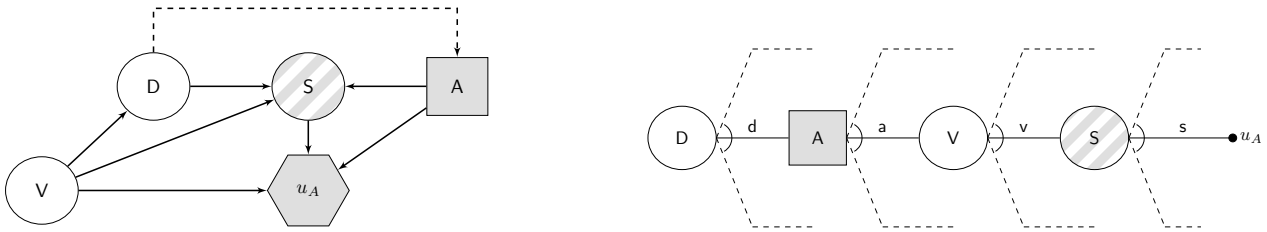
- At chance node S, compute $\psi_D(d, a, v)$ for each (d, a, v) as in (15).
- At chance node A, compute

$$(d, v) \to \psi_D(d, v) = \int \psi_D(d, a, v)\, p_D(A = a|d)\, \mathrm{d}a.$$

- At decision node D, solve

$$v \to d^*(v) = \arg\max_{d \in \mathcal{D}} \psi_D(d, v).$$

To assess $p_D(A|d)$, the Defender must place herself on the Attacker's shoes and solve his decision problem from her perspective. Figure 19 represents the Attacker's decision problem, as seen by the Defender.



(a)Influence diagram (b)Decision tree

Figure 19: The Defender's analysis of the Attacker's decision

Note that the Defender's decision is represented as a random variable in the Attacker's analysis, as it is not under his control. The arrow from (D) to [A] in the influence diagram indicates that the Defender's decision will be known to him at the time he has to decide. As the Attacker does not know the Defender's private information v, his uncertainty is represented through a probability distribution $p_A(V)$, describing the Attacker's (prior) beliefs about the Defender's private information. We assume that the Defender analyses the Attacker's decision considering that he is an expected utility maximiser and that he uses Bayes rule to learn about the Defender's private information from the observation of her defence decision. Thus, the arrow in the influence diagram from (V) to (D), which represents probabilistic dependence, can be inverted to obtain the Attacker's (posterior) beliefs about v: $p_A(V|D = d)$. However, to obtain this we need to assess $p_A(D|v)$ first.

Should the Defender know the Attacker's utility function $u_A(a, s, v)$ and his probabilities $p_A(S|d, a, v)$ and $p_A(V|d)$, she would be able to anticipate his decision $a^*(d)$ for any $d \in \mathcal{D}$ by solving backwards the tree in Figure 19 and computing his expected utility ψ_A as follows:

- At chance node S, compute $\psi_A(d, a, v)$ for each (d, a, v) as in (16).
- At chance node V, compute for each (d, a)

$$\psi_A(d, a) = \int \psi_A(d, a, v)\, p_A(V = v|d)\, \mathrm{d}v. \tag{19}$$

- At decision node A, solve

$$d \rightarrow a^*(d) = \arg\max_{a \in \mathcal{A}} \psi_A(d, a).$$

However, the Defender does not know (p_A, u_A), but she has beliefs about them, say $(P_A, U_A) \sim F$, which will be relevant in her analysis of the Attacker's decision problem. This distribution will induce distributions $\Psi_A(d, a, v)$ and $\Psi_A(d, a)$ on the Attacker's expected utilities defined in (16) and (19), through, respectively,

$$\Psi_A(d, a, v) = \int U_A(a, s, v)\, P_A(S = s|d, a, v)\, \mathrm{d}s$$

and

$$\Psi_A(d, a) = \int \Psi_A(d, a, v)\, P_A(V = v|d)\, \mathrm{d}v,$$

for $(P_A, U_A) \sim F$. Then, the Defender's predictive distribution about the Attacker's response to any of her defence choices d is defined through

$$p_D(A = a|d) = \mathbb{P}_F\left[a = \arg\max_{x \in \mathcal{A}} \Psi_A(d, x)\right],\ \forall a \in \mathcal{A}.$$

The Defender may use Monte Carlo simulation to approximate $p_D(A|d)$ by drawing N samples $\left\{\left(p_A^k, u_A^k\right)\right\}_{k=1}^N$ from F, which produce $\{\psi_A^k\}_{k=1}^N \sim \Psi_A$, and approximating $p_D(A = a|d)$ through

$$\hat{p}_D(A = a|d) = \#\{1 \leq k \leq N :\ a_i^*(d) = a\}/N,\ \forall a \in \mathcal{A},$$

when $A|d$ is discrete, or

$$\hat{p}_D(A \leq a|d) = \#\{1 \leq k \leq N :\ a_i^*(d) \leq a\}/N,\ \forall a \in \mathcal{A},$$

when $A|d$ is absolutely continuous.

To sum up, the elicitation of $F = (P_A(S|d, a, v), P_A(V|d), U_A(a, s, v))$ allows the Defender to solve her problem of assessing $p_D(A|d)$. The Defender may have enough information and judgment available to directly assess $P_A(S|d, a, v)$ and $U_A(a, s, v)$. However, the assessment of $P_A(V|d)$ requires a deeper analysis, as it has a strategic component.

Specifically, assuming that the Attacker has prior knowledge over V modelled through $p_A(V)$, his posterior beliefs about V, after he observes $D = d$, become:

$$p_A(V = v|d) \propto p_A(V = v)\, p_A(D = d|v), \tag{20}$$

where $p_A(D = d|v)$ models the Attacker's probabilistic assessment of what defence she would choose conditional on each possible value of her private information. The elicitation of $p_A(D|v)$ requires an analysis of how the Attacker analyses the Defender's decision. Assuming he thinks that she is an expected utility maximiser, and that the decision problem she tries to solve is as in Figure 18, with A^1 representing the Attacker's decision within this level of recursive modelling, the Defender's elicitation of a probability distribution $G = \left(U_D(d, s, v), P_D(S|d, a, v), P_D(A^1|d)\right)$ representing the Attacker's probabilistic assessments of her utilities and probabilities, allows her to solve her problem of assessing $p_A(D|v)$ by evaluating a tree like the one in Figure 18 as follows:

- At chance node S, compute for each (d, a, v)

$$(d, a, v) \rightarrow \Psi_D(d, a, v) = \int U_D(d, s, v)\, P_D(S = s|d, a, v)\, \mathrm{d}s.$$

- At chance node A^1, compute for each (d, v)

$$(d, v) \rightarrow \Psi_D(d, v) = \int \Psi_D(d, a, v)\, P_D(A^1 = a|d)\, \mathrm{d}a.$$

- At decision node D, solve for each v

$$v \rightarrow p_A(D = d|v) = \mathbb{P}_G\left[d = \arg\max_{x \in \mathcal{D}} \Psi_D(x, v)\right], \forall d \in \mathcal{D}. \tag{21}$$

As the Attacker's beliefs represented within G are assessed from the Defender's perspective, her uncertainty about these beliefs when acknowledged within G will produce the distribution $P_A(D|v)$ in (21), representing what the Defender believes to be $p_A(D|v)$. Note also that $p_A(V)$ in (20) represents the Attacker's prior knowledge about the Defender's private information. As the Defender does not have access to this distribution, we will directly elicit it from the Defender's perspective: $P_A(V)$ represents what she believes to be $p_A(V)$, with the probabilistic model P_A acknowledging her confidence on her assessment of p_A. Then, from the Defender's perspective, the Attacker's learning about V modelled in (20) becomes

$$P_A(V = v|d) \propto P_A(V = v)\, P_A(D = d|v). \tag{22}$$

The only difficulty for the Defender at this step, in order to obtain $P_A(D|v)$, is her assessment of what she thinks to be the Attacker's assessment of the probability model used by her to predict his attack as a response to her chosen defence: $P_D(A^1|d)$ in G. We may go further in the hierarchy of nested decision models and try to support the Defender in the assessment of $P_D(A^1|d)$ through the analysis of how the Attacker, in his analysis of her decision problem, thinks the Defender will analyse his decision problem, similarly as described in Section 3.2.2. However, if no information is available at this level, we can end the hierarchy of analysis with a reference distribution over $P_D(A^1|d)$. This would allow the computation of a recommendation for action to the Defender. Clearly, should this recommendation be sensitive to the reference distribution, this would indicate that there is still relevant information that needs to be elicited before reaching a robust enough recommendation. In such case, it would be desirable to collect more data and/or judgement through intelligence.

ANNEX4. Examples

We provide now examples for all the models discussed in the previous sections. These examples have a double motivation: on one hand, they are intended to illustrate the theoretical results of the ARA analysis developed throughout this deliverable. On the other hand, they will also serve as links to work packages WP1, WP2 and WP3, which are responsible of the case studies that SECONOMICS is dealing with. Specifically:

- The first example, for the Sequential Defend-Attack problem, is related with the issue of anti-social behavior (e.g., graffiti) in metro installations, as described in WP3.
- The second example, for the Simultaneous Attack-Defend problem, illustrates a decision making problem of a transport operator in deploying new security measures, as proposed in WP1.
- The third example, for the Sequential Attack-Defend problem, reflects the problematic of the case study of protecting a critical infrastructure as in WP2.
- The fourth example, for the Sequential Defend-Attack-Defend problem is also related with a decision making problem of a given transport operator in employing new security measures, as in WP1.
- The fifth example, for the Sequential Defend-Attack problem with Private Information also considers protection of critical infrastructures, being therefore related with WP2.

Sequential Defend-Attack model: security staff deployment strategy against vandalic acts

As an illustration for this type of model, we propose a simple example concerning security at the installations of a given metro transport operator, regarding some kind of antisocial behaviour, e.g. acts of vandalism as painting graffiti or scratching the windows of the trains, as discussed in more detail in deliverable *D3.2 - Urban public transport requirements*. In this regard, the metro Chief Executive Officers (M-CEO, the Defender) have reported several acts of vandalism and urban violence from anti system groups against their installations and equipment. The Defender is considering several strategies to protect their fixtures against possible attacks of such anti system groups (the Attacker). In a first approach, M-CEO's strategies can be thought of how many additional staff and security members are going to be deployed in the metro installations to control the agitators, with respect to the usual number of personnel deployed in standard circumstances. Specifically, four different strategies d_1, d_2, d_3, d_4 are being considered respectively consisting of deploying 10, 20, 40 or 50 additional staff and security members in the metro installations.

The Attacker will know the action chosen by the Defender, as such information will be disseminated by the media. We assume that the Attacker aims at causing widespread damage in the metro fixtures, attacking security as well as trains and other installations. Specifically, the Attacker is planning three different types of attack, a_1, a_2, a_3, depending on what means they will use to cause damages: (1) only the strength of their hands; (2) same as before plus using physical weapons as bricks, hammers, containers, or stain balls to break the windows and/or dent the bodywork of the trains; or (3) same as before plus using chemical weapons, as Molotov cocktails, paint, silicon or corrosive acids, to cause more serious harms. We also assume that there are three different levels of success

of a given attack: failure ($s = 0$), moderate damages ($s = 1$), and severe damages ($s = 2$), on any of the targets considered by the Attacker. We denote this set of possible outcomes by $\mathcal{S}$.

We assume that we are able to assess from the Defender:

- Metro's utility function $u_D(d, s)$, which incorporates the increase in security, costs, and other possible consequences, and the probability distribution $p_D(S = s|d, a)$ associated with the decision problem (Figure 6), shown in Tables 1a, 1b and 1c, respectively ($p_D(S = 0|d, a)$ is implicit).
- The Defender presumes that the anti system groups will face a decision problem similar to that described in Figure 7. She assesses that the random utilities and probabilities $(U_A, P_A) \sim F$ of the Attacker are as in Tables 1d and 1e. The probabilities $P_A(S = \{0, 1, 2\}|d, a)$ are modelled through Dirichlet distributions $\mathcal{D}ir(\alpha_1, \alpha_2, \alpha_3)$, with expected values $\alpha_i/(\alpha_1 + \alpha_2 + \alpha_3)$, $i = 1, 2, 3$, respectively, matching the Defender's probabilities. For example, $P_A(S = \{0, 1, 2\}|d_1, a_1) \sim \mathcal{D}ir(4.5, 2.5, 3)$ means that, given that the Defender will deploy a defence d_1 and the Attacker will then choose an attack a_1, she assesses the Attacker's beliefs about the output of his attack ($S = 0$, $S = 1$ or $S = 2$) through point estimates probabilities $\hat{p}_A(S = 0|d_1, a_1) = 4.5/(4.5 + 2.5 + 3) = 0.45$, $\hat{p}_A(S = 1|d_1, a_1) = 0.25$, and $\hat{p}_A(S = 2|d_1, a_1) = 0.3$ (with corresponding variances 0.023, 0.017, and 0.019).

Table 1: Defender's assessments

(a) $u_D(d, s)$

	$s = 0$	$s = 1$	$s = 2$
d_1	200	50	10
d_2	100	20	10
d_3	80	10	0
d_4	50	0	0

(b) $p_D(S = 1|d, a)$

	a_1	a_2	a_3
d_1	0.25	0.45	0.5
d_2	0.2	0.25	0.35
d_3	0.15	0.2	0.25
d_4	0.1	0.15	0.2

(c) $p_D(S = 2|d, a)$

	a_1	a_2	a_3
d_1	0.3	0.35	0.4
d_2	0.25	0.3	0.35
d_3	0.2	0.25	0.3
d_4	0.05	0.1	0.15

(d) $U_A(a, s)$

	$s = 0$	$s = 1$	$s = 2$
a_1	0	$Tri(50, 60, 80)$	$Tri(80, 100, 100)$
a_2	0	$Tri(40, 50, 60)$	$Tri(60, 80, 90)$
a_3	0	$Tri(25, 40, 50)$	$Tri(60, 70, 90)$

(e) $P_A(S = \{0, 1, 2\}|d, a)$

	a_1	a_2	a_3
d_1	$\mathcal{D}ir(4.5, 2.5, 3)$	$\mathcal{D}ir(2, 4.5, 3.5)$	$\mathcal{D}ir(1, 5, 4)$
d_2	$\mathcal{D}ir(5.5, 2, 2.5)$	$\mathcal{D}ir(4.5, 2.5, 3)$	$\mathcal{D}ir(3, 3.5, 3.5)$
d_3	$\mathcal{D}ir(6.5, 1.5, 2)$	$\mathcal{D}ir(5.5, 2, 2.5)$	$\mathcal{D}ir(4.5, 2.5, 3)$
d_4	$\mathcal{D}ir(8.5, 1, 0.5)$	$\mathcal{D}ir(7.5, 1.5, 1)$	$\mathcal{D}ir(6.5, 2, 1.5)$

Note: $Tri(min, mode, max)$ and $\mathcal{D}ir(\alpha_1, \alpha_2, \alpha_3)$ stand, respectively, for triangular and Dirichlet distributions.

To solve the Defender's decision problem, we need to assess $\hat{p}_D(a_j|d_i)$, $i = 1, \ldots, m$, $j = 1, \ldots, n$, her predictive distribution about what the Attacker will do, once they know her defence. Then, she would find the optimal defence. Based on (7), she would proceed as follows:

Simulation for the Sequential Defend-Attack problem

1. Estimate $\hat{p}_D(a_j|d_i)$ for each d_i

For $i = 1$ to m

  For $k = 1$ to N

    For $j = 1$ to n

      Draw $(u_A^k, p_A^k) \sim (U_A, P_A) = F$ for all possible outcomes $s \in \mathcal{S}$

      Compute $\psi_A^k(d_i, a_j) = \sum_{s\in\mathcal{S}} p_A^k(s|d_i, a_j)\, u_A^k(a_j, s)$

    Compute $a^* = \arg\max_{x\in\mathcal{A}} \psi_A^k(d_i, x)$

    $\hat{p}_D(a^*|d_i) = \hat{p}_D(a^*|d_i) + 1$

  $\hat{p}_D(a_j|d_i) = \hat{p}_D(a_j|d_i)/N,\ \forall j$

2. Compute optimal defence

For $i = 1$ to m

  Compute $\psi_D(d_i) = \sum_{j=1}^{n} \hat{p}_D(a_j|d_i)\left[\sum_{s\in\mathcal{S}} p_D(s|d_i, a_j)\right] u_D(d_i, s)$

Compute $d^* = \arg\max \psi_D(d_i)$

In a run with $N = 10,000$, we got the approximation for the probabilities $\hat{p}_D(a|d)$ shown in Table 2.

Table 2: Expected probabilities $\hat{p}_D(a|d)$

$\hat{p}_D(a\|d)$	a_1	a_2	a_3
d_1	0.2493	0.4002	0.3505
d_2	0.3112	0.2818	0.4070
d_3	0.2909	0.3026	0.4065
d_4	0.1630	0.3116	0.5254

The Defender can now solve her decision problem, obtaining that her maximum expected utility defence is $d^* = d_1$ with (Monte Carlo estimated) expected utility 70.09. Therefore, the best strategy for the Defender would be the deployment of 10 additional security staff, since this strategy maximizes her expected utility. On the other hand, and as assessed by the metro executives in Table 2, the most probably attacking strategy chosen by the Attacker would be a_2, i.e., using the strength of their hands and physical weapons to cause as much damage as possible. The complete list of estimated expected utilities is displayed in Table 3.

Table 3: Estimated expected utilities $\hat{\psi}_D(d)$

	$\hat{\psi}_D(d)$
d_1	70.09
d_2	50.53
d_3	45.12
d_4	35.66

Simultaneous Defend-Attack model: A decision making problem for a transport operator

In this second example, we analyse a decision making problem concerning security issues in a transport operator, considering whether or not to deploy new security measures. The case study described in deliverable *D1.3 Airport Requirements* analyses this problem for Anadolu Airport, in Turkey.

The Airport Chief Executive Officer (A-CEO, the Defender) is considering whether to use (d_1) or not (d_2) undercover marshals in the installations of the Airport to prevent terrorists from attacking the airport's fixtures, aircrafts or users (passenger, crew, staff). The terrorists (the Attacker) will not know the action chosen by the Defender in their analysis about whether to try (a_1) or not (a_2) to perform a terrorist attack. We assume that we are able to assess from the Defender:

Table 4: Defender's assessments

(a)$u_D(d,s)$

	$s=1$	$s=0$
d_1	0	80
d_2	10	100

(b)$p_D(S=1|d,a)$

	a_1	a_2
d_1	0.1	0
d_2	0.8	0

(c)$U_{A_I}(a,s)$

	$s=1$	$s=0$
a_1	$Tri(50,100,100)$	0
a_2	100	$Tri(0,0,50)$

(d)$P_{A_I}(S=1|d,a)$

	a_1	a_2
d_1	$\mathcal{U}(0,0.5)$	0
d_2	$\mathcal{U}(0.5,1)$	0

(e)$U_{A_{II}}(a,s)$

	$s=1$	$s=0$
a_1	$Tri(0,100,100)$	0
a_2	100	$Tri(0,0,100)$

(f)$P_{A_{II}}(S=1|d,a)$

	a_1	a_2
d_1	$Tri(0,0,0.5)$	0
d_2	$Tri(0.5,1,1)$	0

(g)$U_{D_I}(d,s)$

	$s=1$	$s=0$
d_1	$\mathcal{U}(0,40)$	$\mathcal{U}(60,100)$
d_2	$\mathcal{U}(0,40)$	$\mathcal{U}(60,100)$

(h)$P_{D_I}(S=1|d,a)$

	a_1	a_2
d_1	$\mathcal{U}(0,b)$	0
d_2	$b \sim \mathcal{U}(0,1)$	0

Note: $\mathcal{U}(min,max)$ stand for uniform distribution.

- Her utility function $u_D(d,s)$, which incorporates the increase in security, the costs, as well as other possible consequences, and her probability distribution $p_D(S=s|d,a)$ associated with her decision problem (Figure 9), shown in Tables 4a and 4b respectively.
- She considers that the terrorist threat may come from two different kinds of Attackers: Class I with probability 0.8 and Class II with 0.2. She also presumes that terrorists will face a decision problem as described in Figure 10. The Defender assesses that the utilities and probabilities of a Class I Attacker in (10) are $(U_{A_I}, P_{A_I}) \sim F_I$, see Tables 4c and 4d, and those of a Class II Attacker are $(U_{A_{II}}, P_{A_{II}}) \sim F_{II}$, see Tables 4e and 4f.
- Based on the information available, the Defender thinks that a Class I Attacker is capable of analyzing her problem as in Figure 9. She estimates that a Class I Attacker's beliefs about her

utilities and probabilities in (11) are $(U_{D_I}, P_{D_I}) \sim G_I$, shown in Tables 4g and 4h. The Defender's confidence in these assessments leads her to elicit $\Pi_{A_I}(D_I = d_1)$ as a beta distribution with mean $\pi_{A_I}(D_I = d_1)$ and precision 10, that is, $\Pi_{A_I}(D_I = d_1) \sim \mathcal{B}e(\alpha, 10-\alpha)$, where $\alpha = \pi_{A_I}(D_I = d_1) \times 10$.

The Defender has no information to assess how a Class II Attacker would analyse her problem. However, she believes that this Attacker estimates that she is more likely to choose d_1, specifically, that $\Pi_{A_{II}}(D_{II} = d_1) \sim \mathcal{B}e(75, 25)$.

- Finally, she assigns a noninformative unconditional distribution on what a Class I Attacker thinks to be her beliefs over his choice of action: $\Pi_{D_I}(A_I^1 = a_1) \sim \mathcal{U}(0, 1)$.

To solve the Defender's decision problem, we need to assess $\pi_D(A = a_1)$, her predictive distribution about what the terrorists will do, where A is the mixture $0.8\,A_I + 0.2\,A_{II}$, with A_I (A_{II}) representing the Defender's beliefs about what attack in $\mathcal{A} = \{a_1, a_2\}$ a Class I (II) terrorist will choose. Thus,

$$\pi_D(A = a_1) = 0.8\ \pi_D(A_I = a_1) + 0.2\ \pi_D(A_{II} = a_1).$$

Based on (10) and (11), $\pi_D(A_I = a_1)$ could be estimated through Monte Carlo simulation as follows:

Simulation for the Class I terrorist

1. For $\mathtt{k} = 1$ to $\mathtt{N}$
   - Draw $\pi^{\mathtt{k}}_{\mathtt{D_I}} \sim \Pi_{\mathtt{D_I}} = \mathcal{U}(0, 1)$
   - Draw $(\mathtt{u}^{\mathtt{k}}_{\mathtt{D_I}}, \mathtt{p}^{\mathtt{k}}_{\mathtt{D_I}}) \sim (\mathtt{U}_{\mathtt{D_I}}, \mathtt{P}_{\mathtt{D_I}}) = \mathtt{G_I}$
   - Compute $\mathtt{d}^{\mathtt{k}}_{\mathtt{I}} = \arg\max_{\mathtt{d}\in\mathcal{D}} \sum_{\mathtt{a}\in\mathcal{A}} \left[\sum_{\mathtt{s}\in\{0,1\}} \mathtt{u}^{\mathtt{k}}_{\mathtt{D_I}}(\mathtt{d}, \mathtt{s})\ \mathtt{p}^{\mathtt{k}}_{\mathtt{D_I}}(\mathtt{S} = \mathtt{s}|\mathtt{d}, \mathtt{a})\right] \pi^{\mathtt{k}}_{\mathtt{D_I}}(\mathtt{A}^{\mathtt{1}}_{\mathtt{I}} = \mathtt{a})$
2. Approximate $\pi_{\mathtt{A_I}}(\mathtt{D_I} = \mathtt{d}_1)$ through $\hat{\pi}_{\mathtt{A_I}}(\mathtt{D_I} = \mathtt{d}_1) = \#\{1 \le \mathtt{k} \le \mathtt{N} : \mathtt{d}^{\mathtt{k}}_{\mathtt{I}} = \mathtt{d}_1\}/\mathtt{N}$
   Set $\alpha = \hat{\pi}_{\mathtt{A_I}}(\mathtt{D_I} = \mathtt{d}_1) \times 10$
   Set $\hat{\Pi}_{\mathtt{A_I}}(\mathtt{D_I} = \mathtt{d}_1) \sim \mathcal{B}\mathtt{e}(\alpha, 10 - \alpha)$
3. For $\mathtt{j} = 1$ to $\mathtt{N}$
   - Draw $\hat{\pi}^{\mathtt{k}}_{\mathtt{A_I}} \sim \hat{\Pi}_{\mathtt{A_I}}$
   - Draw $(\mathtt{u}^{\mathtt{k}}_{\mathtt{A_I}}, \mathtt{p}^{\mathtt{k}}_{\mathtt{A_I}}) \sim (\mathtt{U}_{\mathtt{A_I}}, \mathtt{P}_{\mathtt{A_I}}) = \mathtt{F_I}$
   - Compute $\mathtt{a}^{\mathtt{k}}_{\mathtt{I}} = \arg\max_{\mathtt{a}\in\mathcal{A}} \sum_{\mathtt{d}\in\mathcal{D}} \left[\sum_{\mathtt{s}\in\{0,1\}} \mathtt{u}^{\mathtt{k}}_{\mathtt{A_I}}(\mathtt{a}, \mathtt{s})\ \mathtt{p}^{\mathtt{k}}_{\mathtt{A_I}}(\mathtt{S} = \mathtt{s}|\mathtt{d}, \mathtt{a})\right] \hat{\pi}^{\mathtt{k}}_{\mathtt{A_I}}(\mathtt{D_I} = \mathtt{d})$
4. Approximate $\pi_{\mathtt{D}}(\mathtt{A_I} = \mathtt{a}_1)$ through $\hat{\pi}_{\mathtt{D}}(\mathtt{A_I} = \mathtt{a}_1) = \#\{1 \le \mathtt{k} \le \mathtt{N} : \mathtt{a}^{\mathtt{k}}_{\mathtt{I}} = \mathtt{a}_1\}/\mathtt{N}$

Similarly, $\pi_D(A_{II} = a_1)$ can be estimated by Monte Carlo simulation as follows.

Simulation for the Class II terrorist

3'. For $\mathtt{k} = 1$ to $\mathtt{N}$
   - Draw $\hat{\pi}^{\mathtt{k}}_{\mathtt{A_{II}}} \sim \hat{\Pi}_{\mathtt{A_{II}}} = \mathcal{B}\mathtt{e}(75, 25)$
   - Draw $(\mathtt{u}^{\mathtt{k}}_{\mathtt{A_{II}}}, \mathtt{p}^{\mathtt{k}}_{\mathtt{A_{II}}}) \sim (\mathtt{U}_{\mathtt{A_{II}}}, \mathtt{P}_{\mathtt{A_{II}}}) = \mathtt{F_{II}}$
   - Compute $\mathtt{a}^{\mathtt{k}}_{\mathtt{II}} = \arg\max_{\mathtt{a}\in\mathcal{A}} \sum_{\mathtt{d}\in\mathcal{D}} \left[\sum_{\mathtt{s}\in\{0,1\}} \mathtt{u}^{\mathtt{k}}_{\mathtt{A_{II}}}(\mathtt{a}, \mathtt{s})\ \mathtt{p}^{\mathtt{k}}_{\mathtt{A_{II}}}(\mathtt{S} = \mathtt{s}|\mathtt{d}, \mathtt{a})\right] \hat{\pi}^{\mathtt{k}}_{\mathtt{A_{II}}}(\mathtt{D_{II}} = \mathtt{d})$
4'. Approximate $\pi_{\mathtt{D}}(\mathtt{A_{II}} = \mathtt{a}_1)$ through $\hat{\pi}_{\mathtt{D}}(\mathtt{A_{II}} = \mathtt{a}_1) = \#\{1 \le \mathtt{k} \le \mathtt{N} : \mathtt{a}^{\mathtt{j}}_{\mathtt{II}} = \mathtt{a}_1\}/\mathtt{N}$

In a run with $N = 10,000$, we got $\hat{\pi}_D(A_I = a_1) = 0.84$ and $\hat{\pi}_D(A_{II} = a_1) = 0.39$. Hence, $\pi_D(A = a_1)$ can be approximated by $\hat{\pi}_D(A = a_1) = 0.8\ \hat{\pi}_D(A_I = a_1) + 0.2\ \hat{\pi}_D(A_{II} = a_1) = 0.75$. In other words, the Defender thinks that it is three times more likely that the terrorists (whether of Class I or II), would perform a terrorist attack against the airport installations than the possibility of they remaining inactive.

The Defender can now solve her decision problem in (8), obtaining that her maximum expected utility defence is $d^* = d_1$ with (Monte Carlo estimated) expected utility 74.0, against d_2 whose expected utility is 45.9. Hence, the optimal strategy from the point of view of the Defender is to undercover marshals in the airport installations.

Sequential Attack-Defend model: protection of critical infrastructures

We consider now an example in which the integrity of a major national critical infrastructure is at risk, due to threats of a terrorist organization. This example can serve as an illustration for the deliverable of WP2, *D2.3 National Grid Requirements*, in which the UK National Grid is analysed in detail.

In this simplified version of the case study, let us assume that a Government (the Defender) needs to protect two critical installations 1 and 2 within their National Grid gas and electricity infrastructure. A terrorist organization (the Attacker) may perform a full attack over 1 (a_1), a full attack over 2 (a_2), no attacks (a_3), or two low profile attacks over both installations (a_4). On the other hand, we assume that the Defender can deploy three different levels of defensive actions to recover herself against the Attacker's attack, with different levels of monetary and human resources to recover and fix the possible damages produced by the Attacker. Specifically, we denote the three recovery plans by: low-level plan (d_1), medium-level plan (d_2), and high-level plan (d_3). When greater investments are made, the recovery from the attack will be achieved in shorter times, but the indebtedness incurred by the Government may be too onerous for the public budget. On the other hand, if the Defender decides to invest less money, the recovery will be delayed and/or accomplished in an incomplete manner, leaving the security of the critical installations into jeopardy. We shall simplify the problem by regarding the attack as a binary outcome $S \in \{0, 1\}$, representing its failure or success. The decision tree for this problem would be as shown in Figure 20

We assume that we are able to assess from the Defender the following utilities and probabilities summarized in Table 5:

Table 5: Defender's assessments

(a) $u_D(d, s)$

	d_1	d_2	d_3
$s = 0$	100	80	50
$s = 1$	20	10	0

(b) $p_D(S = 1|d, a)$

	d_1	d_2	d_3
a_1	0.7	0.4	0.05
a_2	0.6	0.3	0.05
a_3	0	0	0
a_4	0.3	0.1	0.05

(c) $U_A(a, s)$

	$s = 0$	$s = 1$
a_1	0	$Tri(60, 80, 90)$
a_2	0	$Tri(50, 70, 80)$
a_3	0	0
a_4	0	$Tri(45, 60, 70)$

(d) $P_A(S = 1|d, a)$

	d_1	d_2	d_3
a_1	$\mathcal{B}e(6, 4)$	$\mathcal{B}e(4, 6)$	$\mathcal{B}e(2, 8)$
a_2	$\mathcal{B}e(6, 4)$	$\mathcal{B}e(4, 6)$	$\mathcal{B}e(2, 8)$
a_3	0	0	0
a_4	$\mathcal{B}e(4, 6)$	$\mathcal{B}e(3, 7)$	$\mathcal{B}e(1, 9)$

(e) $P_A(d|a)$

	$\{d_1, d_2, d_3\}$
a_1	$\mathcal{D}ir(2, 3, 5)$
a_2	$\mathcal{D}ir(2, 3, 5)$
a_3	$\mathcal{D}ir(7, 2, 1)$
a_4	$\mathcal{D}ir(2.5, 3.5, 4)$

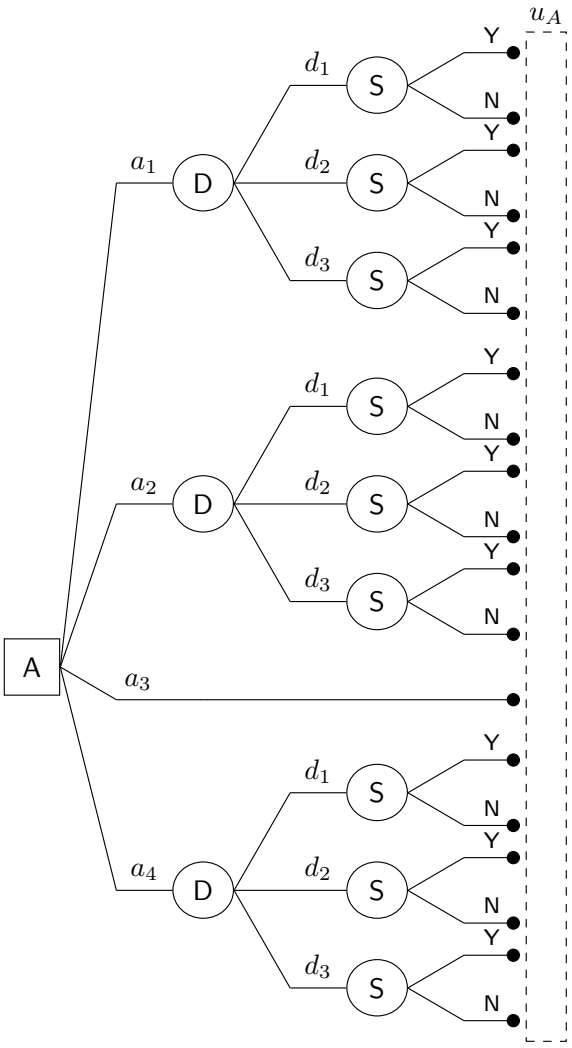


Figure 20: Decision tree for the Sequential Attack-Defend example

In a run with $N = 10,000$, we got the estimated probabilities $\hat{p}_D(a)$ shown in Table 6.

Table 6: Estimated probabilities for the different attacks

	a_1	a_2	a_3	a_4
$\hat{p}_D(a)$	0.5003	0.4666	0	0.0331

As we can observe, attacks a_1 and a_2 are regarded almost as equally likely by the Defender, and much more likely than a_4. In other words, the Government believes that the more realistic scenario, according to their beliefs and information, is that the terrorist will perform a full attack, with almost equal probabilities, over just one of the two installations.

The associated contingency plan for recovery from attacks is shown in Table 7.

Table 7: Optimal recovery plan $d^*(a)$

	a_1	a_2	a_4
$d^*(a)$	d_2	d_2	d_1

The estimated utilities $\psi_D(a, d)$ are shown in Table 8.

Table 8: Estimated utilities $\psi_D(a, d)$

	d_1	d_2	d_3
a_1	44	52	47.5
a_2	52	59	47.5
a_4	76	73	47.5

From Tables 7 and 8 it is clear that the optimal strategy for the Defender is a medium-level recovery plan, provided the terrorist will behave as they expect. Should the terrorists perform two low key attacks against both installations, then the optimal strategy would be a low-level recovery plan, as in this case the damages would be expected to be limited. Strategy a_3 (no attacks from the terrorist) is actually neglected by the Defender, as they assess a zero probability to it.

Sequential Defend-Attack-Defend: defending transportation from terrorist threats

We consider now how ARA may cope with a realistic example. For simplicity, we will follow here the exposition in Sevillano et al. (2012), referring to defending a ship which needs to travel through the Aden Gulf in face of piracy risks. However, this example can be easily adapted to other means of transport and their involved installations as e.g. those related with the airport case study, as discussed in deliverable *D1.3 Airport Requirements*.

Starting from the early 90's, piracy has been a threat to international marine transportation and fishing ships around the coasts of Somalia[1]. Since 2005, several international organizations have expressed their worries about the increase in piracy acts. Nowadays, no ship is safe within several hundred miles from the Somali coast, and this has become a major international security issue. Somali pirates, originally dedicated to fishing, have traditionally claimed that the actual pirates are the foreign fishermen who loot their fish. Piracy in Somalia may be explained in purely business terms, see Carney et al. (2009), as there is actually a whole system supporting their activities. The elderly act, *de facto*, as a government. Local businessmen provide funding. There is a clear organization as attacks are undertaken by small groups of around ten individuals in fast offshore boats which depart from a mothership. Once successful, around fifty pirates remain in the boarded ship, with around fifty more pirates providing logistic support from the coast. Pirates have learned that ransom is more profitable than theft and they reinvest part of their earnings in equipment and training.

We shall assume that we support a (large tuna fish) ship owner in deciding what defensive resources to implement and, if attacked and hijacked, how to respond to Somali pirates demanding a ransom in exchange of the kidnapped ship and crew.

[1] See the Wikipedia page on piracy in Somalia: http://en.wikipedia.org/wiki/Piracy_in_Somalia

Structuring the Somali Pirates Case

We describe here how to support a ship owner in managing risks from piracy in the coast of Somalia, structuring the problem through a game tree. We shall use a Sequential Defend-Attack-Defend model, see Brown et al. (2006), Parnell et al. (2010) or Ríos and Ríos Insua (2012), to formulate the problem. The ship owner will pro-actively decide on a defensive strategy to reduce piracy risks, ranging from different levels of deployed armed security to sailing through an alternative, much longer, route avoiding the pirates completely. The pirates, who have a network of spies and observers informing about security, cargo and crew in ships, will respond to the Defender's move by launching (or not) an attack with the intention of taking over the ship and asking for a ransom. If the Pirates' operation is successful, the ship owner will have to decide on paying or not the ransom, or even asking for the support of the nearby armed forces to release the ship. The ship is assumed to be of Spanish ownership, with Spanish crew, for the economical computations involved.

Specifically, we shall assume that the ship owner (the Defender, She) initially decides on one of the following four alternative defence actions (elements of $\mathcal{D}_1$):

d_1^0 : Do nothing, i.e. no defensive action is taken.

d_1^1 : Use private protection with an armed person.

d_1^2 : Use private protection with a team of two armed persons.

d_1^3 : Do the trip through the Cape of Good Hope, rather than the Suez Channel, thus avoiding the Somali coast and a potential hijack.

Once the Defender has made her initial decision, the pirates (the Attacker, He) observe this and decide whether to attack ($a^1 \in \mathcal{A}$) or not ($a^0 \in \mathcal{A}$). The attack results in either the ship being hijacked ($S = 1$) or not ($S = 0$) by the pirates, with probabilities depending on the initial defence action chosen by the ship's owner. If the ship is hijacked, the Defender has the option of responding by either (elements of $\mathcal{D}_2$):

d_2^0 : Doing nothing, i.e. not responding to the pirates' demands, assuming all entailed costs.

d_2^1 : Pay the amount finally demanded by the pirates, thus recovering the ship and crew.

d_2^2 : Ask for military support to release the ship and crew.

The asymmetric game tree shown in Figure 21 represents the sequence of decisions and events faced by the owner and pirates in this case, where nodes D_1 and D_2 correspond, respectively, to the Defender's first and second decisions, node A represents the Attacker's decision, and chance node S represents the outcome of the attack. We include (c_D, c_A) which represent the generic consequences that the Defender and the Attacker face, respectively, for the corresponding sequence of decisions and attack results.

modelling the Defender's own Preferences and Beliefs In supporting the Defender, her decision problem is seen as the decision tree in Figure 22, in which the Attacker's decision node [A] has been replaced by chance node (A). This reflects that the Attacker's decision is seen as an uncertainty by the Defender, with the bulk of the modelling work consisting of the assessment of her probabilities over the Attacker's actions. Thus, to solve her decision problem, she needs to assess $p_D(A|d_1)$, her predictive probability of an attack given each $d_1 \in \mathcal{D}_1$, besides the more standard assessments $p_D(S|d_1, a^1)$ and $u_D(c_D)$, with c_D representing her monetary cost equivalent of the

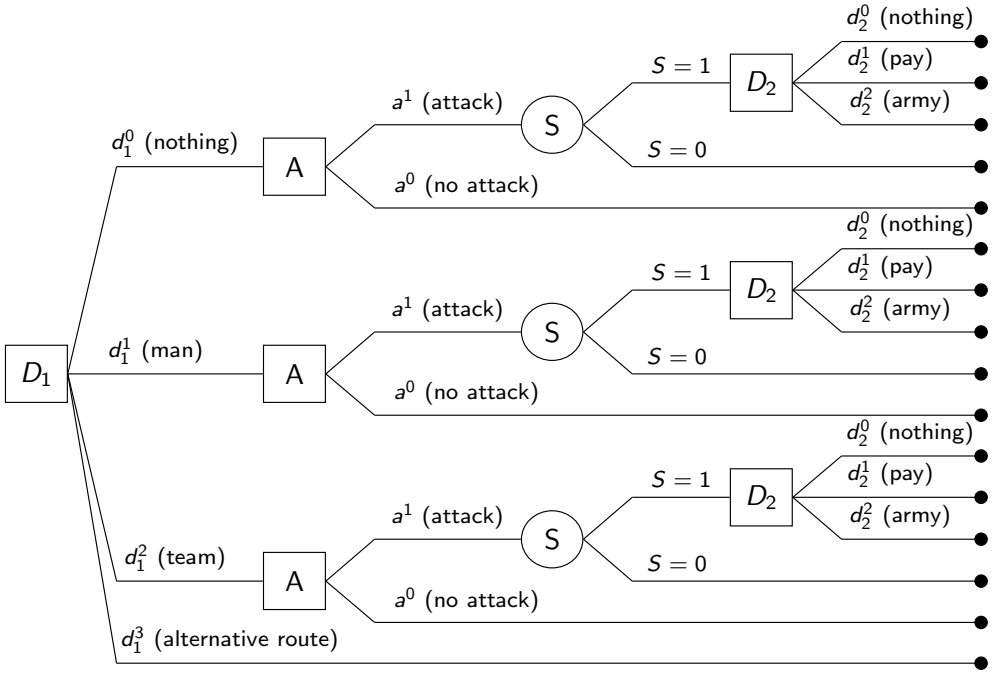


Figure 21: Game tree for the Somali pirates case

multi-attribute consequences associated with each leaf. We now specify the standard assessments, starting with her preferences.

The relevant consequences for the Defender in this problem are

- The loss of the ship,
- The costs associated with defending and responding to an eventual attack, and
- The number of deaths on her side.

As far as the costs associated with implementing her protective and response actions against an eventual hijacking are concerned, we have that, for the defensive actions in $\mathcal{D}_1$, these costs are:

- 0 euros, if she chooses to do nothing, d_1^0,
- 0.05M euros, if she chooses to use one armed person, d_1^1. This corresponds to the salary of the armed person for 6 months, plus equipment.
- 0.15M euros, if she chooses an armed team, d_1^2. This cost corresponds to the salary of two armed persons, with better equipment, for 6 months.
- 0.5M euros, if she chooses d_1^3, going around the Cape of Good Hope. This cost is consequence of the longer distance of the trip. Bad weather conditions might also increase the cost of this longer trip, but we shall neglect this uncertainty here.

The costs associated with the defence actions in $\mathcal{D}_2$ are:

- 0 euros, for option d_2^0, doing nothing.

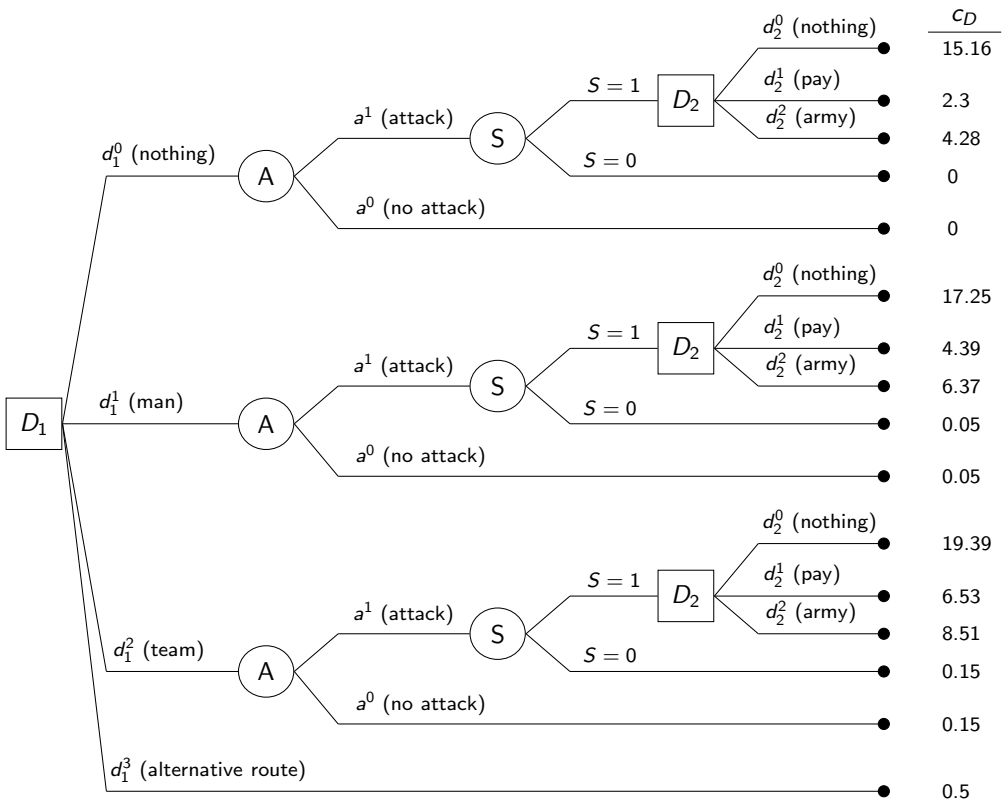


Figure 22: Decision tree representing the Defender's decision problem for the Somali pirates case

- 2.3M euros, for option d_2^1, paying the ransom. We have estimated it through the average of the latest ransoms paid, which were, see Carney et al. (2009), 2.2M for Le Ponant; 2M for Mt Stolt Melati 5; 1.1M for Mt Stolt Valor; 3M for Sirius Star; and 3.2M for Mv Faina. Given the uncertainty in the ransom negotiations involved, we could model this as a random variable, but, for simplicity, we shall not do this here.

- 0.2M euros, for option d_2^2, calling for the Navy. This estimation is based on a military intervention using the international coalition ships already deployed in the area, including one Spanish ship.

As far as human lives are concerned, we consider that if the ship is attacked and the attack is aborted ($S = 0$), there are no lives lost. If the attack is successful ($S = 1$), we assume that the armed Defenders have died and that, depending on the chosen response at D_2, there might be additional lives lost, specifically:

- If the response to the kidnapping is doing nothing, d_2^0, the pirates might kill part of the crew as a warning for future hijacks. We estimate this to be four crew members, though again some uncertainty exists, which we do not treat here.

- If the ship owner decides to pay the ransom, d_2^1, there will be no additional human loss.

- If the hijacked ship is rescued by the Navy, d_2^2, we estimate that there might be two casualties due to both collateral damage during the intervention and/or because the pirates feel threatened and kill some of the crew during the operation. Again, there would be uncertainty involved, not treated here.

We monetize the value of the ship and crew lives. The type of ships operating in that area, focusing on tuna fishing, have a length between 80 and 110 m and lots of technology built in. A new ship of this class costs between 9M and 12M euros. Assuming some depreciation because of time, we shall consider that the incumbent ship is valued in 7M euro. As far as quantifying the value of a human life, we shall use the concept of statistical value of a life, see Martínez Pérez and Méndez Martínez (2009), which, according to Riera Font et al. (2007), was estimated as 2.04M euros for a Spanish person.

Table 9 summarises the estimated consequences and aggregated monetary costs c_D for the Defender associated with each scenario consisting of a path in the tree shown in Figure 21. Clearly, if there is no attack ($a = a^0$), we have that $S = 0$.

Table 9: Consequences of various tree paths for the Defender

D_1	S	D_2	Ship loss	Action costs	Lives lost	c_D
d_1^0 (nothing)	$S = 1$	d_2^0 (nothing)	1	0 + 0	0 + 4	15.16
d_1^0 (nothing)	$S = 1$	d_2^1 (pay)	0	0 + 2.3M	0 + 0	2.3
d_1^0 (nothing)	$S = 1$	d_2^2 (Navy)	0	0 + 0.2M	0 + 2	4.28
d_1^0 (nothing)	$S = 0$		0	0	0	0
d_1^1 (man)	$S = 1$	d_2^0 (nothing)	1	0.05M + 0	1 + 4	17.25
d_1^1 (man)	$S = 1$	d_2^1 (pay)	0	0.05M + 2.3M	1 + 0	4.39
d_1^1 (man)	$S = 1$	d_2^2 (Navy)	0	0.05M + 0.2M	1 + 2	6.37
d_1^1 (man)	$S = 0$		0	0.05M	0	0.05
d_1^2 (team)	$S = 1$	d_2^0 (nothing)	1	0.15M + 0	2 + 4	19.39
d_1^2 (team)	$S = 1$	d_2^1 (pay)	0	0.15M + 2.3M	2 + 0	6.53
d_1^2 (team)	$S = 1$	d_2^2 (Navy)	0	0.15M + 0.2M	2 + 2	8.51
d_1^2 (team)	$S = 0$		0	0.15M	0	0.15
d_1^3 (alternative route)			0	0.5M	0	0.5

We shall assume that the Defender is constant risk averse with respect to monetary costs. Thus, her utility function is (strategically equivalent to) $u_D(c_D) = -\exp(c \times c_D)$, with $c > 0$. We shall study what happens when $c \in \{0.1, 0.4, 1, 2, 5\}$ as a way to perform sensitivity analysis.

Based on information from Carney et al. (2009), we shall assume that the Defender's beliefs about an attack being successful conditional on no initial defensive action taken would be $p_D(S = 1|a^1, d_1^0) = 0.40$. We shall also assume that

- $p_D(S = 1|a^1, d_1^1) = 0.10$, for the case in which she uses private protection with an armed person, and
- $p_D(S = 1|a^1, d_1^2) = 0.05$, for the case in which she uses private protection with two armed persons,

and we shall check sensitivity with respect to such assessments making them smaller (0.05 and 0.025, respectively) and higher (0.2 and 0.1, respectively)

modelling the Defender's Beliefs over the Attacker's Actions We describe now how the Defender may estimate the probability of being attacked, given her implemented initial defence. Carney et al. (2009) suggest that the probability of being attacked is 0.005 based on historical data on piracy in the coast of Somalia. However, this estimate does not take into account that some ships may be more desirable, in terms of obtaining a bigger ransom, than others for the pirates who typically

use observers and informers to decide upon their targets. Our objective is to estimate a predictive probability of attack $p_D(A = a^1|d_1)$ for the type of ship owned by the Defender, conditional on each possible initial protective defence $d_1 \in \mathcal{D}_1 \setminus \{d_1^3\}$ taken. Instead of estimating these probabilities based on data, as in Carney et al. (2009), which corresponds to a 0-level analysis, we do that based on a 1-level analysis, see Banks et al. (2011) and the discussion by Kadane (2011).

To do so, we assume the Attacker behaves as an expected utility maximiser and derive the Defender's uncertainty about the Attacker's decision from her uncertainty about the Attacker's probabilities and utilities. Thus, the Defender must analyse the decision problem faced by the Attacker from her perspective, as shown in Figure 23. Note that the set of alternatives for the Attacker has been expanded to include alternatives $a^i \in \mathcal{A}$, for $i = 2, \ldots, n$, representing the pirates option to attack other ships that are not owned by our Defender. We have also added new chance nodes D_2 at the end of the tree paths starting at a^i, representing the response of ships $i = 2, \ldots, n$ to an eventual kidnapping, which are considered uncertainties from the perspective of the Attacker. This analysis of the pirates decision must lead to the probabilistic assessment of the perceived pirates' preferences (the uncertainty of the Defender over the Attacker's preferences, modelled through a random variable $U_A(a, s, d_2)$, where now $a \in \mathcal{A} = \{a^0, a^1, \ldots, a^n\}$) and beliefs (the uncertainty of the Defender over the Attacker's beliefs, modelled through the random variables $P_A(S = 1|a^1, d_1)$ and $P_A(D_2|d_1, a^1, S = 1)$ as well as $P_A(S = 1|a^i)$ and $P_A(D_2|a^i, S = 1)$ for $i = 2, \ldots, n$). For simplicity, we shall assume that the n ships are of similar value and features, but see our comments below.

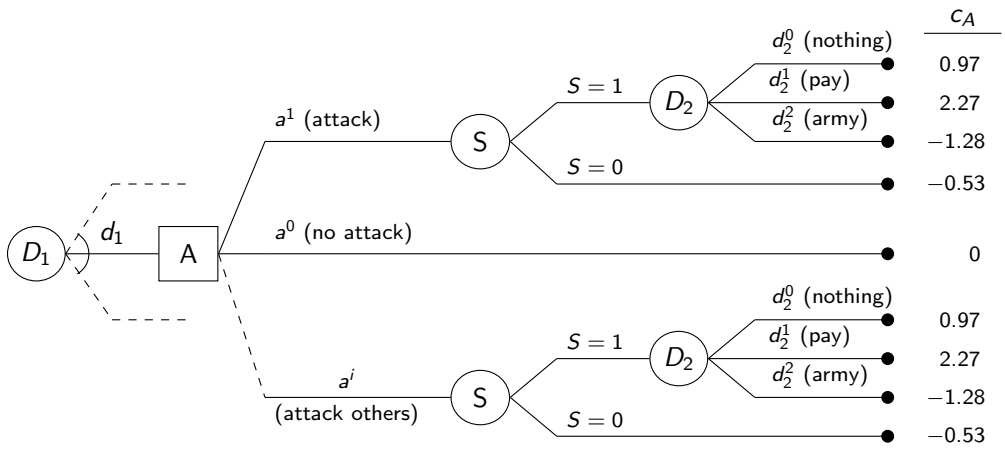


Figure 23: Decision tree representing the perceived decision problem of the Somali pirates

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

- Whether they keep the ship or not.
- The amount of money earned.
- The number of pirates' lives lost.

As described in Carney et al. (2009), the estimated average cost of an attack operation is around 30,000 euros (0.03M euros). The eventual benefits if the Defender pays the ransom are the above mentioned 2.3M euros. As human lives are concerned, we shall assume that two pirates are dead if the attack is repelled and, if successful, no pirates' lives are lost in the attack. However, if the Defender responds by sending the Navy, we shall assume that five pirates will be killed. Again, these numbers

(ransom, lives lost and, to a lesser extent, operational costs) would be affected by uncertainty, but we shall neglect it

If the pirates keep the ship, it will not have the same monetary value as for the Defender. They may use its machinery or its technological instruments, or they could use it as a mothership. We shall assess its economic value for the pirates as 1M euros. We shall assume that they put a value equivalent of 0.25M euros to a pirate's life. Table 10 summarises the consequences for the Pirates of various attack scenarios, including the aggregate monetary equivalent c_A in the last column.

Table 10: Consequences for pirates of various tree paths of their decision problem, $i = 1, \dots, n$.

A	S	D_2	Ship kept	Profit	Lives lost	c_A
a^0 (no attack)			0	0	0	0
a^i (attack)	$S = 1$	d_2^0 (nothing)	1	-0.03M	0	0.97M
a^i (attack)	$S = 1$	d_2^1 (pay rescue)	0	2.27M	0	2.27M
a^i (attack)	$S = 1$	d_2^2 (Navy sent)	0	-0.03M	5	-1.28M
a^i (attack)	$S = 0$		0	-0.03M	2	-0.53M

As stated above, we have assumed that, for the pirates, there are no differences between the consequences of attacking our Defender's ship (a^1) and those from attacking other ships ($a^i, i = 2, \dots, n$), essentially implying that the n ships are of a similar type.

At a qualitative level, the Defender thinks that the pirates are risk seeking over profits. Specifically, she assumes they are constant risk seeking. Therefore, she uses a utility function (strategically equivalent to) $u_A(c_A) = \exp(c \cdot c_A)$, with $c > 0$, to model the pirates' preferences and risk attitudes. However, she is not sure about which c determines the pirates's utility function, but she thinks that $c \sim \mathcal{U}(0, 20)$. This uncertainty over c induces uncertainty over u_A to provide U_A.

As the pirates most likely have access to the same information as the Defender, she assesses the following probabilities for the pirates' beliefs over an attack on her ship being successful, conditional on her initial defence move:

- $P_A(S = 1|a^1, d_1^0) \sim \mathcal{B}e(40, 60)$, for no defensive action taken,
- $P_A(S = 1|a^1, d_1^1) \sim \mathcal{B}e(10, 90)$, for private protection with an armed person, and
- $P_A(S = 1|a^1, d_1^2) \sim \mathcal{B}e(50, 950)$, for private protection with a team of two armed persons.

Note that the expected values of these distributions correspond with the assessed probabilistic beliefs of the Defender on the same uncertainty. Likewise, the Defender assesses that the probabilities representing the pirates' beliefs of a successful attack on ships $i = 2, \dots, n$, which we assumed are of the same class than the Defender's ship, are:

- $P_A(S = 1|a^i) \sim \frac{1}{3}\,\mathcal{B}e(40, 60) + \frac{1}{3}\,\mathcal{B}e(10, 90) + \frac{1}{3}\,\mathcal{B}e(50, 950)$, $i = 2, \dots, n$, acknowledging our lack of information about the defence actions undertaken by other ships and, therefore, about their vulnerability levels. Note that we assume these defensive actions are observed by the pirates, but not by the Defender.

Now, the Defender assesses how the pirates think she will respond to a successful attack. Specifically, she thinks that the pirates expect her to respond along the same lines of the defence chosen by her at the first stage. Thus, a tough deterring defence at her first move is expected to produce an eventual response of similar harshness. Therefore, the Defender assesses the following Dirichlet distributions over d_2^0 (doing nothing), d_2^1 (pay), and d_2^2 (Navy) $\in \mathcal{D}_2$, representing her beliefs on the Attacker's probabilities p_A:

- $P_A(D_2|d_1^0, A = a^1, S = 1) \sim Dir(1,1,1)$: If $d_1 = d_1^0$ (doing nothing) and the ship is hijacked, any response in this case is perceived equally likely by the Attacker.
- $P_A(D_2|d_1^1, A = a^1, S = 1) \sim Dir(0.1,4,6)$: If $d_1 = d_1^1$ (protect with an armed man) and the ship is hijacked, it is perceived that the Attacker expects the Defender to respond doing something, with sending the Navy more likely than paying the ransom.
- $P_A(D_2|d_1^2, A = a^1, S = 1) \sim Dir(0.1,1,10)$: If $d_1 = d_1^2$ (protect with an armed team) and the ship is hijacked, it is perceived that it would be even more likely for the Attacker to believe that the Defender will respond sending the Navy.

Finally, the Defender assesses that

- $P_A(D_2|A = a^i, S = 1) \sim \frac{1}{3}\ Dir(1,1,1) + \frac{1}{3}\ Dir(0.1,4,6) + \frac{1}{3}\ Dir(0.1,1,10)$, for $i = 2,\dots,n$, suggesting our lack of information about the other ships' defensive type and correspondingly their responses. Note that we are acknowledging the Defender's uncertainty about the type of defensive actions taken by these other ships and observed by the pirates.

Based on her above assessments, the Defender may solve the perceived pirates' decision problem using backward induction over the decision tree in Figure 23, propagating the uncertainty of her assessed random preferences and beliefs (U_A, P_A) of the Attacker as follows:

- Compute the random expected utilities associated with the pirates choosing a^1 conditional on each of her initial protective defences $d_1 \in \mathcal{D}_1 \setminus \{d_1^3\}$

$$\Psi_A(d_1, a^1) = P_A(S = 1|d_1, a^1)\left[\sum_{d_2 \in \mathcal{D}_2} U_A(a^1, S = 1, d_2)\ P_A(D_2 = d_2|d_1, a^1, S = 1)\right] + P_A(S = 0|d_1, a^1)\ U_A(a^1, S = 0).$$

- Compute the random expected utilities associated with the pirates choosing a^i for $i = 2,\dots,n$

$$\Psi_A(a^i) = P_A(S = 1|a^i)\left[\sum_{d_2 \in \mathcal{D}_2} U_A(a^i, S = 1, d_2)\ P_A(D_2 = d_2|a^i, S = 1)\right] + P_A(S = 0|a^i)\ U_A(a^i, S = 0).$$

- Compute the Defender's predictive probabilities of being attacked $(A = a^1)$ conditional on each of her initial defences $d_1 \in \mathcal{D}_1 \setminus \{d_1^3\}$

$$p_D(A = a^1|d_1) = \Pr\big(\Psi_A(d_1, a^1) > \max\{U_A(a^0),\ \Psi_A(a^2),\dots,\Psi_A(a^n)\}\big).$$

These probabilities can be approximated by Monte Carlo simulation by drawing a sample $\{(u_A^k, p_A^k)\}_{k=1}^N \sim (U_A, P_A)$ from the pirates' random utilities and probabilities assessed by the Defender and solving for each draw the pirates' decision problem as before. This generates a sample of when $a_k^*(d_1) = a^1$ is the optimal decision for the pirates, and then we approximate $p_D(A = a^1|d_1)$ by

$$\frac{\#\big\{1 \le k \le N : \psi_A^k(d_1, a^1) > \max\{u_A^k(a^0),\ \psi_A^k(a^2),\dots,\psi_A^k(a^n)\}\big\}}{N}.$$

For illustrative purposes, let us assume that $n = 9$: there will be eight other ships (of similar class) exposed to the risk of being seized by the pirates at the time period in which the Defender's ship sails through the Gulf of Aden. Based on 50,000 Monte Carlo iterations, we get the following estimates for the probability of the Defender's ship being attacked, given that she chooses as initial defence action $d_1 \in \mathcal{D}_1 \setminus \{d_1^3\}$

- $\hat{p}_D(A = a^1|d_1^0) = 0.30332$, when the Defender does not take any protective action initially,
- $\hat{p}_D(A = a^1|d_1^1) = 0.02560$, when she uses private protection with an armed person, and
- $\hat{p}_D(A = a^1|d_1^2) = 0.00004$, when she uses private protection with a team of two armed persons.

Note that the probability of attacking the Defender's ship gets smaller if it is protected with an armed guard and even smaller with an armed team. Also these conditional attack probabilities would decrease as n gets bigger, as can be seen in Table 11. We could also analyse the impact of different vulnerabilities among ships if we elicit different $P_A(S = 1|a^i)$ for each type of ship, $i = 2, \ldots, n$. But we have assumed that they are all the same in this case.

Table 11: Sensitivity analysis

$p_D(S=1\|a^1,d_1)$			$\hat{p}_D(A=a^1\|d_1)$					
d_1^1	d_1^2	n	d_1^0	d_1^1	d_1^2	c	d_1^*	$d_2^*(d_1^*)$
0.2	0.1	5	0.41010	0.18354	0.00382	0.1 – 1	d_1^2 (team)	d_2^1 (pay)
						2 – 5	d_1^3 (GH route)	
		9	0.27260	0.05780	0.00008	0.1	d_1^1 (man)	d_2^1 (pay)
						0.4 – 1	d_1^2 (team)	d_2^1 (pay)
						2 – 5	d_1^3 (GH route)	
		15	0.18322	0.01622	0.00000	0.1 – 0.4	d_1^1 (man)	d_2^1 (pay)
						1 – 5	d_1^2 (team)	d_2^1 (pay)
		20	0.14230	0.00628	0.00000	0.1 – 1	d_1^1 (man)	d_2^1 (pay)
						2 – 5	d_1^2 (team)	d_2^1 (pay)
0.10	0.05	5	0.46564	0.12166	0.00328	0.1	d_1^1 (man)	d_2^1 (pay)
						0.4 – 1	d_1^2 (team)	d_2^1 (pay)
						2 – 5	d_1^3 (GH route)	
		9	0.30332	0.02560	0.00004	0.1 – 0.4	d_1^1 (man)	d_2^1 (pay)
						1 – 2	d_1^2 (team)	d_2^1 (pay)
						5	d_1^3 (GH route)	
		15	0.19386	0.00392	0.00000	0.1 – 1	d_1^1 (man)	d_2^1 (pay)
						2 – 5	d_1^2 (team)	d_2^1 (pay)
		20	0.14836	0.00098	0.00000	0.1 – 1	d_1^1 (man)	d_2^1 (pay)
						2 – 5	d_1^2 (team)	d_2^1 (pay)
0.05	0.025	5	0.49010	0.09372	0.00374	0.1	d_1^1 (man)	d_2^1 (pay)
						0.4 – 1	d_1^2 (team)	d_2^1 (pay)
						2 – 5	d_1^3 (GH route)	
		9	0.31764	0.01596	0.00002	0.1 – 0.4	d_1^1 (man)	d_2^1 (pay)
						1 – 2	d_1^2 (team)	d_2^1 (pay)
						5	d_1^3 (GH route)	
		15	0.19842	0.00142	0.00000	0.1 – 1	d_1^1 (man)	d_2^1 (pay)
						2 – 5	d_1^2 (team)	d_2^1 (pay)
		20	0.14778	0.00024	0.00000	0.1 – 1	d_1^1 (man)	d_2^1 (pay)
						2 – 5	d_1^2 (team)	d_2^1 (pay)

Finding the Optimal Defence Strategy We now have all the inputs needed to solve the decision problem for the Defender. Given these, the Defender can solve her decision problem working backwards the tree in Figure 22. At decision node D_2, she can compute her maximum utility action conditional on each $d_1 \in \mathcal{D}_1 \setminus \{d_1^3\}$

$$d_2^*(d_1, a^1, S = 1) = \arg\max_{d_2 \in \mathcal{D}_2} u_D(c_D(d_1, S = 1, d_2)).$$

Afterwards, she will obtain at chance node S her expected utilities

$$\psi_D(d_1, a^1) = p_D(S = 1|d_1, a^1)\, u_D(c_D(d_1, S = 1, d_2^*(d_1, a^1, S = 1))) + p_D(S = 0|d_1, a^1)\, u_D(c_D(d_1, S = 0)).$$

At this point, she will use her probabilistic assessments of being attacked conditional on her initial defence moves, $\hat{p}_D(A = a^1|d_1)$, to compute for each $d_1 \in \mathcal{D}_1 \setminus \{d_1^3\}$ her expected utility at chance node A

$$\psi_D(d_1) = \psi_D(d_1, a^1)\, \hat{p}_D(A = a^1|d_1) + u_D(c_D(d_1, S = 0))\, (1 - \hat{p}_D(A = a^1|d_1)).$$

Finally, she can find her maximum expected utility decision at decision node D_1

$$d_1^* = \arg\max_{d_1^i \in \mathcal{D}_1} \psi_D(d_1^i),$$

where $\psi_D(d_1^3) = u_D(c_D(d_1^3))$ is obtained from Table 9. The Defender's best strategy is then to first choose d_1^* at node D_1, and, if the ship is attacked and hijacked, respond by choosing $d_2^*(d_1^*, a^1, S = 1)$ at node D_2.

For each of the considered risk aversion coefficients determining her utility function, we obtain, based on the above estimates of $p_D(A = a^1|d_1)$ for $n = 9$, that the defence strategies of maximum expected utility are:

- $c = 0.1$ and $c = 0.4$: protect with an armed man ($d_1^* = d_1^1$), and if hijacked ($S = 1$), pay the ransom ($d_2^* = d_2^1$).
- $c = 1$ and $c = 2$: protect with a team of two armed men ($d_1^* = d_1^2$), and if hijacked ($S = 1$), pay the ransom ($d_2^* = d_2^1$).
- $c = 5$: avoid the Somali coast by going through the Cape of Good Hope ($d_1^* = d_1^3$).

We see that choosing to *go through the GH Cape* emerge as optimal decision when the risk aversion coefficient of the Defender is $c = 5$, that is when the Defender becomes most risk averse. This suggests that some security measures are required, but if the Defender is too risk averse it is better for her to change the route. The optimal Defender's response action to a hijacking is always paying the ransom. This is possibly because it is the option that allows the Defender to keep the ship and minimise the lives lost. Clearly, this neglects the political implications of this action, but recall that we are dealing with this problem from the ship owner perspective. One possibility to acknowledge such fact would be to add some extra cost if the ransom is actually paid, reflecting the negative political implication associated with it.

Finally, we show in Table 11 the maximum expected utility defence and estimated attack probabilities for several values of n and $p_D(S = 1|a^1, d_1)$, for $d_1 = d_1^1, d_1^2$, allowing us to check the sensitivity of the solution with respect to these quantities.

Sequential Defend-Attack with Private Information: protection of critical infrastructures

Consider again the situation for the National Grid case study in WP2. We assume again that the Government (She, the Defender) needs to protect two installations within the National Grid network against a potential terrorist attack. The Defender has a limited amount of defensive resources distributed between both sites. The Attacker knows the total amount of defensive resources. This is common knowledge as it was publicised by the Defender. However, the actual distribution of defensive resources between both sites (v_1 for Site 1, v_2 for Site 2 for each unit of defensive resources, $v_1 + v_2 = 1$) is only known by the Defender.

The Attacker has the capacity of launching an attack against just one of the two sites, and he has announced that he will attack one of the sites with all his available resources. Therefore, the available actions for the Attacker are $a \in \mathcal{A} = \{a_1, a_2\}$ with a_i representing attacking Site i, $i = 1, 2$. The Defender has the option of re-distributing her allocation of defensive resources by moving d of them from one site to another. This move will be observed by the Attacker before deciding which site to attack. The set of alternatives for the Defender is then $\mathcal{D}(v_1) = \{d : v_1 - 1 \leq d \leq v_1\}$, where, for example, $d = 0.5$ means that she will move half of her total defensive resources from Site 1 to Site 2, and $d = -0.5$ that half of her defensive resources will be moved from Site 2 to Site 1. If $v_1 \in [0, 1]$ is the initial distribution of defensive resources between sites, the distribution after her move d will be: $v_1 - d$ for Site 1 and $v_2 + d$ for Site 2.

The probability that an attacked site is destroyed (successful attack) depends on the amount of resources committed to that site by the Defender. The more defensive resources allocated to the site, the lower the probability that the attack will be successful. Specifically, they both share the (commonly known) beliefs that

$$p(S_1 = 1|d, a, v) = \begin{cases} 1 - (v_1 - d), & \text{if } a = a_1, \\ 0, & \text{if } a = a_2, \end{cases} \tag{23}$$

$$p(S_2 = 1|d, a, v) = \begin{cases} 0, & \text{if } a = a_1, \\ 1 - (v_2 + d), & \text{if } a = a_2. \end{cases} \tag{24}$$

Note that as deploying more defensive resources at a site reduces the probability that an attack on that site will be successful, $v = (v_1, v_2)$ can be interpreted as a measure of the sites' vulnerability before the Defender's move: the lower the amount of initial defensive resources allocated to a site, the higher the success probability of an attack on the site, and the higher the need for the Defender to move resources to that site in order to reduce that risk. The Defender keeps the information about the sites' vulnerability v as a secret, and, thus, the Attacker does not know v. However, the Defender thinks the Attacker is capable of learning about her private information v by observing her move d using Bayes' rule as in (20).

The Attacker's and Defender's objectives are commonly known to be maximising the probability of succeeding in his attack (for the Attacker), and minimising this probability (for the Defender). Thus, the utilities for the Defender and the Attacker associated with each outcome are known to be, respectively,

$$u_D(s_1, s_2) = \begin{cases} 1, & \text{if and only if } S_1 = 0 \text{ and } S_2 = 0, \\ 0, & \text{otherwise,} \end{cases} \tag{25}$$

$$u_A(s_1, s_2) = \begin{cases} 1, & \text{if and only if } S_1 = 1 \text{ or } S_2 = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{26}$$

Figure 24 shows coupled influence diagrams representing this decision situation. Node S_i represents the uncertainty associated with the success of an attack carried out against Site i, with $i = 1, 2$. These uncertainties depend on the actions taken by both the Attacker and the Defender, as well as on the initial distribution v of defensive resources secretly allocated by the Defender between both sites.

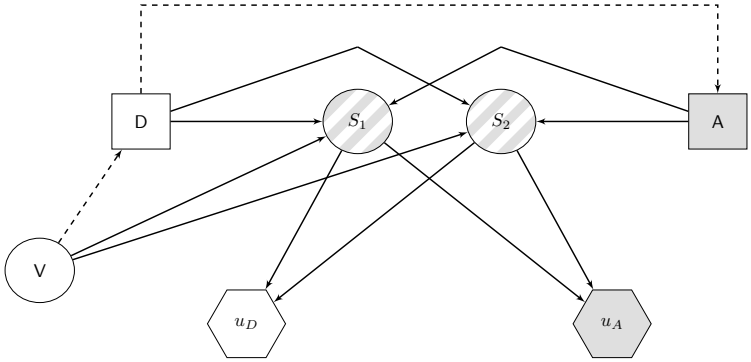
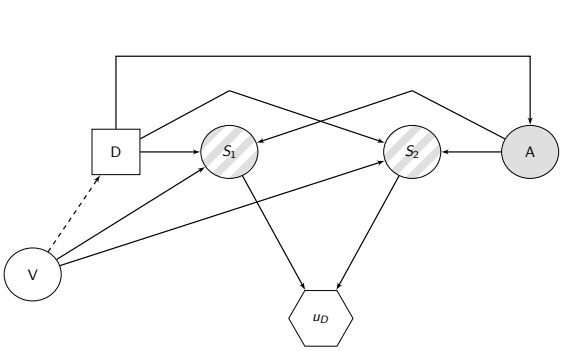


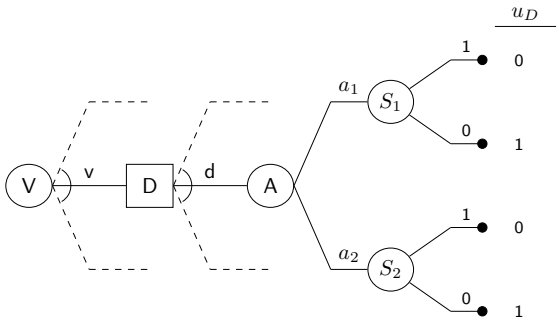
Figure 24: A Sequential Defend-Attack resource allocation problem between two installations on the National Grid network with Defender's private information about the sites' vulnerabilities

To simplify, we have assumed that the Defender's and the Attacker's preferences for the different outcomes are commonly known to be described respectively by (25) and (26), and that both the Defender and the Attacker share the same commonly known beliefs about $S_1|d, a, v$ and $S_2|d, a, v$, described by (23) and (24) respectively. If v were also common knowledge, then the optimal decision for the Defender would be $d = (v_1 - v_2)/2$, thus leaving the same amount of defensive resources in each of both sites after her re-distributing move, with the Attacker indifferent between striking any of the sites.

When v is privately known by the Defender only, the game-theoretic approach based on Bayes-Nash equilibrium assumes that the Attacker's beliefs over v are common knowledge. We deem unrealistic this assumption that the Attacker will reveal his beliefs about v, and solve the problem for the Defender weakening it. Figure 25 shows the influence diagram and the decision tree representing the Defender's decision problem, in which the Attacker's decision is perceived by her as an uncertainty and the value of v is observed by her before making her decision.



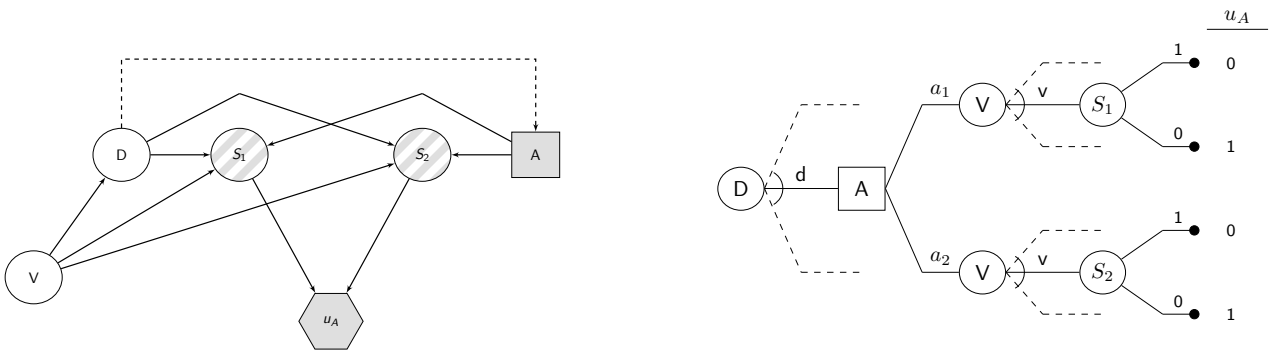
(a)Influence diagram



(b)Decision tree

Figure 25: The Defender's resource re-allocation decision problem

The analysis of her uncertainty about the Attacker's decision requires that she thinks about the decision problem faced by the Attacker, which is shown in Figure 26, where now her decision is modelled as an uncertainty from the Attacker's perspective, and the value of v is unknown to him at the time he makes his decision.



(a)Influence diagram (b)Decision tree

Figure 26: The Defender's analysis of the Attacker's decision on what site to attack

Assume that we are able to obtain from the Defender the following assessments:

- $v = (v_1 = 0.5, v_2 = 1 - v_1 = 0.5)$: The initial allocation of defensive resources between both sites.
- $V = (V_1, V_2 = 1 - V_1)$: The Attacker's assessment of the Defender's private information, as elicited by the Defender. The Defender knows v, but the Attacker does not. The Attacker's (prior) beliefs over the possible values of $V_1 = v_1 \in [0, 1]$ will be represented by $p_A(V_1)$ and will be elicited from the Defender's perspective through $P_A(V_1)$. Based on the information available to her, she believes that $p_A(V_1)$ is a beta distribution $\mathcal{B}e(\alpha, \beta)$ with mean $\mu = \alpha/(\alpha + \beta)$ and precision $\nu = \alpha + \beta$ within the ranges $\mu \in [0.5, 0.8]$ and $\nu \in [10, 30]$, respectively. Based on this, we model $P_A(V_1)$ as a hierarchical beta distribution $\mathcal{B}e(\mu\,\nu, (1 - \mu)\,\nu)$ with $\mu \sim \mathcal{U}(0.5, 0.8)$ and $\nu \sim \mathcal{U}(10, 30)$.
- A heuristic for assessing $p_D(A^1|d)$, the Defender's beliefs about which site the Attacker will attack after observing her move, within the model used by the Defender to represent how the Attacker thinks she will solve her decision problem. To solve the Defender's problem from the Attacker's perspective, he would need to assess $p_D(A^1|d)$. The heuristic model for the Attacker's choice at this level of analysis assumes that the Attacker will choose the site with less defensive resources and that he will not revise his estimate $\hat{v}$ of v after observing her move d. Specifically,

$$A^1 = a_1, \text{ if } \hat{v}_1 - d < 0.5,$$
$$A^1 = a_2, \text{ if } \hat{v}_1 - d > 0.5,$$

  where $\hat{v}_1$ represents the Attacker's estimate of v_1, the initial defensive resources in Site 1. Thus, the Defender ends the hierarchy of recursive decision analysis at this point, disregarding the modelling of further and more complex levels of analysis.

- $\hat{V} = (\hat{V}_1, \hat{V}_2 = 1 - \hat{V}_1)$: The Defender's beliefs of the Attacker's estimate $\hat{v}$ of her private information v, as would be assessed by the Attacker. The heuristic above has reduced the assessment of $p_D(A^1|d)$ to the assessment of $\hat{V}$. We use a triangular distribution on $[0,1]$ with mode ϕ to model the Defender's beliefs about $\hat{v}_1$. Thus, $\hat{V}_1|\phi \sim Tri(min = 0,\ mode = \phi,\ max = 1)$. The Defender also thinks that the Attacker believes that she overestimates what he thinks to be v_1. Specifically, $\phi|\theta, \sigma \sim \mathcal{N}(V_1 + \theta, \sigma)$ truncated on $[0,1]$, with the Defender assessing that $\theta \sim \mathcal{U}(0.1, 0.2)$ and $\sigma \sim \mathcal{U}(0.1, 0.3)$.

We find a solution to the Defender's decision problem as follows.
$P_D(A^1 = a_1|d)$

1. Compute the Defender's beliefs over A^1 based on the proposed heuristic:

$$p_D(A^1 = a_1|d) = \Pr(\hat{V}_1 - d < 0.5|\phi),$$

where $\hat{V}_1|\phi \sim \text{Tri}(0,\ \text{mode} = \phi,\ 1)$. Thus, given ϕ,

$$p_D(A^1 = a_1|d) = \begin{cases} 0, & 0.5 + d \leq 0 \\ (0.5+d)^2/\phi, & 0 \leq 0.5 + d \leq \phi \\ 1 - (0.5-d)^2/(1-\phi), & \phi \leq 0.5 + d \leq 1 \\ 1, & 1 \leq 0.5 + d. \end{cases}$$

2. Given $p_D(A^1|d)$, the Defender can solve her decision problem by working backwards the tree in Figure 25 as follows:

   - At chance nodes S_1 and S_2, compute for each (v, d, a),

$$\begin{aligned} \psi_D(v,d,a) &= \sum_{s_1 \in \{0,1\}} \sum_{s_2 \in \{0,1\}} \left[u_D(s_1, s_2) p(S_1 = s_1, S_2 = s_2|d, a, v) \right] \\ &= p(S_1 = 0|d,a,v)\ p(S_2 = 0|d,a,v) \\ &= \begin{cases} v_1 - d, & a = a_1 \\ v_2 + d, & a = a_2. \end{cases} \end{aligned}$$

   - At chance node A^1, compute for each (v, d),

$$\psi_D(v,d) = \psi_D(v,d,a_1)\ p_D(A^1 = a_1|d) + \psi_D(v,d,a_2)\ \left[1 - p_D(A^1 = a_1|d)\right].$$

   Thus, $\psi_D(v,d)$ is

$$v_2 + d,$$

   if $d \leq -0.5$,

$$(v_1 - d)\ (0.5+d)^2/\phi + (v_2 + d)\ \left[1 - (0.5+d)^2/\phi\right],$$

   if $-0.5 \leq d \leq -0.5 + \phi$,

$$(v_1 - d)\ \left[1 - (0.5-d)^2/(1-\phi)\right] + (v_2 + d)\ (0.5-d)^2/(1-\phi),$$

   if $-0.5 + \phi \leq d \leq 0.5$,

$$v_1 - d,$$

   if $0.5 \leq d$.

- At decision node D, solve for each v,

$$d^*(v) = \arg\max_{d\in[v_1-1,v_1]} \psi_D(v,d)$$

Thus, for each $v_1 \in [0,1]$, the optimal decision for the Defender, $d^*(v_1)$, is

$$-\frac{1}{2} + \frac{2v_1 + \sqrt{4v_1^2 + 6\phi}}{6}, \tag{27}$$

if $v_1 \leq (6\phi - 1)/4$, and

$$\frac{1}{2} + \frac{2(v_1 - 1) - \sqrt{4(v_1 - 1)^2 + 6(1 - \phi)}}{6}, \tag{28}$$

if $v_1 \geq (6\phi - 1)/4$.

From the perspective of the Attacker, $p_D(A^1|d)$ is not known since he does not have access to the value of ϕ used by the Defender in (27). Should the Attacker know ϕ, he would be able to anticipate the Defender's optimal move, $d^*(v)$, for each possible initial allocation v. At this level of the recursive analysis, the Attacker' beliefs about ϕ are propagated to define $p_A(D|v_1)$ from $d^*(v_1)$ in (27)–(28), when $\phi|v_1, \theta, \sigma \sim \mathcal{N}(v_1 + \theta, \sigma)$ truncated on $[0,1]$.

3. Given $p_A(D|v)$ and $p_A(V)$, the Attacker can learn about V from his observation of $D = d$ by computing $p_A(V|d)$ using (20), and solve his decision problem by working backwards the tree in Figure 26 as follows:

- At chance nodes S_1 and S_2, compute for each (d, a, v),

$$\begin{aligned}\psi_A(d,a,v) &= \sum_{s_1\in\{0,1\}}\sum_{s_2\in\{0,1\}} \Big[u_A(s_1,s_2)p(S_1 = s_1, S_2 = s_2|d,a,v)\Big] \\ &= 1 - p(S_1 = 0|d,a,v)\; p(S_2 = 0|d,a,v) \\ &= \begin{cases} p(S_1 = 1|d,a_1,v), & a = a_1 \\ p(S_2 = 1|d,a_2,v), & a = a_2. \end{cases}\end{aligned}$$

- At chance node V, compute for each (d, a),

$$\psi_A(d,a) = \int \psi_A(d,a,v)\; p_A(V = v|d)\; \mathrm{d}v$$

- At decision node A, solve for each d,

$$a^*(d) = \arg\max_{a\in\{a_1,a_2\}} \psi_A(d,a),$$

obtaining that, for each $d \in [-1,1]$,

$$\begin{aligned} a^*(d) &= a_1, \quad \psi_A(d,a_1) > \psi_A(d,a_2) \\ a^*(d) &= a_2, \quad \psi_A(d,a_1) < \psi_A(d,a_2) \end{aligned}$$

where

$$\begin{gathered}\psi_A(d,a_1) > \psi_A(d,a_2) \Leftrightarrow \\ \textstyle\int (1 - 2\,v_1 + 2\,d)\; p_A(V_1 = v_1|d)\; \mathrm{d}v_1 > 0 \Leftrightarrow \\ E_{p_A}(V_1|d) - d < 1/2. \end{gathered} \tag{29}$$

Thus, the optimal decision for the Attacker is

$$a^*(d) = a_1, \text{ if } E_{p_A}(V_1|d) - d < 1/2,$$
$$a^*(d) = a_2, \text{ if } E_{p_A}(V_1|d) - d > 1/2.$$

The Attacker then chooses a_1 (attack Site 1) when, after observing d, he expects less defensive resources in Site 1 than in Site 2, where the Attacker's expectation is computed with respect to his updated beliefs about V: $p_A(V|d)$. Should the Defender know $p_A(V|d)$, she would be able to anticipate the Attacker's choice by computing (29). However, she does not know it as she is uncertain about the Attacker's probabilities $p_A(D|v)$ and $p_A(V)$, which are necessary to compute his $p_A(V|d)$. But we can assess her beliefs $P_A(V) = p_A(V|\mu,\nu)$, $\mu \sim \mathcal{U}(0.5, 0.8)$, $\nu \sim \mathcal{U}(10, 30)$, and $P_A(D|v) = p_A(D|v,\theta,\sigma)$, $\theta \sim \mathcal{U}(0.1, 0.2)$, $\sigma \sim \mathcal{U}(0.1, 0.3)$, to obtain $P_A(V|d)$ as in (22), and, in turn, compute her predictive probability of the Attacker's decision

$$p_D(A = a_1|d) = \mathbb{P}_{\mu,\nu,\theta,\sigma}[E_{p_A}(V_1|d) - d < 1/2].$$

4. We use Monte Carlo simulation to estimate $p_D(A = a_1|d)$

Monte Carlo approximation of $\mathtt{p_D(A = a_1|d)}$

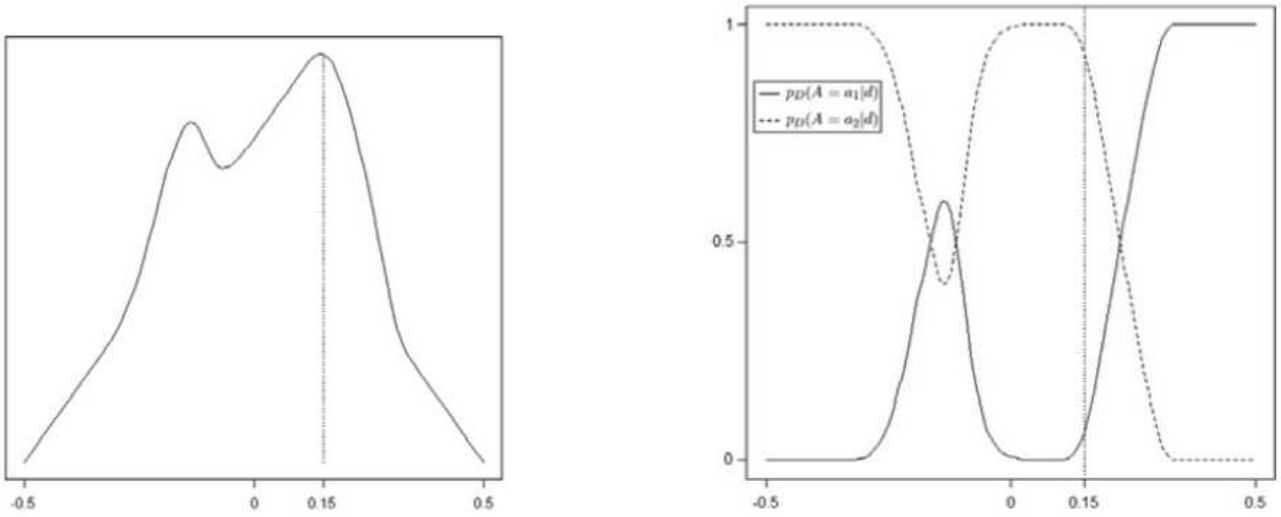
- For $\mathtt{k = 1}$ to $\mathtt{n_k}$
  - Simulate $\mathtt{p^k(V_1)} \sim \mathtt{P_A(V_1)}$
    - $\mu^{\mathtt{k}} \sim \mathcal{U}(0.5, 0.8)$
    - $\nu^{\mathtt{k}} \sim \mathcal{U}(10, 30)$
    - Set $\mathtt{p^k(V_1)} = \mathcal{B}\mathrm{e}(\mu^{\mathtt{k}}\,\nu^{\mathtt{k}}, (1-\mu^{\mathtt{k}})\,\nu^{\mathtt{k}})$
  - Simulate $\mathtt{p^k(D|v_1)} \sim \mathtt{P_A(D|v_1)}$
    - $\theta^{\mathtt{k}} \sim \mathcal{U}(0.1, 0.2)$
    - $\sigma^{\mathtt{k}} \sim \mathcal{U}(0.1, 0.3)$
    - Set $\phi_{\mathtt{k}}|\mathtt{v_1} = \mathcal{N}(\mathtt{v_1} + \theta^{\mathtt{k}}, \sigma^{\mathtt{k}})$ truncated on $[0, 1]$
      - Thus, $\mathtt{p^k(D|v_1)} = \mathbb{P}_{\phi_{\mathtt{k}}|\mathtt{v_1}}(\mathtt{D} = \mathtt{d^*(v_1)})$
  - Simulate $(\mathtt{v_1^i}, \mathtt{d^i})$ from $\mathtt{p^k(V_1, D)} \sim \mathtt{P_A(V_1, D)}$
  - For $\mathtt{i = 1}$ to $\mathtt{n_i}$
    - $\mathtt{v_1^i} \sim \mathtt{p^k(V_1)}$
    - $\phi_{\mathtt{k}}^{\mathtt{i}} \sim \phi_{\mathtt{k}}|\mathtt{V_1} = \mathtt{v_1^i}$
    - $\mathtt{d^i} = \mathtt{d^*(v_1^i)}$, with $\phi = \phi_{\mathtt{k}}^{\mathtt{i}}$ in (27)-(28)
      - Thus, $\mathtt{d^i} \sim \mathtt{p^k(D|V_1 = v_1^i)}$
  - For every $-1 \le \mathtt{d} \le 1$
    - $\{\mathtt{v_j^d} = \mathtt{v_1^i} : (\mathtt{v_1^i}, \mathtt{d^i} = \mathtt{d})\}_{\mathtt{j=1}}^{\mathtt{n_d}} \sim \mathtt{p^k(V_1|d)}$
    - Approximate $\mathtt{E_{p^k}(V_1|d)}$ by $\sum_{\mathtt{j=1}}^{\mathtt{n_d}} \mathtt{v_j^d}/\mathtt{n_d}$
- Approximate $\mathtt{p_D(A = a_1|d)}$ by $\#\{1 \le \mathtt{k} \le \mathtt{n_k} : \mathtt{E_{p^k}(V_1|d)} - \mathtt{d} < 1/2\}/\mathtt{n_k}$.

5. Once $p_D(A|d)$ has been approximated, the Defender can find her (Monte Carlo estimated) maximum expected utility decision $d^*(v)$ by solving the decision tree in Figure 25 using backwards induction:

$$d^* = \arg\max_{d \in [-v_2\,,\,v_1]} (v_1 - d)\, p_D(A = a_1|d) + (v_2 + d)\, p_D(A = a_2|d),$$

with $v = (v_1 = 0.5, v_2 = 0.5)$

We used $n_k = n_i = 5,000$ to run the Monte Carlo simulation and obtained that the Defender's optimal move is $d^* = 0.15$. Thus, given the assessments from the Defender, her maximum expected utility action is to re-allocate 15% of her defensive resources by moving them from Site 1 to Site 2, decreasing her resources in Site 1 from 50% ($v_1 = 0.5$) to 35% ($v_1 - d^*$) and increasing them in Site 2 from 50% ($v_2 = 0.5$) to 65% ($v_2 + d^*$). Figure 27 shows the Defender's (Monte Carlo estimated) expected utilities $\psi_D(d)$ of her feasible moves $-0.5 \leq d \leq 0.5$ as well as her (Monte Carlo estimated) predictive probabilities $p_D(A|d)$ of each site being attacked for each of her feasible d. For $d^* = 0.15$, we have that $p_D(A = a_1|d^*) = 0.06$ and $p_D(A = a_2|d^*) = 0.94$.



(a)$\psi_D(d)$, $-0.5 \leq d \leq 0.5$ (b)$p_D(A|d)$, $-0.5 \leq d \leq 0.5$

Figure 27: Defender's expected utilities and predictive probabilities of site strike

We may see how the solution proposed by the ARA approach is consistent with the Defender's beliefs on the Attacker overestimating her resources initially allocated to Site 1. The move of some defensive resources from Site 1 to Site 2 will reinforce the Attacker's perceived beliefs. Thus, the Defender's expected utility increases by moving resources to Site 2 until her predictive probability of an attack to Site 1 starts increasing sharply, see Figure 27. This allows for the increase of the relative strength of Site 2, the site that a priori is more likely to be attacked, until more resources sent to Site 2 start signalling that Site 1 will end up with less resources. Sending too much defensive resources to Site 2 would allow the Attacker to change his beliefs about which site has less resources and make the Defender vulnerable to an attack on Site 1.

Finally, we also note that the Defender's expected utility function has another local (but not global) maximum which corresponds to $d = -0.15$. This move would allow the Defender to increase the relative strength of Site 1 while at the same time making the Attacker believe that she had less resources in that site. Thus, moving some defensive resources from Site 2 to Site 1 would make the Attacker revise down his (prior) beliefs on the initial amount of defensive resources in Site 1, increasing the Defender's predictive probability of an attack to Site 1 to a point in which for $d = -0.15$, $p_D(A = a_1|d = -0.15) = 0.59$. At this point, the move of more resources to Site 1 would decrease her perceived likelihood of an attack to Site 1, making, in turn, her expected utility to decrease again, see Figure 27.

ANNEX5. Sequential Defend-Attack-Defend for Spacial Settings

We describe now the ARA approach for the model described in Section 4 which essentially may be viewed as a set of ARA models, one for each cell, with models coordinated by resource constraints and value aggregation across each cell for both the defender and the attacker, as specified below. We will illustrate this model with a simple example, related with security issues regarding the installations of a major ground transport operator, see deliverable *D3.2 - Urban public transport requirements*. In this sense, we consider a metro operator (She, the Defender), which deploys several preventive measures against vandalic acts on the metro stations (cells). Under eventual attacks from the hooligans (He, the Attacker), the operator may use additional resources to recover from the attacks.

Defender dynamics

We describe here the dynamics of the metro operator, illustrated with an influence diagram in Figure 28, where the attack node *A* appears, now, as a chance node.

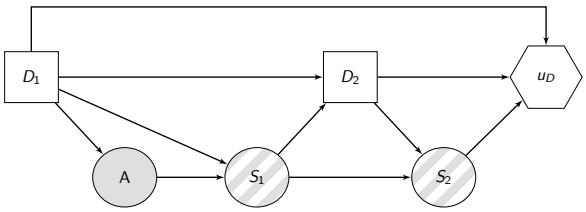


Figure 28: Influence diagram for metro operator dynamics

The operator will:

- Make an initial allocation d_{ij}^1 of defensive resource at every station (i,j) of the metro.
- Face the levels of delinquency a_{ij} at each metro station (i,j), with impacts s_{ij}^1.
- Recover as much as she can, by possibly reallocating resources d_{ij}^2 among stations.
- Face final attack outcome levels s_2^{ij} after the recovery phase.

Finally, they will aggregate the consequences of the delinquency in the metro assets and obtain the corresponding utility.

In order to solve their decision problem, the operator needs to assess the following magnitudes: $p_D(S_1|d^1,a)$, $p_D(S_2|s_1,d^2)$, $u_D(d^1,s_2,d^2,v)$ and $p_D(A|d^1)$. Assuming that they are capable of providing such inputs, the operator would proceed as follows to obtain their optimal resource allocation, by applying standard decision analytic computations based on dynamic programming, see e.g. French and Ríos Insua (2000):

1. Aggregate the consequences at various stations and obtain the utility $u_D(d^1,s_2,d^2,v)$ for every possible scenario (d^1,s_2,d^2,v).

2. At chance node S_2, they compute the expected utilities

$$\psi_D(d^1, s_1, d^2, v) = \sum_{s_2} u_D(d^1, s_2, d^2, v) p_D(s_2|s_1, d^2).$$

3. At decision node D_2, they compute the maximum expected utilities, given the constraints on d^2,

$$\psi_D(d^1, s_1, v) = \max_{d^2} \psi_D(d^1, s_1, d^2, v),$$

and store the optimal recovery allocations $d_2^*(d^1, s_1)$.

4. At chance node S_1, they compute the expected utilities

$$\psi_D(d^1, a, v) = \sum_{s_1} \psi_D(d^1, s_1, v) p_D(s_1|d^1, a).$$

5. At chance node A, they compute

$$\psi_D(d^1, v) = \sum_{a} \psi_D(d^1, a, v) p_D(a|d^1).$$

6. Finally, at decision node D_1, compute, given the constraints on d^1,

$$\psi_D(v) = \max_{d^1} \psi_D(d^1, v),$$

and store the optimal resource allocation deployment $d_1^*(v)$.

We have made the whole evaluation depend on the value v, in case we want to explore solutions for various values. Alternatively, we could fix it and, then, v would disappear from the previous notation. We have assumed that both S_1 and S_2 are discrete, corresponding to discrete levels of success. Note that we may describe the optimization problem for the operator in one shot through the following expression

$$\max_{d^1} \sum_{a} \sum_{s_1} \left[\max_{d^2} \sum_{s_2} u_D(d^1, s_2, d^2, v) p_D(s_2|s_1, d^2) \right] p_D(s_1|d_1, a) p_D(a|d_1).$$

This form would be easily amenable of being treated through the augmented probability simulation approach in Bielza et al. (1999).

The most problematic assessment in the above approach is that of $p_D(A|d^1)$, which describes the beliefs of the Defender about the attacks as a response of its deployed defences d^1 across the metro stations. We provide now an ARA approach to assess such distribution. To do that, we solve the Attacker problem, assuming uncertainty over his assessments and propagating such uncertainty to obtain the desired distribution.

Attacker dynamics

We describe now the dynamics of the Attacker, illustrated in Figure 29 as an influence diagram.

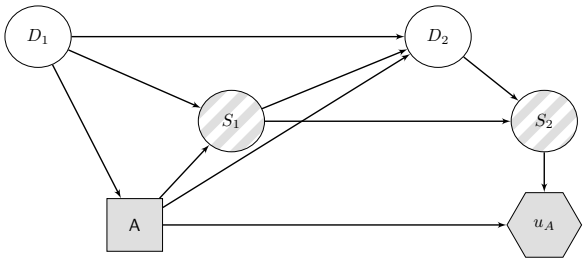


Figure 29: Influence diagram for Attacker dynamics

The Attacker will:

- Observe the defensive resource d_{ij}^1 allocated at each metro station (i, j).
- Undertake attacks a_{ij}, taking into account their constraints, which will produce impacts s_1^{ij} across the network.
- Observe levels of attacks' success s_2^{ij} after the operator tries to recover by reallocating their defensive resources d_{ij}^2.

Finally, it would aggregate the consequences at each station and obtain the corresponding utility.

In order to solve his decision problem as an expected utility maximiser, the Attacker would need to assess $p_A(S_1|d^1, a)$, $p_A(S_2|s_1, d^2)$, $u_A(a, s_2, v)$ and $p_A(D_2|d^1, a, s_1)$. Since we do not have them available, suppose we model our uncertainty about them through probability distributions (i.e., we get random probabilities and utilities) $P_A(S_1|d^1, a)$, $P_A(S_2|s_1, d^2)$, $U_A(a, s_2, v)$ and $P_A(D_2|d^1, a, s_1)$. Then, we may propagate such uncertainty using the standard influence diagram reduction algorithm, see Shachter (1986), and obtain the optimal (random) attack $A^*(d_1, v)$, as a response to each d_1. This provides us with $p_D(A = a|d^1) = \mathbb{P}(A^*(d^1, v) = a)$, assuming the space of attacks is discrete, and, similarly, for the continuous case. The reduction algorithm would run like this, for each d^1:

1. Aggregate the consequences at various stations and apply the random utility $U_A(a, s_2, v)$.
2. At chance node S_2, compute the random expected utilities

$$\Psi_A(a, s_1, d^2, v) = \sum_{s_2} U_A(a, s_2, v) P_A(s_2|s_1, d^2).$$

3. At chance node D_2, compute the random expected utilities

$$\Psi_A(d^1, a, s_1, v) = \sum_{d^2} \Psi_A(a, s_1, d^2, v) P_A(d^2|d^1, a, s_1).$$

4. At chance node S_1, compute the random expected utilities

$$\Psi_A(d^1, a, v) = \sum_{s_1} \Psi_A(d^1, a, s_1, v) P_A(s_1|d^1, a).$$

5. At decision node A, compute the (random) optimal attack as a response to each d^1, taking into account the constraints,

$$A^*(d^1, v) = \arg\max_a \Psi_A(d^1, a, v).$$

Again, we have made the analysis depend on v, in case we are interested in undertaking the analysis for several v values. Otherwise, we would eliminate it from the above notation. Note that the above ID reduction may be written in one shot through

$$A^*(d^1, v) = \arg\max_a \sum_{s_1} \sum_{d^2} \sum_{s_2} U_A(a, s_2, v) P_A(s_2|s_1, d^2) P_A(d^2|d^1, a, s_1) P_A(s_1|d^1, a).$$

This may be undertaken efficiently through the augmented probability simulation approach, as mentioned above.

In order to estimate the required distribution, we may proceed by Monte Carlo sampling. To do it, we may sample N times from

$$F = (P_A(S_1|d^1, a), P_A(S_2|s_1, d^2), U_A(a, s_2, v), P_A(D_2|d^1, a, s_1)),$$

and apply the previous procedure (1)–(5) to compute the optimal attack A_k^* for d_1 at the k-th step of the MC simulation. Then, we can approximate $p_D(A = a|d^1)$ by

$$\text{card}\{A_k^*(d^1, v) = a\}/N.$$

We would proceed in a similar fashion in the continuous case.

Note that, of the four components in F, the first three may be comparatively easily obtained from intelligence. However, the last one may require strategic thinking and some kind of recursion as in Ríos and Ríos Insua (2012), which puts us within the k-level thinking realm, see Stahl and Wilson (1995). Indeed, the approach presented here may be seen as a 1-level thinking model.

The global approach

The previous approaches may be integrated in a two-phase procedure in which we first forecast the attack distribution for each initial defence allocation, and we then find the optimal of these defence allocations.

Initialise parameters

1. For the attacker: For each d_1, repeat for $k = 1, 2, \ldots, N$

At node S_2 and for all feasible (a, s_1, d^2)

Generate $u_A^k(a, s_2, v) \sim U_A(a, s_2, v)$ for all (a, s_2, v)

$p_A^k(S_2^{ij} = 1|s_1^{ij}, d_{ij}^2) \sim P_A(S_2^{ij} = 1|s_1^{ij}, d_{ij}^2)$, for all (i, j) and (s_1, d^2)

Compute $\psi_A^k(a, s_1, d^2, v) = \sum_{s_2} u_A^k(a, s_2, v) \prod_{ij} p_A^k(S_2^{ij} = s_2^{ij}|s_1^{ij}, d_{ij}^2)$

At node D_2 and for all feasible (d^1, a, s_1)

Generate $p_A^k(D_2|d^1, a, s_1) \sim P_A(D_2|d^1, a, s_1)$

Compute $\psi_A^k(d^1, a, s_1, v) = \sum_{d^2} \psi_A^k(a, s_1, d^2, v)\, p_A^k(d^2|d^1, a, s_1)$

At node S_1 and for all feasible (d^1, a)

Generate $p_A^k(S_1 = 1|d^1, a) \sim P_A^k(S_1 = 1|d^1, a)$

Compute $\psi_A^k(d^1, a, v) = \sum_{s_1} \psi_A^k(d^1, a, s_1, v) \prod_{ij} p_A^k(S_1^{ij} = s_1^{ij}|d_{ij}^1, a_{ij})$

At node A and for all feasible d^1

Compute $A_k^*(d^1, v) = \arg\max_a \psi_A^k(d^1, a, v)$

2. For each d^1, approximate $p_D(A = a|d^1)$ through $\#\{1 \leq k \leq N : A_k^*(d^1, v) = a\}/N$, for all a

3. For the Defender

At node S_2, for all feasible (d^1, s_1, d^2)

Compute $\psi_D(d^1, s_1, d^2, v) = \sum_{s_2} u_D(d^1, s_2, d^2, v) \prod_{ij} p_D(s_2^{ij} i|s_1^{ij}, d_{ij}^2)$

At node D_2, for all feasible (d^1, s_1)

Compute $d_2^*(d^1, s_1) = \arg\max_{d^2} \psi_D(d^1, s_1, d^2, v)$

At node S_1, for all feasible (d^1, a)

Compute $\psi_D(d^1, a, v) = \sum_{s_1} \psi_D(d^1, s_1, d_2^*(d^1, s_1), v) \prod_{ij} p_D(s_1^{ij}|d_{ij}^1, a_{ij})]$

At node A, for all feasible d^1

Compute $\psi_D(d^1, v) = \sum_a \psi_D(d^1, a, v)\, p_D(a|d^1)$

At node D_1

Compute $d_1^* = \text{argmax}_{d^1} \psi_D(d^1, v)$

Example: security deployment strategy against vandalic acts on a metro

We illustrate this model with a simple example which will serve us to show some of its computational subtleties. This example is also related with WP3, and the security issues regarding the installations of a major ground transport operator, see deliverable *D3.2 - Urban public transport requirements*.

We consider a small subnetwork within the whole network, composed of three stations as shown in Table 12. The relative value of the assets associated with each station of the subnetwork, evaluated on a scale 0–2, are: $v_1 = 1$, $v_2 = 0.75$, and $v_3 = 2$.

Table 12: Metro subnetwork topology and station's values

1	0.75	2

Suppose that the defensive resources available to the metro operator (the Defender, She) are measured in indivisible units. Specifically, suppose that the metro operator has $R_D^1 = 4$ defensive

units to be distributed before the Attacker has the opportunity to attack. A feasible first-stage resource allocation is described through $d^1 = (d_1^1, d_2^1, d_3^1)$, where $\sum_i d_i^1 \leq 4$, $d_i^1 \geq 0$, and d_i^1 integer for $i = 1, 2, 3$. One possible resource allocation would be $d_1^1 = 1, d_2^1 = 3, d_3^1 = 0$.

Suppose that attackers undertake attacks a_i on metro stations $i = 1, 2, 3$ of the type described on deliverable *D3.2 - Urban public transport requirements*. Assume their attack resources are limited to $R_A = 2$ and, again, assume they can only be distributed in indivisible resource units. Thus, a feasible attack $a = (a_1, a_2, a_3)$ must satisfy that $\sum_i a_i \leq 2$, $a_i \geq 0$, and a_i integer. One possible assignment of attack resources would be $a_1 = 1, a_2 = 0, a_3 = 0$.

The operator can use its resources R_D^2 to recover from the attacks. In this example, we assume that second stage defensive resources will depend on the initial allocation, in that resources can only be moved to neighboring stations, say because only rapid response is reasonable. Therefore, given an initial assignment of resources $d^1 = (d_1^1, d_2^1, d_3^1)$, a feasible allocation $d^2 = (d_1^2, d_2^2, d_3^2)$ must satisfy the constraints:

$$\begin{aligned} \sum_{i=1}^{3} d_i^2 &\leq 4 \\ d_1^2 &\leq d_1^1 + d_2^1 \\ d_2^2 &\leq d_1^1 + d_2^1 + d_3^1 \\ d_3^2 &\leq d_2^1 + d_3^1 \\ d_i^2 &\geq 0,\ i = 1, 2, 3 \\ d_i^2 &\text{ integer.} \end{aligned}$$

Assessments for the metro operator

Assessment of $p_D(S_1|d^1, a)$. $S_1 = (S_1^1, S_1^2, S_1^3)$ represents the initial success/faliure of each possible attack to each station of the subnetwork. To assess the probability that $S_1^i = 1$ at each station $i = 1, 2, 3$, we essentially compare the resources/efforts of both agents allocated to such station. Table 13 shows $p_D(S_1^i = 1|d_i^1, a_i)$, assuming the same success probability at every station i. For example, the position associated to $(d_j^1 = 3, a_j = 2)$ means that two attackers against three security units will lead to a success (in terms of attack) probability of 0.1 (and, therefore, attack failure probability 0.9). We assume independence over various stations.

Table 13: Initial attack success probabilities $p_D(S_1^i = 1|d_i^1, a_i)$, for stations $i = 1, 2, 3$

		a_i		
		0	1	2
d_i^1	0	0	0.85	0. 95
	1	0	0.6	0.75
	2	0	0.3	0.5
	3	0	0.05	0.1
	4	0	0	0.05

Assessment of $p_D(S_2|s_1, d^2)$. We also need to assess $p_D(S_2^i|s_1^i, d_i^2,)$ at every station $i = 1, 2, 3$. Clearly, $p_D(S_2^i = 0|s_1^i = 0, d_i^2) = 1$. For the rest of assessments, we illustrate $p_D(S_2^i = 1|s_1^i = 1, d_i^2)$ in Table 14. We assume the same probabilities at each station i and that these are independent of whatever the amount of damage caused by a successful attack at the first-stage.

Table 14: Final attack success probabilities $p_D(S_2^i = 1|s_1^i, d_i^2)$ after recovery at any station i

		d_i^2				
		0	1	2	3	4
s_1^i	0	0	0	0	0	0
	1	1	0.95	0.8	0.6	0.4

Assessment of $u_D(d^1, s_2, d^2, v)$. For the evaluation of u_D, we assume that the costs of security are already budgeted (the metro operator has already paid them) and, therefore, $u_D(d^1, s_2, d^2, v) = u_D(s_2, v)$. The objective of the metro operator is to minimise the aggregated impact of attacks across the subnetwork stations. The impact of a successful attack (after the operator tries to recover) on a station i is given by a factor ρ_i of the initial value v_i. For simplicity, we assume the same factor across stations: $\rho_i = \rho = 0.1$, for $i = 1, 2, 3$, i.e. the Attacker takes 10% of the value of a station, if successful after the recovery phase. Thus, the value of the i-th station at the end of the game is given by $v_i \times (1 - \rho s_2^i)$. Assuming that the total value of the subnetwork assets is additive, we have that

$$\sum_{i=1}^{3} v_i \, (1 - \rho \, s_2^i).$$

Assume that the operator is (constant) risk averse over the installations value. Since the operator will want to maximise the final aggregated value of the installations, its utility function is

$$u_D(s_2, v) = -\exp\left[-c \sum_i v_i \, (1 - \rho \, s_2^i)\right], c > 0. \tag{30}$$

Since maximising $u_D(s_2, v)$ is equivalent to maximising

$$-\exp\left(c \sum_i v_i \rho \, s_2^i\right), \tag{31}$$

which is a decreasing function on the company loss $\sum_i v_i \rho \, s_2^i$, the operator equivalently would minimise the company loss. Note that (31) represents a (constant) risk averse utility function on the company losses, with the same risk aversion constant c than in (30).

Metro operator assessments about the Attacker decisions

In order to estimate $p_D(A|d^1)$, we must put ourselves in the Attacker's shoes and make the following (uncertain) assessments of the Attacker's beliefs and values from our perspective.

Assessment of $P_A(S_1|d^1, a)$. We assume that $P_A(S_1^i = 1|d_i^1, a_i)$ is similar to $p_D(S_1^i = 1|d_i^1, a_i)$ for stations $i = 1, 2, 3$. To represent our uncertainty about the probabilities used by the Attacker to solve his decision problem, we add some uncertainty by making $P_A(S_1^i = 1|d_i^1, a_i) \sim \beta e(\alpha, \beta)$, so that its mean is $p_D(S_1^i = 1|d_i^1, a_i)$ and its standard deviation is 0.05. For example, if $p_D(S_1^i = 1|d_i^1, a_i) = 0.8$, we easily get $\beta = 1.08$ and $\alpha = 4.32$. We will do this except for the cases in which $p_D(S_1^i = 1|d_i^1, a_i)$ is 0 or 1, for which we assume the Attacker will share these beliefs with the Defender.

Assessment of $P_A(S_2|s_1, d^2)$. As before, for those cases in which $p_D(S_2^i = 1|s_1^i, d_i^2)$ is 0 or 1, we have that $P_A(S_2^i = 1|s_1^i, d_i^2) = p_D(S_2^i = 1|s_1^i, d_i^2)$. Otherwise, we make $P_A(S_2^i = 1|s_1^i, d_i^2) \sim \beta e(\alpha, \beta)$, with mean $p_D(S_2^i = 1|s_1^i, d_i^2)$ and standard deviation 0.05.

Assessment of $P_A(D_2|d^1, a, s_1)$. To simplify matters, we shall actually consider that we know the Attacker probability distribution $p_A(D_2|d^1, a, s_1)$. We assume here that the Attacker expects a proportioned response of the Defender to the type of attack a in each station, taking into account the re-allocation restrictions due to her first allocation d^1 of defensive resources. Thus, we assess that

- If $s_1^i = 0$, then $D_2^i = d_i^1$, unless d_i^1 units are required in other places. This means that the operator shall not move defensive resources, unless necessary. Therefore, $p_A(D_2^i \leq d_i^1 | d_i^1, a_i, s_1^i = 0) = 1$.
- If $s_1^i = 1$, then the operator will try to make $D_2^i \geq a_i$ (moving resources to that station, if possible). We assume proportioned responses in the sense that

$$p_A(D_2^i = a_i + j | d^1, a_i = 1, s_1^i = 1) \propto 0.5^{(j+1)}, \; j \geq 0,$$

  if $a_i + j$ is feasible. In the case this is not possible, D_2^i will be as high as possible within $d_i^1 \leq D_2^i < a_i$.

Given an attack $a = (a_1, a_2, a_3)$, we calculate for all possible reallocations $d^2 = (d_1^2, d_2^2, d_3^2)$ based on the rules above the following

$$p_A(D_2 = d^2 | d^1, a, s_1) \propto \prod_i p_A(D_2^i = d_i^2 | d^1, a_i, s_1^i).$$

and finally, normalise them to add up 1.

Should we wish to add uncertainty around such assessments, we could use a Dirichlet model, with means based on the above assessments, see French and Ríos Insua (2000).

Assessment of $U_A(a, s_2, v)$. We assume that the consequences for the Attacker are related with the value taken from the installations minus the cost of implementing the attacks. In particular, for each station i we have that

$$u_A^i(a_i, s_2^i, v_i) = \begin{cases} -a_i k & \text{if } s_i^2 = 0 \\ \rho v_i - a_i k & \text{if } s_i^2 = 1, \end{cases}$$

where k is the cost of the resources used in an attack to station i. Thus, assuming additivity across the subnetwork stations, the overall value obtained by the Attacker is

$$\sum_{i=1}^{3} (s_i^2 \rho v_i - a_i k).$$

We assume that the Attacker is (constant) risk prone in profits and, therefore, his utility function is strategically equivalent to

$$u_A(a, s_2, v) = \exp\left[c \sum_i (s_i^2 \rho v_i - a_i k)\right], \; c > 0.$$

By assuming, $c \sim U(0, C)$, we account for uncertainty in the utility function, leading to the uncertain $U_A(a, s_2, v)$.

Results

We have solved the example implementing the proposed approach in R. As indicated, we first simulate to estimate $p_D(A|d^1)$ for every feasible d^1 and then calculate the best defensive resource allocations of the operator for both the initial and recovery phases.

The predictive conditional distributions $p_D(A|d^1)$ were estimated through MC simulation and the results are given in Table 15, where blank cells indicate a negligible probability.

Table 15: Predictive distributions over attacks, given first stage allocation of defences

		$A = (a_1, a_2, a_2)$									
		000	001	002	010	011	020	100	101	110	200
d^1	004	0.46			0.54						
	013	0.03						0.71		0.26	
	022		0.03	0.01		0.01		0.48	0.47		
	031		0.25	0.01		0.03		0.01	0.7		
	040		0.22	0.02					0.76		
	103	0.07			0.28			0.24		0.41	
	112	0.13	0.2	0.03	0.01	0.05		0.17	0.3	0.11	
	121		0.38	0.05		0.09			0.48		
	130		0.53			0.01			0.46		
	202	0.07	0.16	0.08	0.26	0.37			0.06		
	211		0.45	0.09		0.3			0.16		
	220		0.65	0.03		0.14			0.18		
	301		0.43			0.52			0.05		
	310		0.71			0.24			0.05		
	400	0.35			0.65						

We have computed the expected utilities of the fifteen feasible defensive allocations at the first stage, and $d_1^* = (0, 4, 0)$ results to be the initial defence allocation with the highest expected utility. The associated contingency plan for recovery from attacks is shown in Table 16.

Although the strategy starts by offering maximum protection to the station with smallest value, this defence is the one that offers more flexibility for response recovery, given the displacement constraints. Moreover, when it is only the final outcome of the attacks after the recovery phase the ones that affect the utility of the defender. We can think of the defender's resources allocated at the first stage as preventive ones aimed at interdicting an attack before it is launched and the resources on the second phase as reactive ones aimed at neutralising an attack that has been successfully initiated before it can cause adverse effects. Thus, the intuition of protecting more the most valuable stations seems false (given the structure, beliefs and preferences in the problem), due to being less flexible. The contingency plan associated with the optimal initial defence does not provide any reallocation defence in case no attack succeeds before the recovery phase (this circumstance is common to any initial allocation). As attacks have a certain level of success, reallocations start to take place, taking advantage of the flexibility of the initial resource allocation.

Clearly, the problem has a combinatorial nature. As an illustration, our small example has:

- 15 possible initial defence allocations: $d^1 = (4, 0, 0), (3, 1, 0), \ldots, (0, 0, 4)$
- 10 possible types of attacks: $a = (0, 0, 0), \ldots, (0, 0, 2)$
- 7 possible attack outcomes: $s_1 = (0, 0, 0), \ldots, (0, 1, 1)$

Table 16: Optimal recovery plan $d_2^*(d_1^*, a, s_1)$, where d_1^* = 040

a	s_1	$d_2^*(d_1^*, a, s_1)$
	000	040
001	001	031
002	001	022
010	010	040
011	001	031
011	011	031
011	010	040
020	010	040
100	100	130
101	001	031
101	101	121
101	100	130
110	010	040
110	100	130
110	110	130
200	100	220

- 15 possible defence recovery reallocations (not all of them feasible given the initial ones): $d^2 = (4, 0, 0), (3, 1, 0), \ldots, (0, 0, 4)$
- 7 possible recovery outcomes: $s_2 = (0, 0, 0), \ldots, (0, 1, 1)$
- The corresponding decision tree, given the various constraints, would have 1902 strategies.

We are, therefore, currently working on approaches that reduce the computational load in realistic size problems, as those being posed in WP1, WP2 and WP3.

ANNEX6. Modelling Adversaries

Traditional statistical risk analysis assumes that the outcome of situations when two or more opponents are in conflict with each other or they are fighting for the same resources is governed by chance rather than the self-interested malicious actions of intelligent actors. Thus, existing decision-theoretic abstractions and tools may be inadequate when there are two or more intelligent opponents who make decisions for which the outcome is uncertain, as it happens in SECONOMICS environments. We have tackled this problem from the perspective of Adversarial Risk Analysis, see Ríos Insua et al. (2009), and one needs some model for the decision making of all the participants. The objective, therefore, is to formalize the analysis of risk from intelligent opponents. We thus argue for decision-theoretic asymmetric prescriptive/descriptive approaches, in which we build a decision theoretic model for one of the participants, which somehow captures the beliefs and preferences of other participants. This approach to games, advocated by Kadane and Larkey (1982), has been favored in the recent literature in counterterrorism and auctions; see e.g. Ríos and Ríos Insua (2009). However, the literature has barely scratched how to proceed on modelling and learning about the preferences and beliefs of the other agents, mainly appealing to heuristics.

Especially relevant could be methods that have been developed in the realm of machine learning in games, which explicitly aim at modelling the utilities of players from observed game traces or from its own experience, see e.g. Rezek et al. (2008). Particularly interesting in this context are approaches to opponent modelling, which aim at capturing the opponent's utility function from its observed behavior, with the goal of predicting its actions and exploiting its weaknesses. Even if a game-theoretically optimal solution to a game is known, a system that has the capability to model its opponent's behavior may obtain a higher reward.

We describe in what follows a description on how to model adversaries and its motivations within a specific security context in relation with hacking activities. This type of modelling may be directly relevant on how we currently perceive the case studies in WP1, and provides also hints on elements concerning cases in WP2 and WP3.

Introduction

There is widespread agreement that the high dependence on the Internet technology is causing a higher security risk to customers, businesses and the society as a whole. A wide variety of business models such as spam campaigns, botnets, identity theft and stealing credit card account information has been flourishing in the last years. The prevalence of this phenomenon led government agencies, international organizations and security vendors to make a concerted effort to develop several security policies against security threats. As a result, various policy tools and strategies have been proposed by researchers see van Eeten and Bauer (2008); van Eeten et al. (2010), and have been enacted by governments (e.g., the U.S. security breach notification laws and data protection laws) and supranational organizations (e.g., the Seoul-Melbourne Anti-Spam Agreement and OECD Security Guidelines). While a range of policy tools and strategies continue to be developed to deal with this issue, most of them tend to be adopted without ascertaining their effectiveness. Moreover, few countermeasures are currently addressing the ever increasing issue of cybercrime markets, see Kanich et al. (2008); Motoyama et al. (2011). We investigate here the effectiveness of

possible policies and strategies focusing mainly on exploit markets in which tools, exploits and means to automatize cyberattacks are traded. Specifically, we use a scenario which features two players: a hacker, who needs to choose between legal activities (i.e., selling exploits to legitimate security vendors) and illegal activities (i.e. writing and selling an exploit kit in a black market), and a defender (i.e., a software vendor and/or a policy-maker) who need to develop policies to mitigate hackers' illegal activities. In the analysis, we use a simple game theoretic model. We believe an exploit market is an appropriate target for the application of game theory, since it can assist in increasing our understanding of the effects of implemented security strategies on the decision making process of a hacker. Our primary objectives are, therefore, to:

1. Form a foundation for an analysis of a hacker's behaviour using game theory; we aim at explaining why illegal hacking behaviour is preferred to lawfully conforming behaviour.
2. Study how hacking technologies affect and are affected by changes in regulation.
3. Investigate possibly effective strategies and policies to be enforced by government agencies and security vendors to deter hackers' malicious activities.

We show that, interestingly, hackers with average skill are prone to participate in malicious cyber-activities. On the other hand, highly skilled hackers are more likely to engage in legitimate activities and disregard criminal ones. We also identify that, of an array of potentially effective strategic alternatives, directly reducing the returns from malicious activities is the only effective strategy for hackers both with a low-medium skill and with a high skill. Furthermore, our results confirm that policy makers should put more effort into reactive strategies than into proactive strategies to mitigate hackers' malicious activities, as indicated by Anderson et al. (2012).

However, we should note that this study is only a first step toward a more complete modelling of cyber-perpetrators' actions and incentives for a variety of decision-making situations. The results presented are not to be intended as definitive, but rather as a starting point for more complete and articulated models for cybercrime. Nevertheless, we think our work provides interesting insights into the cyber-security environment, including noteworthy observations on which defensive actions are effective against strategic cyber-attackers.

Literature Review

While many studies have recognized and addressed the harmful effects of cyber-perpetrators' wrongdoings, few have studied policies and strategies that can mitigate cyber-perpetrators' malicious activities. Accordingly, a growing number of strategies and policies related with cyber-crime have been employed in recent years, without enough consideration of the effects of these on cyber-attackers. Furthermore, most of the studies that suggested measures for preventing security incidents have been concerned about potential victims' prevention activities rather than investigating solutions to mitigate cyber-perpetrators' criminal activities. We first discuss cyber black market economics that initially motivated this study. Then, we explore studies related with the redress of malicious cyber-activities.

Cyber Black Market Economics

A first analysis of black market economics was addressed in Franklin et al. (2007). They analysed the amount of credit card numbers, banking information, and Social Serial Numbers (SSNs) circulating in Internet Relay Chat (IRC)[2] markets for a period of 7 months. According to their estimations the market is worth, overall, about 100 Million USD. Moreover, they show that about 5 percent of the logged data concerns trading of compromised hosts.

However, Herley and Florêncio (2010) are skeptical about the reliability of these results. They show that IRC markets feature all the characteristics of a typical "market for lemons" Akerlof (1970): the vendor has no drawbacks in scamming the buyer because of the absence of a unique-ID and of a reputation system. Moreover, the buyer cannot in any way assess the quality of the good (i.e. the validity of the credit card and the amount of credit available) beforehand. On a folkloristic note, indeed, IRC markets are well known, in the underground community, to be markets for "newbie" and wanna-be scammers, see Herley and Florêncio (2010). There are underground markets other than IRC ones: Motoyama et al. (2011) analysed the private messages exchanged in six underground forums. Most interestingly, their analysis shows that these markets feature the characteristics typical of a regular market: sellers do re-use the same ID, the transactions are moderated, and reputation systems are in place and seem to work properly.

Dealing with criminals and illegal underground activities can be not only difficult and prone to error, but interpretation of experimental results can also be tricky and sometimes misleading, see Herley and Florêncio (2010); Kanich et al. (2011). Moreover, Anderson et al. (2012) showed that, when it comes to new crimes perpetrated through and thanks to the Internet, the investment to defend against them surpasses the gains for the attacker of one order of magnitude: traditional technical countermeasures and strict business-internal policies proved to be extremely expensive and unfruitful. This suggests that more efficient and practical policies and "reactive" practices should be considered when dealing with cybercrime (e.g. increasing the cost of attacks by putting the bad guys in jail).

In regards with these new forms of cybercrime, we are mainly interested in Exploit Kits: these are tools traded in the black markets, see e.g. Symantec (2011), that, once deployed, attack the victim systems that try to connect to them. They are widely used by cybercriminals to, for example, build botnets. These attack techniques are very well explored in a foundational study from Provos et al. (2008).

The economic returns for an attacker have been studied in literature as well. Kanich et al. (2008) analyse the return on investment for three spam campaigns launched by the Storm botnet, and show that the conversion rate (i.e. number of times the victim "clicks" on the spammed link and goes through the trade process to buy the product) are extremely low. This low success rate is taken into consideration by Herley (2012): he observes that attackers pay the cost of "false positives" as well (e.g. users that are accounted as victims but are not). As a result, the cost for an attacker steadily increases as the density of "vulnerable" users decreases. Therefore, to economise the attack process, the attacker needs to choose carefully the population of victims he/she is going to attack. For example, less unsuccessful attacks (false positives) mean less visibility, which means that attackers can minimize the chance of having the police knocking on their door.

[2] IRC used to be a very popular channel for quasi-anonymous instantaneous interactions between users.

Redress of Malicious Cyber Activities

There has been abundant research on individual criminal behaviour. While the literature focused mostly on analyzing a general model of criminal behaviour, Cornish and Clarke (1987) started to study a crime-specific model. They argue that people's choice to participate in criminal activities might be very different according to what specific goal and act are taken into account. More recently, many studies have started to apply the previous models and findings to malicious behavior in cyber-space. Of these studies, the most referred policies for mitigating illegal activities in cyber-space were the legal system. According to Lipton (2010), despite several deficiencies, criminal laws could be the most effective way to deal with many malicious activities in cyber-space. He also points out that criminal laws that deal particularly with malicious cyber-activities should clearly state what constitutes cyber-crimes and avoid relying on an approach from a pre-Internet era.

Recent literature suggests several additional mechanisms that could prevent cyber-perpetrators' wrongdoings. Lipton (2010) and Broadhurst (2006) suggest to use education and training to foster morality which could lead users to behave in a socially acceptable manner by creating an internal sense of guilt and increasing moral satisfaction. Several researchers including Hennig-Thurau and Walsh (2003), Kwok and Gao (2004), Liu et al. (2007) and Wang et al. (2009) argue that monetary and economic rewards are one of the most important mechanisms that promote users' well behaviour. They therefore conclude that the existence of the reward system which allows users to converts their activities into monetary rewards might increase their positive cyber-conduct. In designing a theoretical model, strategies and policies against various malicious cyber activities identified in the literature review are used as variables.

Game Theoretic Model for a Hacker's behaviour

Alongside with our literature review, we base our model on our direct observation of the black markets. With the purpose of getting a more detailed and precise idea of how *blackhat* trades and tools work, we monitored the activities of many black markets for over 6 months. In this work, in particular, we are interested in one of the kinds of tools traded in these markets: Exploit Kits. These tools are usually licensed over a one-year period; prices may vary in between 1,500 USD and 2,500 USD per year. In our model, cyber-attackers act as utility maximizers evaluating various factors including penalties and rewards in perpetrating cyber-crimes. In particular we consider a utility function that allows cyber-offenders to allocate their time to illegal cyber-activities while considering potential benefits and costs resulting from their wrongdoings.

The Basic Model

We consider two types of players in the study: a hacker who can sell an exploit kit which includes various vulnerabilities, or can sell the vulnerabilities to legitimate vendors (e.g., Google's bug bounty program, tipping point initiative or exposing them in a black-hat conference to be hired as a penetration tester) and a defender (e.g., a policy-maker or a security vendor). We regard a hacker as a single decision making entity no matter who is an individual hacker or a hacking group and, throughout, we use he for a hacker. He faces uncertain

situations and needs to make a choice from a set of available actions. Each of these actions has a different probability of yielding an outcome. We assume that a hacker will choose the action that is likely to produce the highest utility from monetary and nonmonetary rewards. Actual outcomes are then assumed to be the result of the interplay between the decisions made by a hacker and a defender.

Since exploit-kit markets consist of players with competing and conflicting interests, we assume that the players make an effort to maximize individual payoffs (i.e., a noncooperative form). In order to investigate the game, we adopt and extend the framework of traditional game theoretic models Dixit et al. (1999) used in the studies of Mesquita and Cohen (1995) and Krebs et al. (2003). Specifically, the game we propose here posits that a hacker's decision is a function of the expected payoffs from the exploit kits and the opportunity cost from committing these malicious activities. In contrast, defenders are assumed to formulate strategies based on what they know about hackers and exploit kit markets to deter hackers from producing, spreading and selling their exploit kits.

Table 17 reports a sum-up of the variables and their respective meaning. First, we consider a hacker. He has total time, T, and is assumed to participate in only two types of activities: malicious activities, such as producing and selling exploit kits in black markets, and normal activities including the development of legitimate software, that are socially acceptable. Therefore, we denote a fraction of a hacker's total time devoted to normal activities as L and a fraction of his total time spent on malicious activities as I (i.e., $L = T - I$).[3]

Table 17: Map of variables and their meaning in the model

Activity type	Variable	Meaning
General	T	hacker's total time
	t	time for detection and neutralization of criminal activity
	p	probability of obtaining maximum benefit from legal activities
	1-p	probability of obtaining only minimum benefit from legal activities
	q	probability of detection of the criminal activity
	1-q	probability of non-detection of the criminal activity
Legal	L	fraction of time the hacker devotes to legal activities
	B	maximum benefit gained from a legal activity
	S	minimum benefit gained from a legal activity
Criminal	I	fraction of time the hacker devotes to criminal activities
	Z	maximum benefit gained from a criminal activity
	C	cost for the hacker in perpetrating criminal activities

We now consider a hacker's expected utility. We assume that, from legitimate activities, a hacker can achieve a maximum benefit B with probability p. In contrast, the hacker can achieve only minimum benefits, S, such that $B > S$, with probability $1-p$. It should be noted that B and S can be increased not only by incrementing monetary rewards from legitimate activities, as suggested by Hennig-Thurau and Walsh (2003), Kwok and Gao (2004) and Liu et al. (2007), but also by fostering morality or the intrinsic motivation to act legitimately as proposed by Lipton (2010) and Broadhurst (2006). The levels of p and $1-p$ are often considered to be influenced by the hacker's personal characteristics, including education

[3]We also assume that there is no cost for the movement between the activities.

level and previous job experience. The hacker's expected utility from legitimate activities, therefore, can be expressed as

$$EU_N = L[pB + (1 - p)S],$$

where $L = T$.

We now take into account the case where a hacker chooses to participate in malicious activities (i.e., writing an exploit kit and selling it in black markets). We denote by q the probability of an exploit kit developed by the hacker being detected and disabled by defenders. The returns to the malicious activities are determined by the benefits gained from the exploit kit, Z, the timing of the detection and disablement of the exploit kit, t, which is normalized to be $[0, 1]$ (i.e., $0 \leq t \leq 1$), and the costs to the hacker, C. Similarly with the benefits from legitimate activities, Z is an important factor that determines a hacker's behaviour as explained by Wang et al. (2009). The costs to the hacker, C, are caused by the detection and disablement of the exploit kit, including the loss of reputation and the penalty from criminal laws considered by Lipton (2010). Three things should be noted here: first, benefits and costs are not restricted to monetary payoffs and losses. These can also take the form of psychological rewards (e.g., self-esteem or self-confidence) and disappointment (e.g., a sense of sinfulness or guilt). Second, unlike the previous criminology research, since it is extremely difficult, if not impossible, to arrest a malicious hacker who develop an exploit kit, see Group IB (2011), we assume that the hacker can still have the returns from his legitimate activities even after an exploit kit developed by him is detected and disabled by defenders. Lastly, unlike the previous literature, we include the time of the detection and disablement, t, in the model since time has a high impact on a hacker's final payoffs. As a result, we define the returns from an exploit kit being detected as $(T - L)(Zt - C) + L[pB + (1 - p)S]$. On the other hand, the probability of a hacker's exploit kit not being detected by defenders can be expressed as $(1 - q)$. In this case, the returns are equal to $(T - L)Z + L[pB + (1 - p)S]$. Putting it all together, a hacker's expected utility of committing malicious activities in line with the ideas of the time allocation can be denoted as

$$EU_M = q\{(T - L)(Zt - C) + L[pB + (1 - p)S]\} + (1 - q)\{(T - L)Z + L[pB + (1 - p)S]\}.$$

As a result, if a hacker puts all of his time on malicious activities, the expected utility becomes $T[q(Zt - C) + (1 - q)Z]$. From these expected utility functions, we can use a game theoretic model to investigate a hacker's decision process.

In the game, a defender moves first, so as to decide whether to enforce security policies and strategies against the activities related with exploit kits. A hacker then should decide whether he will involve in normal activities or malicious activities. If the hacker chooses to participate in malicious activities, the defenders again have to decide whether or not to impose additional security policies and strategies to the hacker's behaviour. To solve this game theoretic model, it is important to identify the equilibria of the game. These show us under which conditions a hacker is expected to choose his involvement between socially acceptable activities and malicious activities. Briefly speaking, a hacker determines whether malicious activities or socially acceptable activities will yield a greater expected utility. If he believes $EU_N \geq EU_M$, then socially acceptable activities will be selected. Otherwise, a hacker will start allocating his time to malicious activities.

A Hacker's Response to Parameter Shifts

In this subsection, we examine the hacker's supply shift of malicious activities in response to changes in strategies. Following Mesquita and Cohen (1995) and Krebs et al. (2003), we manipulate six possible remedies for malicious activities in the model: p, q, S, B, C and Z. In addition to these variables, we also propose manipulating the timing of the detection and disablement (t). This is because defenders (e.g., security vendors) can affect the value of an exploit kit by providing their customers with patches which can disable the exploit kit, or can shorten the timing of the detection of the exploit kit by monitoring exploit markets.

Our simulation adopts an approach used in the study of Krebs et al. (2003). In each simulation analysis, we normalize all the values of the variables to $[0, 1]$. We then fix all of the variables except for the value for the key variable being manipulated: other things being equal, the key variable whose effect is being simulated will increase from 0.05 to 1.00 by 0.05 steps. As pointed out by Krebs et al. (2003), while fixed values used in the previous studies might be appropriate for the purpose of each of them, some of the variables should be adjusted for the purpose of this study. We therefore estimate the values of q, C, Z, B, t and L based on several months of explorations in the exploit markets while we follow the study of Krebs et al. (2003) for the values of p and S at .5 and .3, respectively. As for q, it may be very low as explained in Verizon's 2012 report on data breaches investigations Baker et al. (2012). Moreover, cooperation between law forces is often difficult[4], and the rate at which an attacker can change the address of his exploit kit is way higher than its detection rate by lawful security researchers. As a result, we fix the value of q at 0.1. C may also be low since arrest of a hacker is quite hard and the actual arrest rate is very low, see Baltazar (2011); Herley (2009); Group IB (2011). While cyber-criminals face very severe penalties when caught[5], it is certainly hard to prosecute and apprehend them since they usually stay outside the reach of law enforcement, see van Eeten and Bauer (2008). Given this situation, we fix the value of C at 0.2.

As for Z and B, we consider two cases: In one case, we fix the values of Z at 1.0 and B at 0.8 ($B < Z$). In the other case, we choose the values of Z at 0.8 and B at 1.0 ($Z < B$). This is to compare different types of hackers: a hacker valuing self-esteem and altruism *vs* a hacker valuing sense of superiority and dominance. While indeed regular criminals often act out of need (e.g. they do not have a satisfying social status or they do not have a job), cyber-criminals are seemingly often well-educated and financially stable members of the society, see Group IB (2011). Hackers are indeed well-known to often act for fun or for reputation, see Turgeman-Goldschmidt (2005). Being hackers' motivation not strictly related with their condition in the society, but rather an "emotional state", we feel that we should distinguish between the two cases in which the hacker is *a)* lawful-but-curious and *b)* criminally-minded.

In addition to these values, we also estimate the values for t and L which were not introduced in the previous studies. As previously mentioned, the detection rate of exploits is traditionally very low. Exploit kits continuously change domain, therefore tracking them down and disabling them is a very hard if not impossible task, see Grier et al. (2012). In our observation of exploit markets, we found a number of Exploit Kits that feature 5+ years old

[4] http://nakedsecurity.sophos.com/2012/01/19/koobface-gang-servers-russia-police/, accessed July 05 2012

[5] http://www.darkreading.com/database-security/167901020/security/attabreaches/224200531/index.html, accessed July 05 2012

vulnerabilities at the time of release. We therefore conclude that the average time for the neutralisation of an Exploit Kit is very high: we set t to .9.

As for L, we fix its value at 0.9, meaning that the fraction of time they devote to the criminal activity is low (0.1). This is because most of the hackers have regular jobs, see Group IB (2011), and exploit kits do not require much time or effort to be managed, once their development is complete and the final product marketed.

Results

We now discuss the results of the simulation tests. In the simulation we let the variables p, q, S, Z change from 0.05 to 1 with 0.05 steps. When a variable does not change, it is fixed to the value identified above. We ran simulations for both $Z > B$ and $B > Z$. Unsurprisingly, we found that most of the strategies and policies for reducing malicious activities of a hacker do not work as intended by defenders when the hacker values the benefits from exploit kit development and marketing more than the benefits from legitimate activities ($Z > B$).[6] However, it confirms that lowering the value of Z is the only effective strategy for hindering hackers participating in malicious activities. These results correspond to those from Mesquita and Cohen (1995)'s foundational study from 1995.

The results for the second case ($B > Z$) are reported in Table 18.

Table 18: Simulation Results when $B > Z$. Z is fixed at 0.8 and B is fixed at 1.0.

Changes in key variable	**Model 1:**	**Model 2:**	**Model 3:**	**Model 4:**
	p changes	q changes	S changes	Z changes
0.05				**Succeed**
0.1				**Succeed**
0.15				**Succeed**
0.2				**Succeed**
0.25				**Succeed**
0.3				**Succeed**
0.35				**Succeed**
0.4				**Succeed**
0.45				**Succeed**
0.5				**Succeed**
0.55		**Succeed**	**Succeed**	**Succeed**
0.6		**Succeed**	**Succeed**	**Succeed**
0.65		**Succeed**	**Succeed**	**Succeed**
0.7	**Succeed**	**Succeed**	**Succeed**	
0.75	**Succeed**	**Succeed**	**Succeed**	
0.8	**Succeed**	**Succeed**	**Succeed**	
0.85	**Succeed**	**Succeed**	**Succeed**	
0.9	**Succeed**	**Succeed**	**Succeed**	
0.95	**Succeed**	**Succeed**	**Succeed**	
1	**Succeed**	**Succeed**	**Succeed**	

[6] The table of the results is not presented here, but is available for the interested reader upon request.

The first column indicates the changes of the key variable in increments of 0.05 ranging from 0.05 to 1.00. The columns of each simulation model show the results of the comparison between the expected utilities from normal activities and malicious activities (i.e., $EU_N - EU_M$). That is, these columns display whether the changes in the variable are likely to be effective for reducing malicious activities: **succeed** indicates that the key variable might be effective whereas a blank cell means that the changes in the key variable will not be effective. Note that the models with the changes in the values of C, B and t are eliminated from Table 18 because changes in these variables are not effective for mitigating malicious activities.

Table 18 indicates that, in addition to the strategies for decreasing the value of Z, several other strategies that are not effective in the previous tests become effective for reducing malicious activities if a hacker values the benefits from lawful activities more than the benefits from malicious activities. In detail, Model 1 suggests that increasing the value of p will make normal activities more attractive than malicious activities. Model 1 also indicated that only highly skilled hackers (i.e., hackers with a high probability of getting the maximum benefits from legal activities) are likely to devote their resources to legitimate activities. Model 2 confirms that the increase in the value of q can be an effective strategy for reducing malicious activities while such a scenario is unlikely as explained above. Model 3 also suggests that the reduction of the gap between the minimum and maximum benefits from legitimate activities increases hackers' participation in legitimate activities. Lastly, Model 4 indicates that reducing the value of Z makes malicious cyber activities less attractive.

In sum, the simulation models suggest the following facts: first, the only key variable which can be effective for hackers with either $Z > B$ or $B > Z$ is to reduce the value of Z. However, developing policies and strategies to reduce the value of Z might be difficult. While several researchers have suggested building legitimate "markets for vulnerabilities" for reducing the the value of Z, see Anderson and Moore (2006), these markets are not as well-activated and well-developed as originally intended, as discussed in Miller (2007). Second, while shortening the timing of the detection and disablement of a security threat might be an effective tool for reducing malicious activities, it might do nothing to make hackers reduce their malicious activities. Third, it is identified that developing policies and strategies for hackers with $Z > B$ is more problematic than developing those for hackers with $B > Z$. That is, hackers who value the benefits from legitimate activities more than the benefits from malicious activities are likely to give up malicious activities by changing the values of p, q, S and Z; on the other hand, hackers who regard the benefits from malicious activities higher than the benefits from normal activities are still likely to participate in malicious activities even after the manipulation of the key variables except for Z. This result corresponds to the hackers' profiles reported in other articles and in the news, see Group IB (2011)[7,8]: since they are relatively young, these traffic hackers are more likely to participate in malicious activities motivated by thrill-seeking, feelings of addiction, peer recognition, boredom with the educational system and lack of money, see Turgeman-Goldschmidt (2005); Taylor (1999).

[7] http://www.informationweek.com/security/management/amazoncom-ddos-attacker-busted-in-cyprus/240004073
[8] http://nakedsecurity.sophos.com/koobface/

Discussion

Currently, most of the research on malware threats has been studied from a technical lens, and hence other domains such as economic and political perspectives have been largely ignored. Furthermore, the focus on the research is mostly on the targets of attacks rather than on strategies and policies that can mitigate criminal activities associated with malware. We aimed at filling in this gap in the literature by conducting a study on strategies and policies for reducing malicious cyber-activities from an economic perspective. The results of this study are therefore not to be intended as definitive: while many of our conclusions are, we believe, sound and promising for future research, more complete models are needed to design realistic and effective mitigation strategies.

However, some key insights identified in this work could be interesting pointers for future work. Specifically, our results show that only *very good programmers and professionals* who have high probability of getting maximum payoffs from legitimate activities *are not prone to engage in criminal activities*. Indeed, only when one's likelihood of getting maximum benefits from lawful activities rises we can expect the actor not to play maliciously. This implies that it is not only true that one does not have to be a very good programmer in order to be a malicious hacker, but also true that a *very good programmer is not likely to be a malicious hacker*. Therefore,

1. Good policies that can increase the likelihood of achieving maximum returns from lawful activities would prevent the very good professionals from going rogue.

2. Policies could also be tuned to assure that only low-scale professionals are willing to "join the dark side". Accordingly, this would *decrease the quality of the attack tools* traded in black markets, and possibly their effectiveness in infecting machines and, for example, building botnets.

Another possible strategy would be to increase the minimum benefits for a hacker (S in our model). This would encourage even "average skilled" hackers in joining legal activities rather than criminal ones.

Moreover, despite resulting from a completely different approach, our conclusions are in accordance with those of a recent study from Anderson et al. (2012): "response policies" is where policy makers should put more effort into, and increasing detection rates is an effective strategy to deter cyber-criminals from going rogue. We are, however, very far from achieving that goal: our model predicts a detection rate higher than 50% to be effective; in the current state of cyber-security, this is far from being accomplished. A more plausible strategy is to cleverly increase the minimum benefit for legitimate activities (S) in cooperation with higher detection rates (q): this may turn out to be an effective strategy in real-world scenarios.