SECONOMICS

D8.3: Complete Design of Prototype: Security Problem Modeller

Authors:
Matthew Collinson, David Pym, and Julian Williams
University of Aberdeen

Robert Coles and Raminder Ruprai
National Grid

Review Woohyun Shim and Fabio Massacci *University of Trento*

SEVENTH FRAMEWORK PROGRAMME

Document Number	D8.3
Document Title	Complete Design of Prototype: Security Problem Modeller
Version	1.0
Status	Final
Work Package	WP 8
Deliverable Type	Report
Contractual Date of Delivery	31.07.2013
Actual Date of Delivery	31.07.2013
Responsible Unit	NGRID
Contributors	Authors Detailed Above
Keyword List	CNI, Economic Models, Systems Models
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	Universitï¿œ 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-Straï¿œe 91 44227 Dortmund, Germany http://www.isst.fraunhofer.de/en/	Contact: Prof. Jan Jï¿œrjens jan.juerjens@isst.fraunhofer.de
4	Universidad Rey Juan Carlos	UNIVERSIDAD REY JUAN CARLOS, Calle Tulipï¿œn s/n, 28933, Mï¿œstoles (Madrid), Spain. http://www.urjc.es	Contact: Prof. David Rï¿œos Insua david.rios@urjc.es
5	1495 UNIVERSITY OF ABERDEEN	THE UNIVERSITY COURT OF THE UNIVERSITY OF ABERDEEN, a Scottish charity (No. SC013683) whose principal administrative office is at 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 METROPOLITA DE BARCELONA SA, 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 ANONIMA ESPANOLA, Calle Albarracin, 25, 28037, Madrid, Spain http://es.atos.net/es-es/	Contact: Alicia Garcia 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	SOÚ 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 Mansfeldova 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, Eskizehir, Turkey http://www.anadolu.edu.tr/akademik/yo_svlhvc/	Contact: Nalan Ergun nergun@anadolu.edu.tr

Document Drafting Record

Document change record

Version	Date	Status	Author (Unit)	Description
0.1	10/07/2013	Draft	J. Williams (ABDN)	LaTeX and LyX templates and Sections 3 and 4
0.2	11/07/2013	Draft	M. Collinson	Section 2
0.3	12/07/2013	Draft	D. J. Pym and R. Ruprai	Introduction and formatting. Section 1
0.4	16/07/2013	Draft	J. Williams and R. Ruprai	Corrections and Drafting.
0.5	22/07/2013	Draft	R. Coles and R. Ruprai	Corrections and Drafting.
0.6	30/07/2013	Draft	E. Chiarani	Formatting Check.
1.0	30/07/2013	Final	W. Shim and F. Massacci	Scientific Check.

Deliverable Description

This document outlines a case of the SECONOMICS modelling framework aimed at differentiating different policy problems for critical national infrastructure. The document works through an analysis of differentiating between regulatory types for electricity transmission and builds on previous work documented in Deliverables D2.2, D2.3 and D6.1. For analysis of the underlying tool architecture see deliverable D8.2 for programming details.
D8.3: Complete Design of Prototype: Security Problem Modeller Description of deliverable: Complete Design of Prototype: Security Problem Modeller: D8.3 will describe the complete design of the integration of the Security Problem Modeller developed in WP6. Additionally first prototypes of the tool integration will be implemented.

Related Tasks

T8.2 Design of interfaces between existing tools (ISST, M12 – M24) Based on the above Task 8.1 we design interfaces between existing tools to realize an integrated tools chain to minimize the manual interaction/transformation as far as possible. Depending on the number of non-functional properties /complexity of models, transformations between tools/models have to be defined to realize a seamless integration.

Contents

1. Introduction

The SECONOMICS framework is designed to delineate between various policy approaches for a variety of security problems. This document is designed to demonstrate the technical methodology needed to analyse a security problem from the conceptual issues to the choices needed to construct different tests of competing regulatory approaches. In this document, we focus on Case Study 2 from WP2 and the mechanisms needed to regulate the security of electricity transmission systems and critical national infrastructure (CNI).

The CNI work package, WP2, introduced the National Grid's Electricity Transmission Network. Through looking at the detail of electricity transmission the impacts from security threats could be better understood. Deliverable D2.3, National Grid's Requirements, provided an overview of the security threat and risk landscape to their Electricity Transmission network.

This document assumes prior knowledge of the following deliverables: D2.2, D2.3, D6.1, and D8.2. The objective of the deliverable is to scope the modelling problem and provide an initial analysis of the assumptions needed to construct tests of differing policy régimes.

The document introduces a framework for systematically identifying the regulatory framework (Section 2), identifying and motivating the system specific components (Section 3), motivating an economic model and then calibrating it to the specific case (Sections 4 and 5) of CNI.

2. The Need for Security Policy and Regulation

Electricity transmission is just one form of CNI that a nation may possess. Other parts of electricity delivery, such as a nuclear power stations or key distribution substations, are considered to be CNI. Outside of electricity delivery — and given the potential information or cyber-security impacts if there was a compromise of confidentiality, integrity, or availability of the systems or key data — water treatment and delivery, telephone/broadband infrastructure, transport infrastructure, and more are also be considered to be CNI.

In the UK, many CNI operators/providers are private companies that are often listed on the UK stock exchange. For these private organisations information and cyber security is normally considered a cost of business, albeit essential, as it is not directly linked to revenue. Instead there is a drive to lower costs, one pillar of which is security. Given the potential operational/service impacts of security incidents for CNI providers, government has a responsibility on behalf of society to ensure that the providers protect the essential systems and services that are critical to the nation. From the governmental regulator's perspective, the key concern is how best to ensure that information/cyber-security risks to CNI are appropriately mitigated. Another way of looking at this problem is as follows: How can the CNI operators be incentivized to identify and mitigate the security risks that have the potential to impact the CNI and the services it supports?

2.1 Principles, Risk, and Rules

Principles are the top-level organizing concepts in the regulatory space. Any regulatory framework may be based on the principles that its governing society requires to be supported. Principles are designed to be general statements that define a goal or objective of the organization adhering to the principle. Principles are normally written at a high-level and, as a result can be adhered to in a number of different ways, depending on the type of organization and its level of security posture.

Society's regulators can choose to deliver the required principles using two main tools:

- Risk-based management: in the context of the principles communicated by regulator, the organization actively monitors its operations and observes its threat environment, investing and intervening according to the assessed criticality of risks. In this case, liability for failure to deliver appropriate standards, relative to the stated principles, resides with the organization and may lead to claims for compensation and, ultimately, to loss of permission to operate;
- Rules-based management: in the context of society's desired principles, the regulatory formulates a system of rules with which the organization is required to comply. In this case, failure to comply with stated rules may lead to fines and, ultimately, loss of permission to operate.

A regulatory régime may be wholly risk-base, wholly rules-based, or employ some combination of rules and risk analysis.

In the absence of a guiding set of principles, a regulatory régime can only be based on compliance with rules. Thus, in the absence of both guiding principles and rules, there is no regulation. In the presence of guiding principles, but the absence of rules, regulation is purely risk-based.

We can illustrate the space of possible regulatory régimes diagrammatically, as in Figure 1.

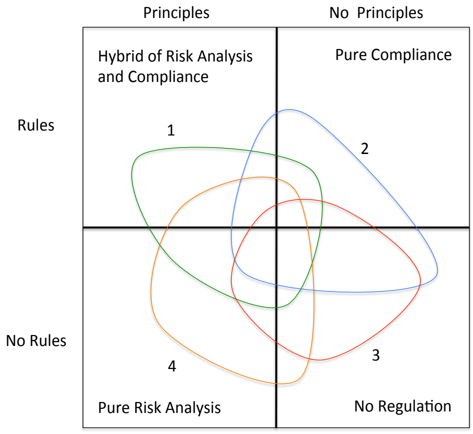

Figure 1: **The Components of a Regulatory Framework**

By way of an illustrative discussion, we consider the curves 1–4 in Figure 1, each representing regulated organizations. The area within a curve represents the space of activities in the sector that is regulated. The parts of the area within the curve that are in each quadrant have the regulatory régime determined by that quadrant. For example, the greater the proportion of the area inscribed by curve that is in the top-left of the diagram, the more of the operations of that organization are regulated by rules.

Consider the organization described by the curve labelled 1. A large proportion of its operations is regulated by the régime described in the top-left of the diagram; that is, a set of principles that is implemented by a set of rules. Similarly, a quite large proportion of its operations is regulated by a set of principles that is implemented by allowing the organization to assess risk and invest accordingly. Some of the organization's operations are regulated by rules that do not derive from current principles. This may arise, for example, from legacy regulatory policies or the accretion of constraints deriving from the interpretation of common laws lying outwith the regulator's remit. Finally, some of the organisation's operations lie in an area where there are no guiding principles and no rules: these operations are essentially unregulated.

The other curves $(2$–$4)$ may be interpreted similarly.

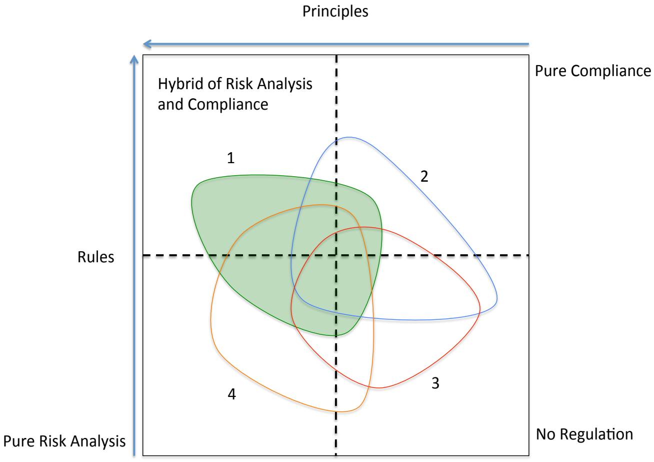

Figure 2: **The Components of a Regulatory Framework, Graded**

In Figure 2, we suggest the possibility that both the presence/absence of rules and the distinction between rules and risk assessments is not necessarily clear cut. For example, principles formulated in very general terms may be too abstract to guide either the formulation of rules or the assessment of risk. Similarly, the methodolgies of risk assessment may be quite tightly structured, drawing upon various forms and sources of rules as appropriate for the situation at hand. As a result, the weighting of the area within the curves with respect to rules, risk, and principles is not uniform. For example, towards the top-left of the region, the operations of the sector are subject to many principles that are implemented by many rules.

Risk-based regulatory régimes tend to have very high-level aims where it would be difficult to audit an organization against those objectives. Hence, the regulator may perform a holistic review of the organization in which information security forms merely one part of the scope of the assessment.

2.2 National Grid's Perspective

Workpackage WP2 is lead by National Grid and serves as the case study example for CNI. National Grid operates in both the US and UK jurisdictions and further details of the operations of National Grid in these countries is described in SECONOMICS Deliverable D2.3.

For National Grid's US operations the North American Electric Reliability Corporation (NERC) provides part of the regulatory oversight. NERC is an independent organisation that provides guidelines and standards for bulk electricity delivery operators (electricity generators and transmitters) in North America and has the legal authority to enforce reliability standards on them. Specifically NERC develops reliability standards that apply to electricity transmission system operators in North America and monitors the status of various elements of the power distribution system (including cyber security assets).

NERC publishes a number of reliability standards and the adherence to these standards is monitored by independent audit. The standard which focuses on information/cyber security as well as the CNI aspects of electricity transmission is the Critical Infrastructure Protection (CIP) reliability standard. More details on the specifics of this regulatory régime are given in Deliverable D2.3 "National Grid Requirements".

In the UK, National Grid holds a licence to transmit electricity that is granted by the Department for Energy and Climate Change (DECC). The headline duty of the licence holder within the Electricity Act of 1989 is stated as follows:

> It shall be the duty of the holder of a licence authorising him to transmit electricity to develop and maintain an efficient, co-ordinated and economical system of electricity transmission ... .

Even though the Electricity Act does not specifically require the transmission licence holder to be 'secure' one could argue that not having the relevant information security controls in place could jeopardize the efficient, co-ordinated and economical system of electricity transmission. National Grid is therefore free to decide how it will secure its information and cyber-operations.

Figure 3 gives a diagrammatic overview of the different regulators, regulatory régimes, and high level requirements to which National Grid is required to adhere in the UK and US.

The UK's risk-based regulatory system has some key advantages and disadvantages. The key advantage of this regulatory system is that it gives a CNI operator the flexibility to identify, assess, and appropriately mitigate security risks as the organization sees fit. The conceptual underpinning behind this is that the CNI operator is best placed to understand its infrastructure and thus best placed to assess and mitigate security risks. This also allows for CNI operators — both in different industries or different parts of the same supply chain — to apply different risk methodologies as they feel are appropriate to their organization. The outcome is better security buy-in by the organization as a whole and a more thorough assessment and mitigation of risks for a better overall security posture.

However, there is a directly opposing disadvantage to this risk-based system. Some organizations may not understand or appreciate the risks to their businesses and so may not

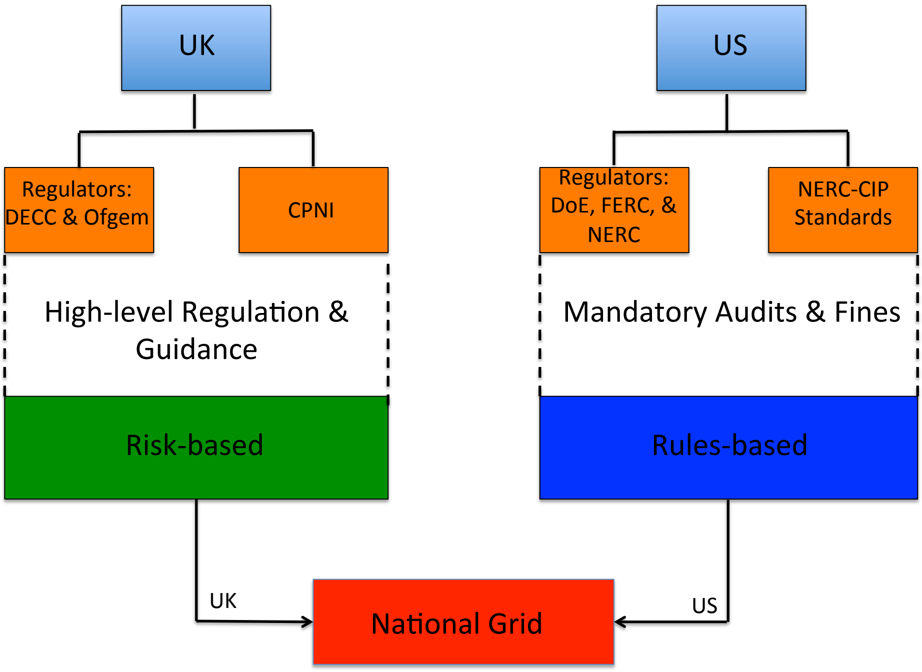

Figure 3: **Regulation of National Grid in the UK and US**

put a sufficient amount of emphasis on security. Historically, this has been the case with many corporate organizations until significant incidents have affected, or had the potential to affect, their operations. CNI operators may choose to accept risks they do not fully understand, so increasing the risk exposure.

In a rules-based regulatory system, there are also both advantages and disadvantages for CNI operators. The requirements or rules within such a regulatory structure sets a minimum level of security across all the operators. Therefore, government, regulators, and citizens can be assured that there is a minimum level of security across all CNI operators. On the other hand, National Grid's electricity transmission business in the US has come across various obstacles, concerns and issues. A number of those have been described below.

- NERC CIP requires that operators of critical assets adhere to their own policies and standards. Thus if an operators standards are set at a higher bar than the NERC CIP standards the operators must adhere to their more stringent requirements. This then presents a potential concern that NERC can fine an operator if it fails to meet its own policies and standards even if the operator is within the minimum standard set out in NERC CIP. This situation provides no incentive for a CNI operator to set their policies or standards above the minimum bar set by NERC CIP.

- The set of requirements or rules set within NERC CIP are created through consensus across the energy industry, therefore the rules created are the lowest common denominator that the majority of the industry can agree on. Achieving formal consensus across the industry takes a significant amount of time, so the rules are not agile to potentially changing risks and therefore could be considered out-of-date.

- To reduce costs of complying with NERC CIP, operations personnel can be utilized to help with compliance work internally as they are subject matter experts in the critical cyber assets. As a result this can create a conflict of interest with employees ‘marking their own homework’. There is no requirement in NERC CIP for a segregation of duties around compliance work and less security mature organizations may have gaps in their security, which are not identified or covered up.

- The cost of compliance to NERC CIP has caused security priority concerns. Previously, there has been a trade-off between meeting the compliance requirements and increasing the organization’s security posture ‘being more secure’. Whilst, the minimum costs of compliance requirements are recoverable through the regulator, costs to go beyond the compliance requirements are often not recoverable. This can make the operation of CNI less profitable and thus draws in less investment.

In summary, the requirement to comply with rules that may or may not contribute to an appropriate overall secure posture, can divert resources away from mitigating the true risks. Instead, pro-active risk-based management may be capable of mitigating threats not anticipated within the formulation of the rules, so leading to a less resilient (see Section 4.1, below) system.

The concepts, methods, and tools of economics provide range of approaches to assessing the right mix of risk- and rules-based regulation for cost-effectively delivering society’s desired security outcomes in CNI. These include ideas from the analysis of principal-agent problems within ecosystems of firms, the analysis of optimal investment strategies in information security, and the theory of public-policy interventions in markets.

National Grid is supportive of deploying these ideas, seeing them all as facets of the broader problem: what type of regulatory structure best incentivizes a CNI operator/owner to be appropriately and justifiably information- and cyber-secure?

Within WP2 a significant amount of work has already been done to understand the detail of the different regulatory structures that National Grid is subject to. In particular, *Deliverable D2.3: National Grid Requirements — Final Version* not only presents the detail of the regulatory structures in the UK and US, but also describes the different control variables in both systems that drive the behaviour of the organization towards the identification and mitigation of risk.

In order to accurately build and calibrate these models we will build upon this work by parametrizing these control variables so that the model can help to differentiate between the regulatory systems. In addition to the information provided in Deliverable D2.3, other areas of National Grid’s security operations must be considered, including

- how security investments are chosen and driven within a risk-based versus a rules-based regulatory system,

- how incidents feed into the analysis and change of security controls in both a rules- and risk-based system,

- the adequacy and relevance of the requirements within a rules-based system,

- speed at which a change in the risks to CNI are filtered into the rules-based system,

- issues with showing compliance to a rules-based system, and
- how the audit process in a rules-based systems feeds back into the security management and controls.

To consider these areas, key information and data will be required from National Grid. These are given below.

- Previous security incidents in National Grid and in the wider energy industry.
- Security incident statistics; that is, the number of incidents broken down by type and time.
- Detailed security investment plan and financials.
- Anecdotal issues, concerns, and past experiences around the requirements within NERC-CIP.
- Anecdotal issues, concerns, and past experiences around the compliance to and audit processes within NERC-CIP.
- Anecdotal issues, concerns, and past experiences around how the UK's price controls are directly affecting National Grid's security investments and operations.

This information will be essential to parametrize and calibrate the economic and system regulatory models.

3. Towards a Model of the Effects of Regulatory Structure

Critical National Infrastructure (CNI) providers are normally subject to some regulatory régime set out by policy makers for the nation or group of nations in question. For brevity, the provider will be referred to as the firm, or F, and the policy-maker as P.

It has been observed that different regulatory régimes lead to a different emphasis of effort on behalf of F. In particular, this applies to the division of efforts put into various security controls and processes. Let us call this the response. Each response will have costs and benefits associated, including a significant term representing risks such as those materialising from security incidents, particularly those that disrupt the core operational service provided by F. For one example, one may contrast a principles-risk-based approach to regulation (as in the UK electricity transmission sector) with a rules-compliance-audit-based approach (such as that operating in the US, although it has multiple providers).

Economic regulation, and policy for regulation, for enterprises of this scale are highly complex matters. A key difficulty comes from the way in which policy, anticipated effects of deviation from policy, and performance measurements set-up complicated feedbacks that are intended to stabilize behaviour at desirable equilibria. The modelling methodology sketched below blends a simple economic framework with a well-understood mathematical control description. Nevertheless, even with many simplifying assumptions the result is far from straightforward.

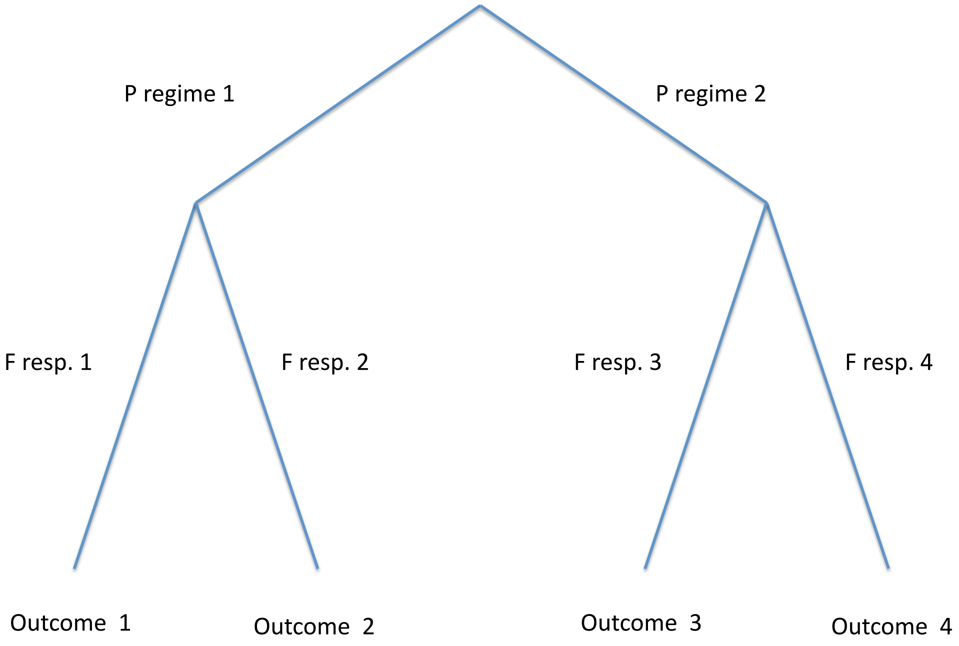

Figure 4: **Stackelberg Policy Game**

A choice of policy régime by P, followed by a response from F determines an outcome, say O; moreover, the firm will have preferences over outcomes, encoded in some loss function $L_F(O)$, and the policy-maker will have preferences over outcomes encoded in some loss function $L_P(O)$. For a given policy choice, the firm's choice will thus be determined by L_F, and therefore the policy choice will also be determined. This kind of anticipation is an important form of feedback that determines behaviour.

In economic terms, this analysis is strongly suggestive that a Stackelberg-style game will be a useful model, see Figure 4 for an example with two response states and two régimes. In order for this to work, an important simplifying assumption for this model will be that there is only one provider. Generalized (or just different) models will be required for other situations.

3.1 Policy régime Choices

What are the choices of policy régime? In other words, what levers does a policy-maker have (with respect to security), that they can delegate to a regulator to work? Below we consider the following: they can set an overall budget; they can put in place a system of objectives (e.g. a few high-level principles, or a complex rule-set; they can choose the mechanism by which performance of the firm is monitored, the relative importance of the performance measures, and the incentive scheme that determines how the firm is rewarded for its performance.

Ignoring the budget constraint for a moment, Figure 5 illustrates the difference between régimes focussed on direct monitoring of compliance with low-level (high-granularity) rule-sets, and those focussed on high-level principles and outcomes: the parameter $w \in [0, 1]$ is set by the P according to its preferences, and determines the degree to which it chooses to reward F for compliance or for operational performance.

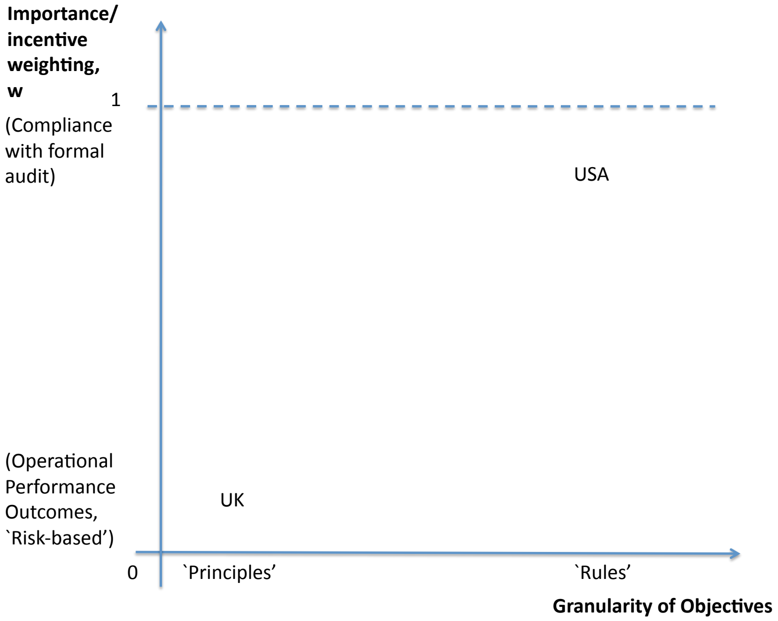

Figure 5: **Differences between régimes**

The firm may respond in a number of ways to the choice made by P. It's choices will also be determined by unpredictable and uncontrollable events, namely the discovery of new security vulnerabilities requiring action. We refer to the portfolio of security choices made (over time) by the firm as the control path, and write it as C_t. Detailed description of this will not be given here, but roughly speaking F has a choice of how to divide its effort between compliance with rules (that have been tailored to fit known current threats and situations), and risk-based mitigation (with greater agility to deal with new threats).

3.2 Conceptual Requirements

A modelling methodology must say how outcomes arize, and how the loss values over those outcomes are calculated. Figure 6 is an example of an idiom for describing the calculation of loss values L_F and L_P. It is something like a block-diagram as used in control theory and engineering, but with some non-standard nuances tailored to this particular setting. Each arrow carries a data structure of some kind: in some cases this is just a simple numerical value, in others it is a tuple, in still others it could be more general. Each box represents a transform that is applied to the input arrows to produce an output arrow. Below, we will not attempt to describe the components of the diagram in complete detail, but only to hint at its overall structure and function.

A particular complexity of modelling regulation of this kind is that, in general, a policy-maker has the capacity to set radically different régimes in place, including the monitoring régimes that evaluate firm performance and reward or determine and limit loss. In the present context, this means that the policy-maker could choose to 're-wire' substantial parts of Figure 6. In order to impose a degree of uniformity upon the present discussion, we limit the rewiring to the setting of the parameter w. In the diagram, this determines the extent to

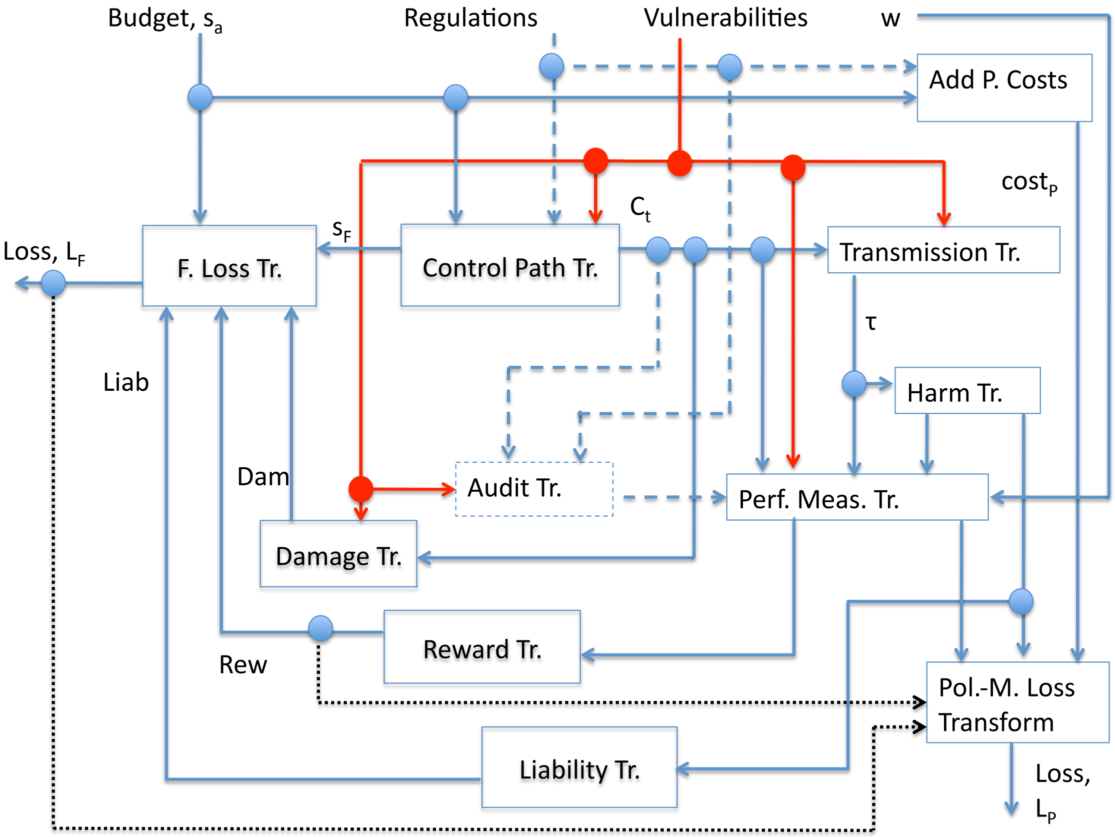

Figure 6: **Diagram of Loss/Preference Calculation. The policy régime inputs into the system via 'Budget s_a', 'Regulations' and w a parameter that determines the incentive structure used by the policy maker.**

which the arrow from the 'Audit Tr.' box is significant, relative to the other arrows into the 'Perf Meas Tr.' box: we can imagine that when $w = 0$, the 'Audit Tr.' and its incoming and outgoing arrows are blanked out of the diagram. Thus a policy régime chosen by P is here a triple consisting of a $budget, s_a$ for security spend allocated to the firm by P, a set of regulations (at some level of granularity as described above), and a choice of weighting w reflecting the importance of compliance evaluated via formal audit.

As noted above, a triple results in a control path, but the way in which this happens is partly through a feedback *not* marked in the diagram: this is the anticipatory Stackelberg feedback mentioned above; the firm will set its control path to minimize its loss.

The control path leads to some transmission path. In the diagram this is just marked τ that is the output of the 'transmission transform' box. It is some measure of the level of provision of the core service. It may be a tuple, rather than just a single value. If the transmission path is poor[1], for example the transmission drops below a certain level, then this will cause some harm to society that should be factored into the policy-maker's loss as

[1] We use the term transmission in the sense of modelling the response of the model to changes in other parts of the model. It is not to be confused with the specific quality of electricity transmission.

an important factor. The ‘harm transform’ box takes care of this, and typically it will encode much information regarding the critical levels of service provision. More generally, P cares about a whole range of performance measures relating to security, as encapsulated by the ‘performance measure transform’. However, there is good reason to suppose that in the CNI setting that harm to society will be a major concern and for this reason it has a separate transform, denoted Pol.-M Loss Transform.

The w input to the performance measure transform determines the degree to which output of Audit (as determined by the ‘Audit transform’ is of significance). The performance measure is used by P to set the reward for F (according to some pre-agreed scheme). The loss function of the firm derives from the reward it gets (including any penalties applied by P), any damage it accrues (from the security incidents), or any liabilities it has arising from security incidents. Finally, P’s loss derives principally from the harm, other performance measures and the costs it bears. These costs include overall harm to society from loss of availability and harm to the firm in terms of loss of reputation and public perception (including financial harm to shareholders).

Simplifications of the above model will often be appropriate: for just one example, in situation where the legal liabilities of F to parties other than P are negligible the liability transform can be omitted.

4. Calibration of Security Models

The preceding section has carefully illustrated the differentiation in risk and rules based systems. In this section, we demonstrate using a game-theoretic model of resilience, the effects of imposing unilateral rules on a purely risk-based system and identify critical tipping points in the risk-generating system.

4.1 Resilience Models with Hidden Risk Component

A common feature of risk assessment models in SCADA and control systems is the ability to determine assets at risk in audits. General economic models of security have considered a continuum of target firms and attackers in a Nash equilibrium with a Stackelberg policy-maker. We can extend this concept to a single firm with N_T employees (or business groups for a greater level of abstraction) with risks driven by N_A antagonists seeking to gain rent from successful attacks of reward R.

When dealing with individuals we now have to explicitly capture the concept of risk aversion. A good summary of risk aversion is found in [1]. Two approaches for risk aversion are generally considered, for one period (where the firm must make a single investment choice with commitment) models a risk premium that is proportional to a measure of dispersion of outcomes is subtracted from the risk neutral expectation to produce a *certainty equivalent* valuation. In multi period models (where firms can adjust their investment either continuously or at future discrete dates) we can translate this risk premium into an *adjusted discount rate*, higher levels of risk aversion more rapidly discount uncertain future revenues and a lower discount on uncertain future losses.

Both the certainty-equivalent and adjusted-discount-rate methods of incorporating risk aversion allow calibration to individual risk preferences. When choosing between various policy frameworks deciding on the variation in risk bearing between individual agents within the firm and the policy maker implementing the policy framework is of paramount concern. Most of the variation in incentives between individual agents and the collective firm is driven by variation in valuation of forward looking risks.

As we look at policy making from a variety of scales (government to firm, firm to employee) we shall use the phrase steward to denote the social coordination action. In the previous sections we have looked at social coordinators as benevolent actors imposing regulation on firms by designing legal structures that align welfare incentives.

We will limit our coverage of welfare incentives to risk reduction and trade-offs with investment. Our specific interest is in delineating between imposed expenditure and expenditure based on forward looking risk analysis. The literature on stewardship is quite varied, see [2] for coverage relevant to information and physical security.

In this section we shall discuss an economic model whereby misalignment of incentives are driven by externalities derived from how risks are generated. We define risk in terms of the variation in the valuation of future expected losses (variation in the discount rate of individuals versus the steward), with costly initial investment. For exposition purposes we will focus on a one period model.

Furthermore, we will consider coordination activities in the narrow sense of directing specific costly investments in security controls, designed to mitigate or eliminate the threat of successful attacks with well defined losses. One aspect of our analysis will focus on mandating investment versus allowing individuals to set risk adjusted targets, this will reflect on advantages and disadvantages of setting precise investment targets through the use of rules.

It is instructive to solve a one-dimensional example of an attack and defence game before solving a more complex problem with potentially hidden actions.

4.2 Motivating A Simple Risk Generating Model

Consider an individual target choosing a level of investment in security over a continuous time horizon. They are faced with the following problem: find the optimal initial investment x (which maybe a vector of choices), with commitment given future losses described by a loss function $L\Psi(\eta, x, t)$, where L is the instant loss function and $\Psi(\eta, x, t)$ is the instantaneous probability of a successful attack. Here η is a measurement of attacking intensity and t is set in continuous time in the range $t_0 < T$.

The individual target solves his decision making by minimising:

$$x^*(\eta) = \arg\min \int_{t_0}^{T} e^{-\beta t} L\Psi\left(\eta, x, t\right) dt + g\left(x\right)$$

where β is a discount rate and $g(x)$ is an investment function, presumed to be a linear aggregation across investment items. We will assume basic regularity conditions on this function, i.e. that $x^*(\eta)$ is unique for given values of $[x] \geq 0$. Where the brackets indicate that x is an element from a vector.

Let us now index the individuals investment choice $x^*(\eta)$ across $i \in \{1, \ldots, N_T\}$ targets, we therefore index the individual targets choices as $x_i^*(\eta_i)$.

For a policy maker observing the whole firm the aggregate investment in security is $\sum_{i=1}^{N_T} x_i^*(\eta_i)$, if they allow all individuals or business groups to decide on their own resource allocation.

$$\left[x_i^P\right]_i^{N_T} = \arg\min \sum_{i=1}^{N_T} \int\limits_{t_0}^{T} e^{-\delta t} L \Psi\left(\eta_i, x_i, t\right) dt + \sum_{i=1}^{N_t} g\left(x_i\right)$$

in this case the policy maker (at the firm level) is choosing their desired optimal allocation based on the discount factor δ assuming that η is set exogenously.

4.3 Incentive Incompatibility in Security Provisioning

Let us assume that ex-ante all targets $i \in \{1, \ldots, N_T\}$ are identical, in this case the optimal policy allocation of x is determined by:

$$x^P(\eta) = \arg\min \int\limits_{t_0}^{T} e^{-\delta t} L \Psi\left(\eta, x, t\right) dt + g\left(x\right)$$

we can see that for cases where $\delta = \beta$, then the allocation x^* is incentive compatible with the allocation x^P as the policy maker and target optimizations are identical.

However, in the case where $\delta \neq \beta$ then we see that the optimal allocation determined by individuals namely x^* will differ, by construction, from that considered to be optimal by the policy maker x^P.

There is a considerable coverage in the contemporary economics literature on the divergence of social and private discount factors. In the attached paper [2] in Section 3 we provide an extended discussion of this phenomenon. An important point to note is that decomposition of discount rates is one of the primary mechanisms for computing the cost sharing of investment for regulated industries and this is also discussed in the attached paper.

Using the diminishing marginal returns to security investment let the risk function be given by the following equation:

$$\Psi\left(\eta, x, t\right) = e^{-\psi x} - e^{-\alpha \eta t - \psi x}$$

where α and ψ are technology parameters that can be calibrated to the specific performance of the system in question. An interpretation of this functions is that it represents the instantaneous probability of a successful attack at time t. The integral with respect to time represents the cumulative exposure to attackers and is most usefully considered in terms of an average across the potential space of attacks.

Two measures can be created from this type of model, first the relative-marginal- effectiveness of defensive expenditure:

$$-\frac{\partial \Psi\left(\eta, x, t\right)}{\partial x} \frac{1}{\Psi\left(\eta, x, t\right)} = \psi$$

and second the inter-temporal relative change in risk,

$$-\frac{\partial \Psi\left(\eta, x, t\right)}{\partial \eta} \frac{1}{\Psi\left(\eta, x, t\right)} = \frac{\alpha t}{1 - e^{\alpha \eta t}}.$$

Note that the variation in the attacker versus defender dynamics in this case. Defensive choices taken at t_0 have a permanent marginal impact of ψ on the level of risk. However, attackers have increasing impact with increasing t, as $T \to \infty$ then the marginal contribution increases linearly with time. However, the value of this contribution is discounted at $e^{\beta t}$, which decays to zero at an exponential rate. We can use this result to derive an approximation for the time horizon T, let T^* be a time horizon accounting for $1 - \lambda$ of the total value of future losses. Then the proportion of present value accounted for in the integral is:

$$1 - \lambda = \int_0^{T^*} \beta^{-1} e^{-\beta t} dt$$

and as such $T^* = -\beta^{-1}\log(\lambda)$, where $\lambda \to 0$. Recalling that

$$\lim_{T\to\infty} \int_t^T \beta^{-1} e^{-\beta t} dt = 1.$$

This allows us to set an upper limit for T, therefore the time horizon T^* is simply a function of the discount rate β. In Figure 7 we plot the minimization problem for an individual firm, group or target, given an exogenous attacking intensity $\eta = 1$, over a range of values for β. In this case $\alpha = 0.1$ and $\psi = 0.05$. In this case the instant probability of a successful attack by a single attacker is just under 10% if no defensive effort is made. With an investment of 2 units of expenditure (per 100 units of loss) then this reduces to 7%, with ten units of expenditure it is reduced to 4% and so on. So this is actually a relatively high risk state on a per annum basis.

Given that the mechanism for increasing risk from the attackers side is $\alpha\eta$, from the defensive point of view, how α and η are decomposed is irrelevant in this part of the derivation. Later we shall show that α being constant for both attackers and defenders and η as the choice variable for attackers does affect the general equilibrium of the attack defence game. Therefore analysis of defensive characteristics maybe analysed in terms of varying α and keeping η as unity.

We see that as β increases the optimal investment point shifts to the left (indicating a lower optimal investment in security) for the individual.

Once we have determined the optimal investment x^* given a set of technology parameters α and ψ for a given attacking intensity η we can explore the solution space. In this case we represent the amortized value of the system such that the total value TV of assets is $TV = \int_0^{T^*} e^{-\beta t} L dt$, therefore L maybe determined from the booked value of assets of the firm. We can construct a counterfactual value for L based on total damages to a firm from successful attacks.

For instance we might determine that for each successful attack the loss L is higher than the total discounted value of assets for instance in the CNI case if punitive reputational damages are incurred that cannot be recovered through an actuarial process (such as private or public insurance provision).

4.4 Calibration to the technology of security and attack

It is instructive to explore the optimal defensive solutions for exogenous attacking intensity, to understand how this type of model maybe calibrated to the information provided in the

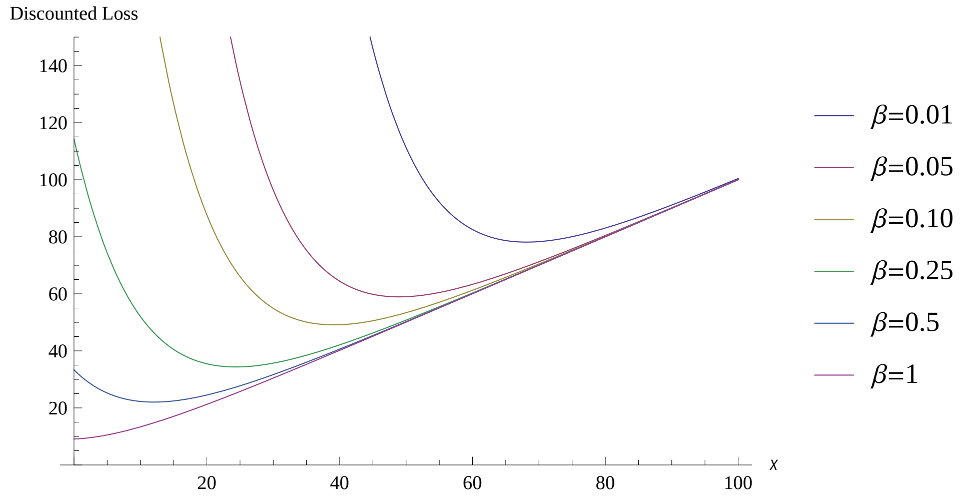

Figure 7: **The individual loss minimization problem, over a variety of discount rates β. As the discount rate increases the choice of allocation x, decreases as future losses are discounted more aggressively. We can interpret the higher discount rate as a high risk appetite for the individual.**

case studies. For this part of the modelling exposition we shall concentrate on calibration in respect of discount rates (time preferences). The usefulness of this part of the work is that discount rates are easily discernible from analysis of investment timing and the amortization of assets. For each parameter in the model, a similar exercise needs to be undertaken, however, we shall demonstrate that time preferences (in terms of return on investment, or losses mitigated) dominate the investment side. In particular variation in the relative valuation of future losses is of predominant importance in the social coordination action.

We have incorporated a single decision variable x for which we need to determine the optimal investment bundle, denoted x^*. In general we have determined x^* as a function of a level of threat denoted by the attacking intensity variable η. For general forms of our model the Nash equilibrium x^N and η^N denote the equilibrium best replies of defensive expenditure versus attacking intensity. Prior to determining x^N and η^N we need to explore the sensitivities of solutions of investment x^* with exogenous levels of attacking intensity η to changes in the technology parameters α and ψ over a range of discount rates.

We can now define x^* in terms of a derivative with respect to the underlying technology parameters α and ψ. All of the plots are displayed in terms of $L^{-1}x^*$, i.e. the investment per unit of asset at risk. We first consider the optimal investment as a function of α the technology of attack. In this case we assume that η the intensity of attack is unity and we shall deal with endogenous attacking intensity in the next section.

From data provided in the case studies, we determine a range of β, the time preference, of the target to be between 0.2 and 1. We fix ψ to be 0.2 and we will see from analysis of the derivative of x^* with respect to ψ that there is convergence across the range of defensive effectiveness that is deemed reasonable. Figure 8 and 9 present respectively the variation in x^* per unit of L for a given α and its derivative.

We can see that defensive expenditure is always increasing with increasing attacking technology. The rate of increase in x^* declines and the speed of decline is proportional to the size of the discount rate (the contour nearest the origin represents the $\beta = 0.2$ the

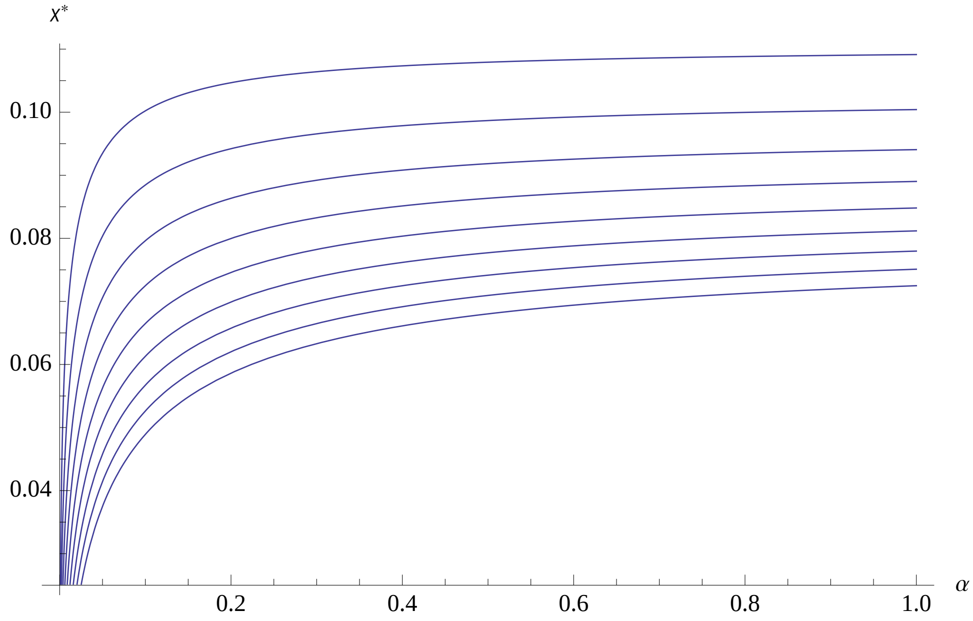

Figure 8: **Variation of $L^{-1}x^*$ as a function of α, the abscissa values. This is the variation in the optimal investment relative to the technology of attack. The contours are in relation to changing the discount rate β from 0.2 to 1. The intensity of attack is assumed to be unity, $\eta = 1$, and the technology of defence is fixed at $\psi = 0.2$**

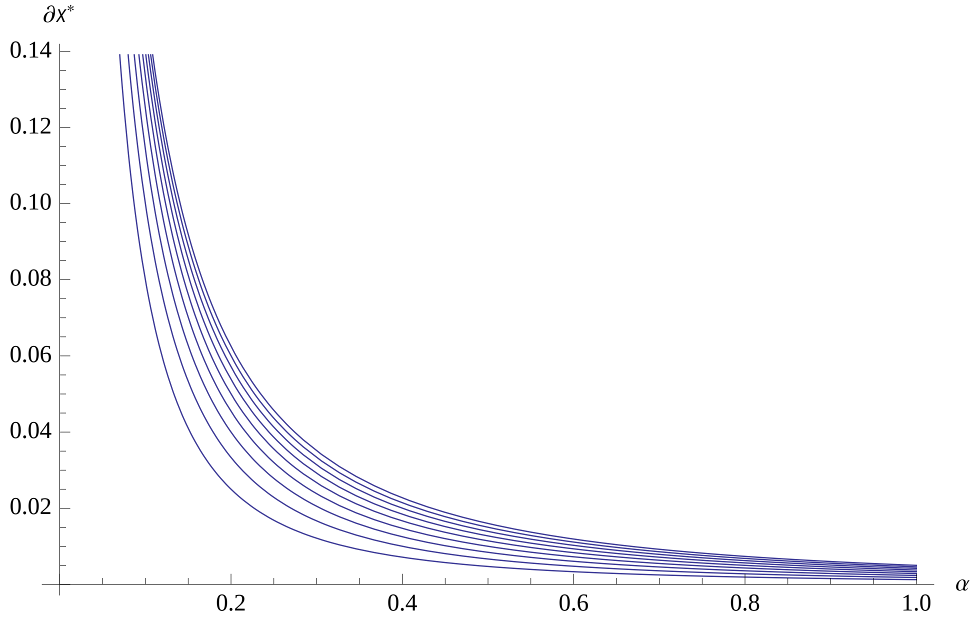

Figure 9: **The first derivative of $L^{-1}x^*$ assuming the same configuration as Figure 8.**

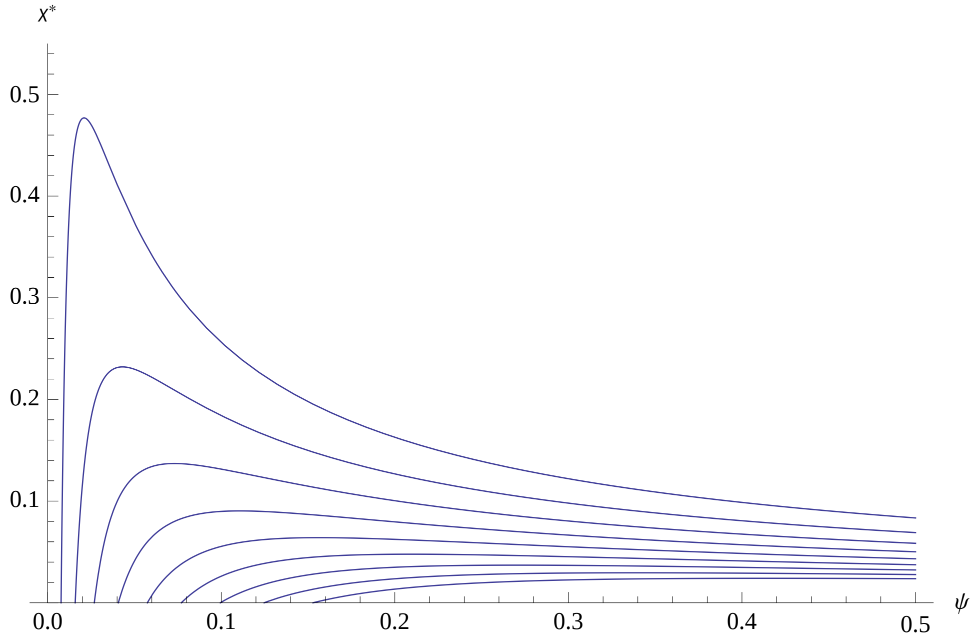

Figure 10: **Optimal defensive expenditure x^* when varying marginal defensive effectiveness ψ over a range of time preferences. the various contours represent different discount rates in the range $\beta = 0.2$ (nearest the origin) to $\beta = 1$ (furthest away from the origin), attacking intensity is set to being unity, $\eta = 1$, and attacking effectiveness is a constant $\alpha = 0.2$.**

contour furthest away from the origin represents $\beta = 1$).

For calibration purposes defining a group of points on this curve will allow the reconstruction of other parameters that might be less easily determined from data. Investment and perceived performance of defensive expenditure are more easily determined from case study evidence than the mechanism and choices of attackers.

An easier point of calibration is the technology of defence, in this mode denoted by the parameter ψ. As previously noted ψ is a constant marginal effectiveness of defence for a given level of permanent investment x. Figure 10 presents the variation in optimal defensive expenditure x^* with ψ as the abscissa. Figure 11 presents the first derivative of x^* relative to varying ψ. It is obvious to note that the variation in x^* is far more complex than the same condition with attacking effectiveness α. This emphasises that in this modelling set-up the choices of the target are far more important to the overall risk level than the choices of the attacker. The technical explanation is that attackers provide complementary slackness to the Nash equilibrium. The Nash equilibrium is stiff to the parametric solution to defence.

The contours illustrate that optimal defensive expenditure x^* is most variable when effectiveness is low. At this point the firm weighs up the small marginal improvements in reducing risk, ψ, with the cost of those improvements. This investment is then spread over the time horizon t, T, so the tipping point for low discount rates is the most acute. The derivative illustrates that changes in the effectiveness of defence will have little impact when ψ is high, but can cause rapid changes in investment policy when effectiveness is generally low. The interesting point from this analysis is that ψ is arguably the most important technological factor for investment behaviour. This is a testable prediction that the technology of attack is in effect

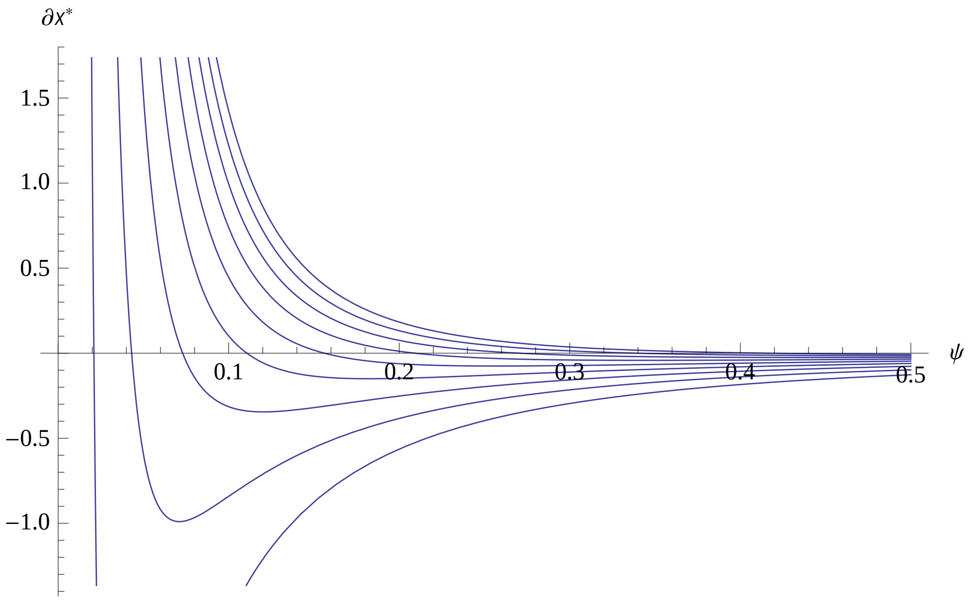

Figure 11: **The first derivative of x^* when varying marginal defensive effectiveness ψ over a range of time preferences.**

a constant, ascribing only a point of irreducible risk. The technology of defensive mediates almost all of the substantive variation in investment. The ability to translate investment into protection is the most important factor in risk mitigation, ceteris paribus.

4.5 Introducing Equilibrium

At this point we have illustrated the model with η set to unity as attacking behaviour is treated as being exogenous to the reaction function of the target. Therefore at attacking intensity from the viewpoint of the target is $\alpha\eta$ comparative statics of defensive choice can be illustrates in one dimension in terms of varying α, with $\eta = 1$. We denote η as an attacking intensity choice variable. Depending on the type of attacker model η maybe considered to be the following:

- A number of attackers per target $\eta = N_A/N_T$.
- A number of executed attacks per target $\eta = N/N_T$, where N is chosen by a single attacker.
- A distribution or expectation of attacks, so η is set in expectations and each realization is a draw from a distribution $\eta \sim \Phi(\cdot)$ where $\Phi(\cdot)$ is either an unconditional distribution or some form of Bayesian sub game.

For this expeditionary part of the problem structurer we shall assume the first interpretation, however, we ail include all three assumptions in the final version of the models.

Designing realistic attacker models is extremely difficult as motivations are currently not well understood. Evidence suggested in [2] indicate that attackers have low discount rates (i.e. long time horizons) and moderate fixed costs (this includes the expected cost of legal remediation).

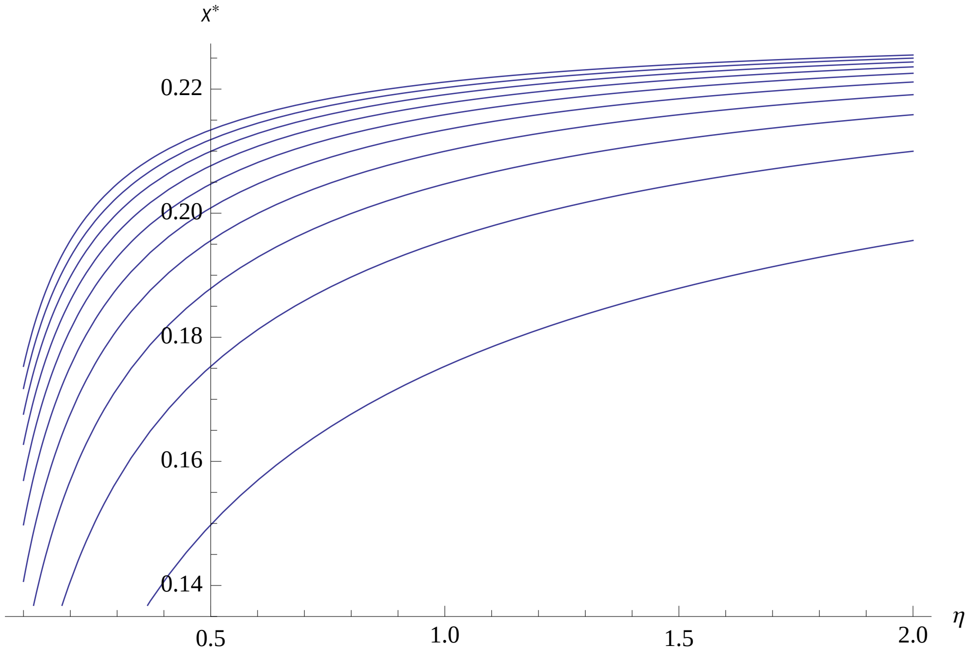

Figure 12: **Variation in optimal defensive expenditure x^* with respect to attacking intensity η. The contours represent different discount rates ranging from $\beta = 0.2$ (curves furthest from the origin) to $\beta = 1$ (curves nearest the origin)**

The variation of x^* to changes in η will necessarily mimic that of its coefficient α as illustrated in Figures 12 and 13, which we can see are effectively scalar adjustments of the reaction plots for α. Therefore as attacking intensity increases so does x^* however, ∂x^* is decreasing (although always positive) with respect to η for each of the illustrated discount rates, β, in the range 0.2 to 1.

Equilibrium occurs when η is a choice variable for the continuum of attackers. In this case we can conceive of two types of attacker, first a single attacker choosing to mount a number of attacks across targets. For simplicity of exposition we assume that attacks are un-targeted, in the sense that an attacker has no ability to discern specifically ex-ante if security measures are stronger in a particular target. This optimising attacker single allocates resources by maximising a reward function

$$\max_{\eta} \int_{t_0}^{T} e^{-\delta t} R \Psi\left(x, \eta\right) dt - \eta c$$

where δ is the discount rate and c is the cost per attack. We can now specify $\eta = N_A^{-1} N_T$, as the ratio of attackers to targets. Therefore if $\eta = 0.2$, then there is one attacker for every five targets. Recalling that R is the expected reward for the attacker. The major point to consider here is that attackers achieve maximum utility by solving this functions, this is not necessarily the attacker utility function, it is simply their pay-off in this part of the game.

An alternative to the profit maximising single attacker choosing an average η is a continuum of attackers that choose a single attack investment without coordination to other attackers. In competition they will force out extra attackers until the system is cost neutral.

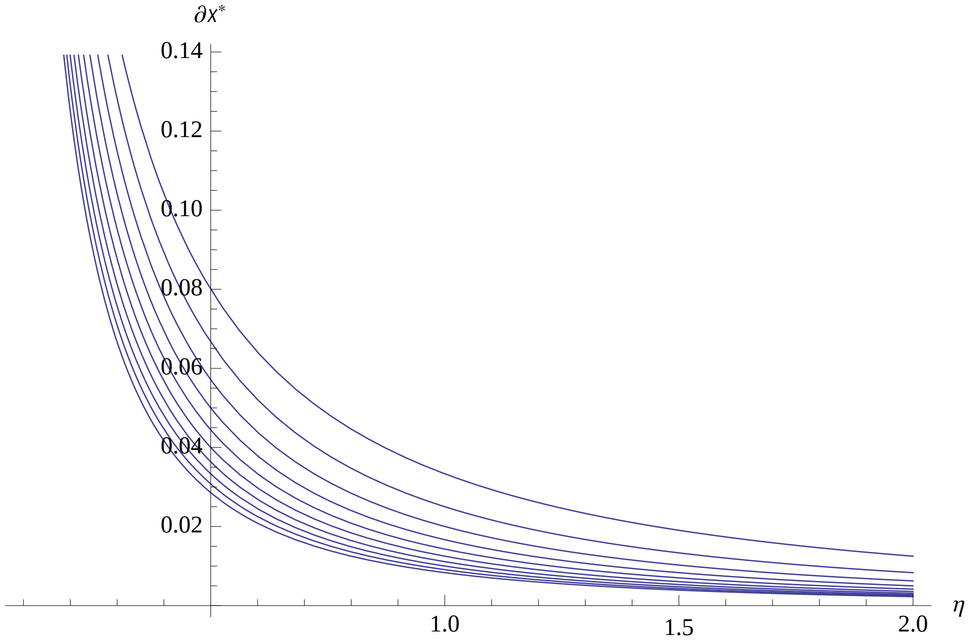

Figure 13: **The first derivative of x^* with respect to η. Parameters are consistent with 12.**

Therefore the continuum of attackers settles on an equilibrium attacking effort of:

$$\int_{t_0}^{T} e^{-\delta t} R\Psi\left(x,\eta\right)dt = c$$

we will concentrate our analysis on the second sub-case for demonstration purposes. The reasons are two-fold. First, there is little evidence for very broad coordination of attacking effort, even if large collections of attackers are coordinating, having more than two groups in existence will result in the analysis tending towards the uncoordinated competitive attacker case. Indeed there is evidence for fierce competition amongst attackers and this is best described by the second, Cournot, type case.

For a Nash equilibrium to exist, the continuum of attackers must treat the strategic instrument of the targets (namely x the investment in defensive actions) as exogenous and adjust η to solve their objective function. Following from the target model let:

$$\Psi\left(\eta, x, t\right) = e^{-\psi x} - e^{-\alpha\eta t - \psi x}$$

in this case the algebraic formulation for the attacker is:

$$\eta^* = -\alpha^{-1}T^{-1}\mathcal{Z}\left(\frac{\delta T e^{(\mathcal{A}T)}}{e^{\delta T}\left(c\delta e^{x\psi} - 1\right) + 1}\right) + \mathcal{A}$$

where

$$\mathcal{A} = \frac{\delta e^{\delta T}}{e^{\delta T}\left(c\delta e^{x\psi} - 1\right) + 1} + \delta$$

and $\mathcal{Z}(\cdot)$ is the Lambert-W function. Exploring the optimal attacking intensity we see that the presence of the Lambert-W function in the solution provides certain discontinuities in the equilibrium which we can exploit to make specific predictions.

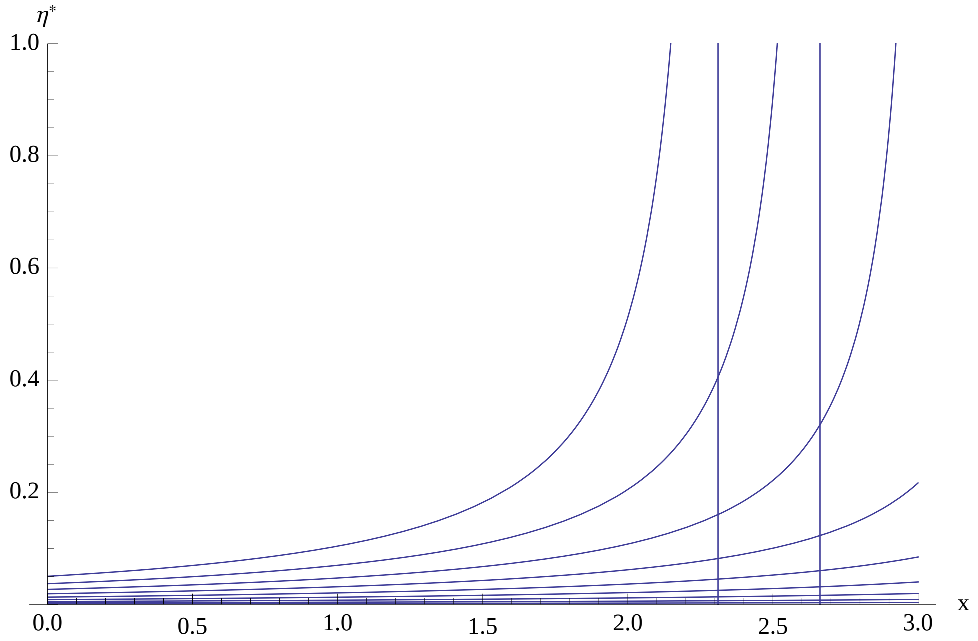

Figure 14: **The Nash equilibrium of the game. Attacker increase their effort to a point, however after a critical threshold attacking effort is no longer viable. The vertical line represents the threshold of attacking intensity.**

4.6 Analysing Attacker Behaviour

How does the intensity of attacks vary with investment? The sharpness of competition between attackers in this framework leads to a series of interesting predictions. First, it is quite likely that attacking effort may increase with defensive expenditure to a point. However, after a critical threshold is reached attacking effort will actually fall away rapidly as it is no longer viable to engage in costly attacking behaviour.

Figure 14 presents the variation in optimal attacking intensity, η^*, with defensive expenditure, x, over a range of attacker discount rates. The parameter choices for α and ψ are consistent with the previous examples, i.e. $\alpha = 0.2$ and $\psi = 0.5$. Pattern-wise the choice of α and ψ simply shift the contours left or right depending on magnitude. In Figure 15 we present the first derivative of the variation in η^* with respect to investment x.

Both patterns illustrate the prediction from this type of model, that optimal attacking effort will exhibit strong discontinuities with respect to defensive expenditure x. Counter to intuition, attackers will increase their effort in an arms race with defenders up to a critical point. After this the attacking effort with drop below zero. Therefore certain types of defensive expenditure are likely to be important, even in the absence of any observed attacking behaviour, as current defensive expenditure is above the critical value. Indeed, under most plausible values of attacking effectiveness α and marginal return to defensive expenditure ψ the tipping points will lie within the domain of potential discount rates for both attackers and defenders.

Figures 16 and 17 present the variation in attacking intensity and its first derivative, with respect to the effectiveness of attack α. The contours present a variety of defensive expenditures $x = 0$ (furthest from the origin) to $x = 10$ (furthest away). We can see that for certain

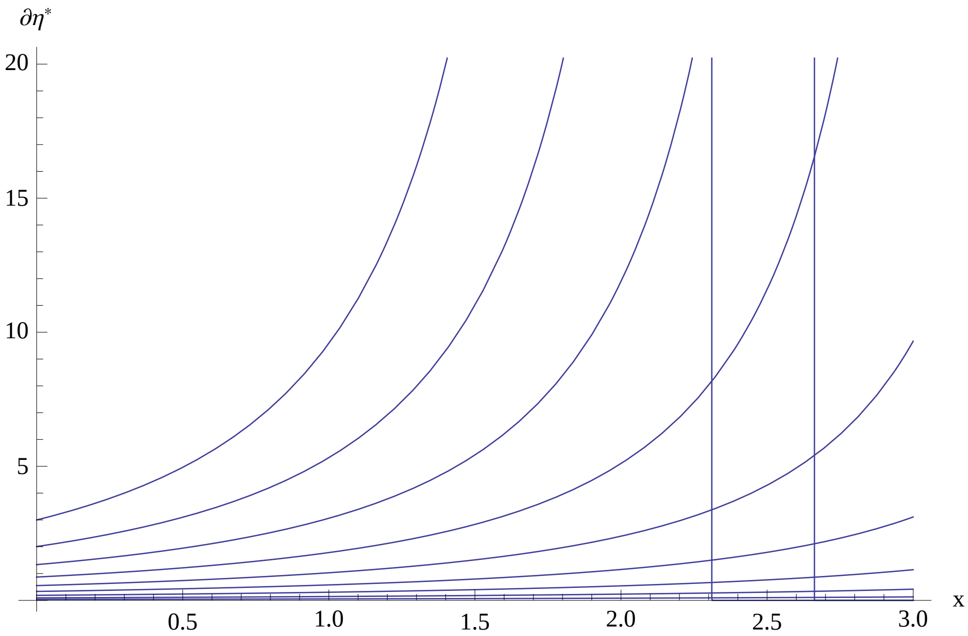

Figure 15: **The first derivative of the reaction functions illustrates the key thresholds of the model.**

discount rates the optimal level of attacking intensity decreases with attacker proficiency as attacking effectiveness substitutes for attacking intensity (the total profit from attacking being capped by the competition amongst attackers).

In contrast to the simple comparative statics of α, changes in the marginal effectiveness of attack ψ have a radical impact on the attacking intensity. Figure 18 illustrates the variation in attacking intensity η^* with respect to ψ over a range a of defensive expenditures. Figure 19 presents the first derivative. We can note that as ψx are both exogenous from the perspective of the attacker then the variation of η^* with ψ should mimic that of the variation with x. Indeed the discontinuities present in Figure 14 are present in Figure 18.

We can see that if tuning the defensive expenditure ψ is possible then exploiting potential points of discontinuity will result in very significant reductions in risk. Solving for the reaction functions $x^*(\eta)$ and $\eta^*(x)$ yields the Nash equilibrium level of attacking intensity and the level of defensive expenditure denoted η^N and x^N respective. In Figure 20 we select an example of a Nash equilibrium occurring prior to a discontinuity. Here $\beta = 0.2$ and $\delta = 0.1$, that is attackers have a lower discount rate than the defenders. Here ψ and α are calibrated to 0.5 and 0.3 respectively. Despite the fact that in this example defensive expenditure has a higher permanent impact on reducing risk than attacker intensity has on increasing it, the Nash equilibrium expenditure lies before the discontinuity in attacker effort (the blue contour line) relative to defensive effort (the pink contour).

A second discontinuity will occur at a larger value of x^* as at this point no attacking effort would be forecast to succeed in gaining any reward. The position of this equilibrium point is therefore stricIty a function of cost of attack c and size of losses L. The shape of the equilibrium is affected by the discount rates and the technology parameters α and ψ.

In Figure 21 we plot the reaction functions for $\eta*$ and x^* over a variety of discount rates to illustrate how the points of discontinuity can occur prior to the intersection and subsequent

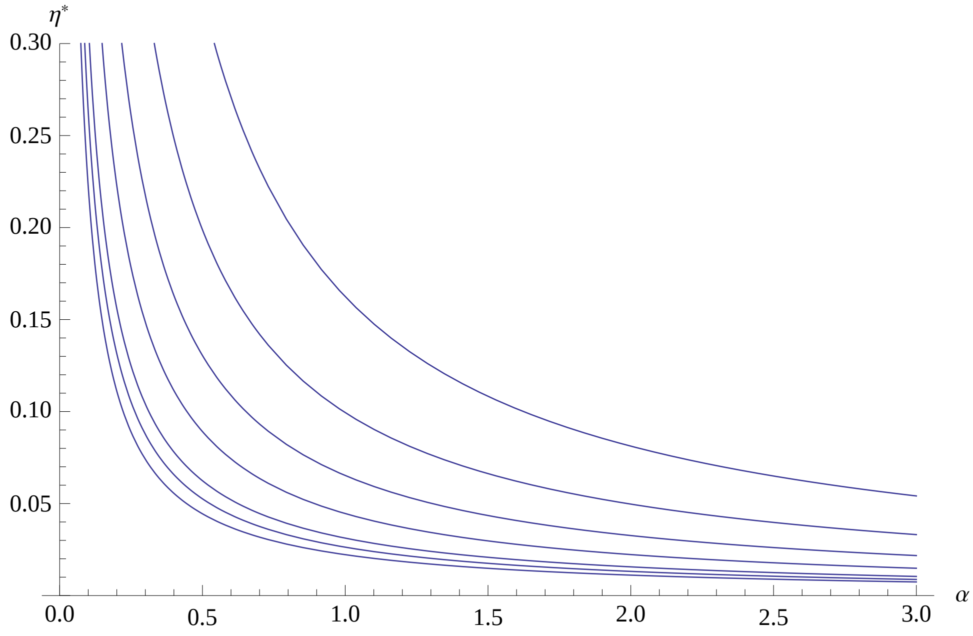

Figure 16: **The variation in η^* with respect to α.**

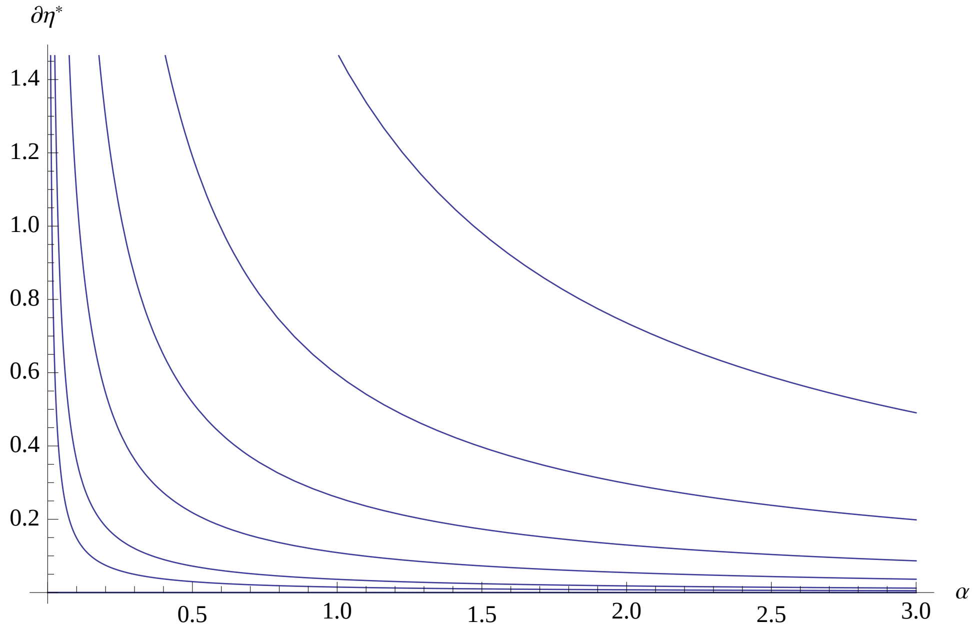

Figure 17: **The variation in the first derivative of η^* with respect to α.**

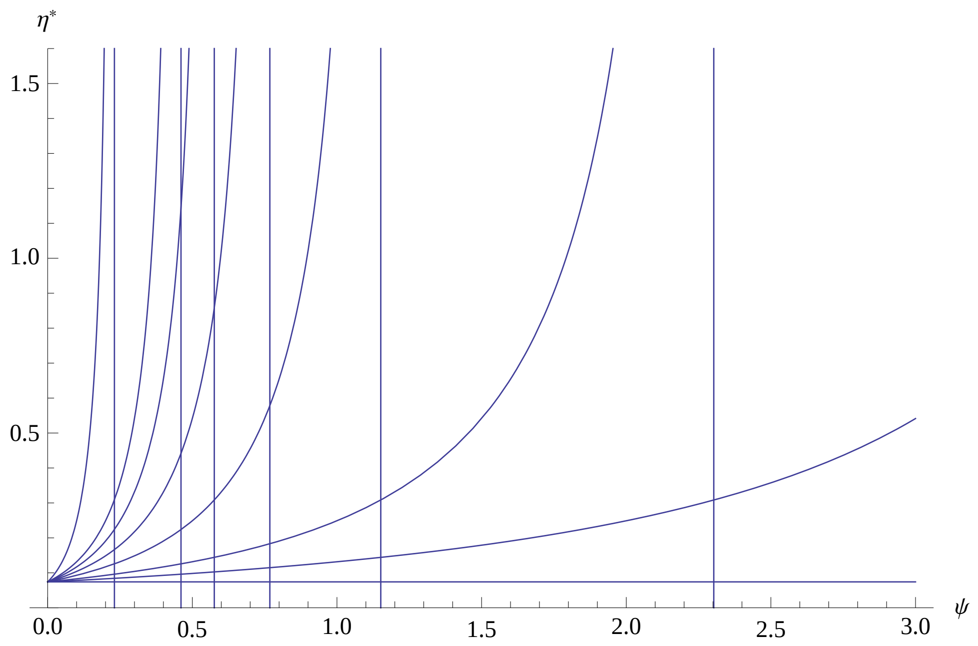

Figure 18: **The variation in η^* with respect to ψ.**

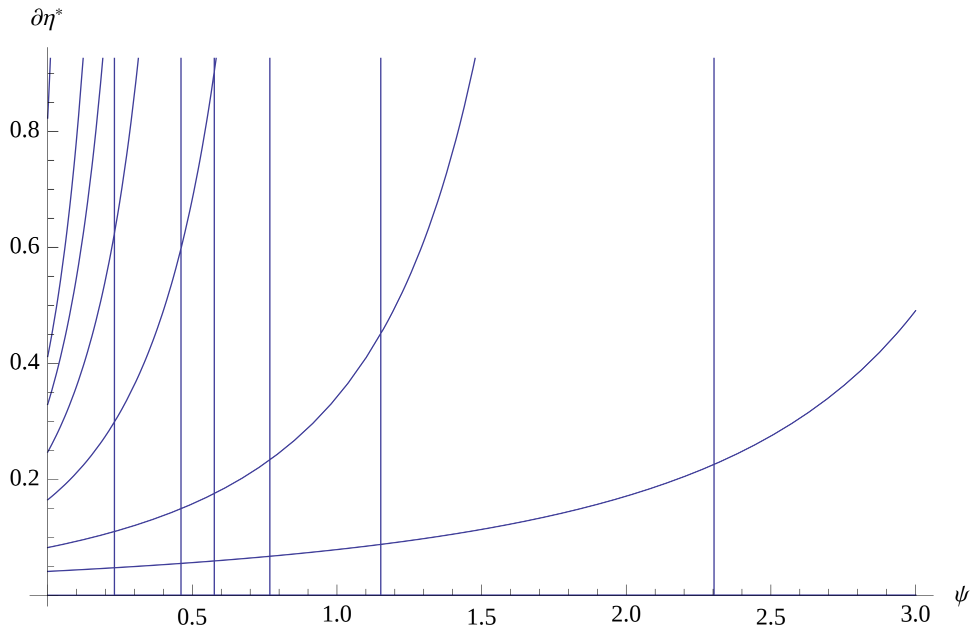

Figure 19: **The variation in the first derivative of η^* with respect to ψ.**

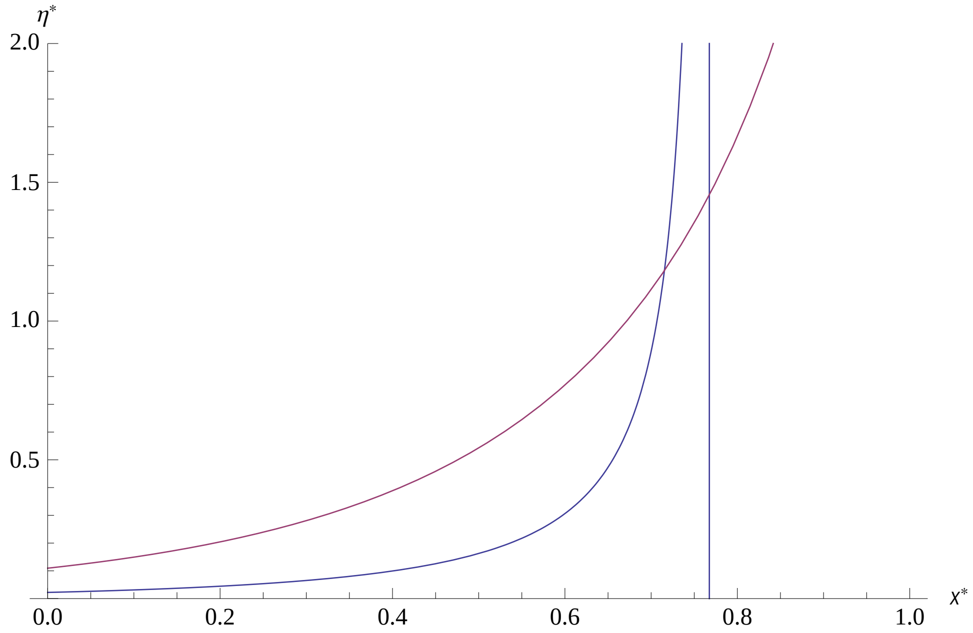

Figure 20: **The reaction functions of $\eta*$ and x^* points of intersection are Nash equilibria for $\beta = 0.2$ and $\delta = 0.1$.**

equilibrium and as such the optimal expenditure is driven to the point of discontinuity. In most circumstances this is the desired result as risk is driven virtually toward zero at this point. This is useful in illustrating the viable points in the model for calibration purposes.

4.7 Policy Intervention

We have illustrated the Nash equilibrium solution to a simple attack and defence game when both targets and attackers are pay-off maximising and measuring rates of success with equal accuracy. We are prudent in our approach in that we give attackers the ability to detect vulnerabilities and engage in attacking endeavour with equal likelihood, something which is currently not supported by the prevailing literature. The need for policy intervention is illustrated when the Nash equilibrium level of defensive expenditure for individual targets does not coincide with the objectives of the steward.

The sensitivity of the Nash equilibrium to changes in the discount rate β is far higher than the technology of attack parameter α. Even in this basic framework discontinuities exist and are primarily driven by the technology of defence ψ and the discount rate of the target β. The importance of this result is in emphasising that the choices of the defender, their technology of defence and their time preferences in valuing the cost of future attacks is the primary driver of the Nash equilibrium in this game theoretic set-up.

5. Vector Bundles of Security Investment

We now extend the analysis to include more complex investment arrangements to capture the impact of varying policy features. In this instance we now split the assets under threat

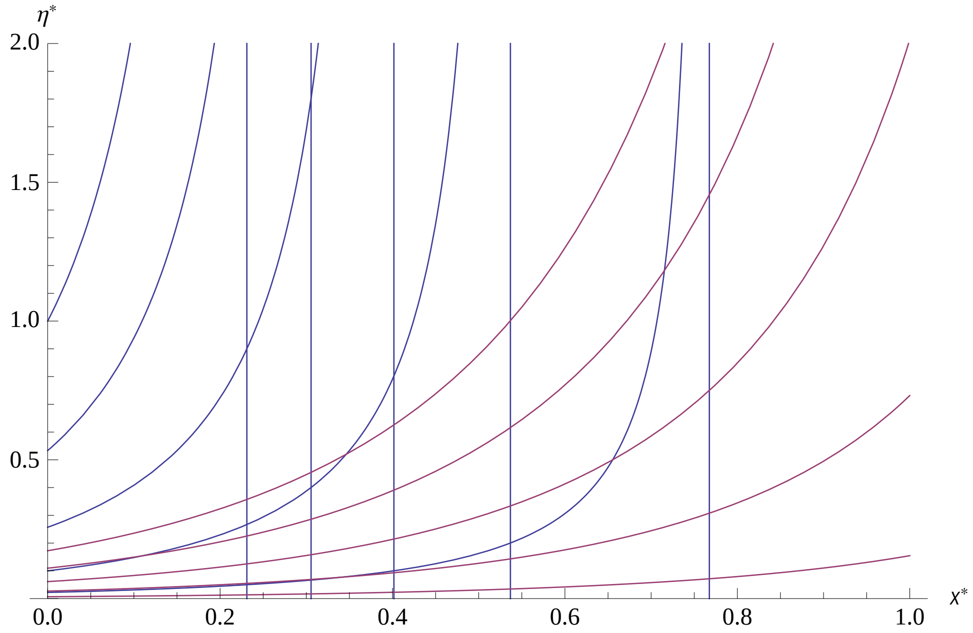

Figure 21: **The reaction functions of $\eta*$ and x^* points of intersection are Nash equilibria for a variety of discount rates β in the range 0.2 to 1 and δ in the range 0.2 to 1 (from near the origin outwards). In this case $\psi = 0.2$ and $\alpha = 0.3$.**

into two classes, those that are audited notionally and 'rules' based versus those that are un-audited and as such subject, exclusively, to the 'risk' choices of the firm.

We can consider assets that fall under the auspices of rules as being 'audited'. In this sense they exist to the external policy maker placing restrictions on behaviour in firms or individuals. By contrast assets for who security the individual firm or target are responsible are 'un-audited'. These assets do not have a specific classification in terms of the policy makers list of rules. Investment in securing these assets is the responsibility of the individual target and the policy maker is unable to positively identify of regulate these assets.

We assume that there is a weighting z which is either chosen by the individual target or is imposed exgenously by the mechanism. We can see that in very simple games, if the target has a freedom to choose then the ability to secure the asset is the primary driving force in determining the optimal structure. However, treating z as exogenous imposes interesting constraints on the targets investment choices.

The weighting acts as a mathematical tool for delineating assets for which security investment is already prescribed (the parameter ψ_l dictates the level of effectiveness of the imposed controls) versus those assets for which the firm/individual chooses their level of expenditure (with effectiveness ψ_h). A point of calibration here is in imputing the ratio ψ_l/ψ_h that determines the relative effectiveness of rules versus risks (see Section 2). For instance when $\psi_l > \psi_h$ the imposed investment is not as effective (on a per unit basis) as that chosen by the firm (for instance rules maybe expensive to implement and cover redundant items).

In order to extend our model we need to adjust our notation slightly and decompose some of the terms in order to have a more formal separation of the first order conditions. First we take the risk function and further decompose it into $\Psi(\eta)\Delta(x)$, where $\Psi(\eta)$ is separably additive to $\Delta(x)$. This is the case in the preceding example although for tractability in the vector framework it is now a necessary condition.

Let V_l be the expected losses at time t from attacks on the un-audited system and V_h for attacks on the audited system. We assume that the instantaneous expected loss is

$$\begin{aligned} V_l = \tilde{V}_l\left(\alpha_l, \eta_l, x_l, \psi_l, L, z, t\right) &= zL\Psi_l\left(\alpha_l, \eta_l, t\right)\Delta_l\left(x_l, \psi_l\right) \\ V_h = \tilde{V}_h\left(\alpha_h, \eta_h, x_h, \psi_h, L, z, t\right) &= (1-z)L\Psi_h\left(\alpha_h, \eta_h, t\right)\Delta_h\left(x_h, \psi_h\right) \end{aligned}$$

where $\Psi_{j\in\{l,h\}}(\alpha_j, \eta_j, t)$ and $\Delta_{j\in\{l,h\}}(x_j, \psi_j)$ are functions of attack and defence respectively. The total expected loss function for the i company from threats is therefore:

$$V = \tilde{V}\left(x_l, x_h, z\right) = \int_t^T e^{-\beta t}\left(V_l + V_h\right)dt$$

Therefore the defender has a net present loss of $V + x_l + x_h$. The optimal choices (x_l^*, x_h^*, z^*) of defensive expenditure for a given level of attacking intensity for the audited and un-audited systems (η_l, η_h) and the constant technological parameters $(\alpha_l, \alpha_h, \eta_l, \eta_h)$ is computed in terms of:

$$-\frac{\partial\tilde{V}\left(x_l, x_h, z\right)}{\partial x_l} = 1, \quad -\frac{\partial\tilde{V}\left(x_l, x_h, z\right)}{\partial x_h} = 1, \quad \frac{\partial\tilde{V}\left(x_l, x_h, z\right)}{\partial z} = 0$$

Let $x_h^*(\eta_l, \eta_h; \alpha_l, \alpha_h, \eta_l, \eta_h, \beta)$, $x_l^*(\eta_l, \eta_h; \alpha_l, \alpha_h, \eta_l, \eta_h, \beta)$ and $z^*(\eta_l, \eta_h; \alpha_l, \alpha_h, \eta_l, \eta_h, \beta)$ be, respectively, the reaction functions of investment (x_l, x_h) and asset allocation z for a given security threat vector (η_l, η_h) that satisfy the derivatives in 5.

We extend and generalize the derivatives from the one dimensional example so they are separably additive. We can build super and sub-modular payoffs in more complex games, however these interactions detract from the core focus of the analysis.

$$v_l\left(x_l^*; \eta_l\right) = -\frac{\partial\tilde{V}\left(x_l, x_h, z\right)}{\partial x_l}, \quad v_h\left(x_h^*; \eta_h\right) = -\frac{\partial\tilde{V}\left(x_l, x_h, z\right)}{\partial x_h}$$

here we have a loss function for both audited v_L and un-audited v_h states that react to attacking intensity in each state. Furthermore

$$\frac{\partial^2\tilde{V}\left(x_l, x_h, z\right)}{\partial x_l \partial x_h} = 0,$$

that is the loss functions are separable as we assume in the first instance that the joint partial derivative is zero, which is now a second order condition on the model.

5.1 Attackers In a Multi-State Setting

Attackers have the following decision tree: first the decision to attack, second whether to attack the audited or un-audited systems. Attackers are assumed to be randomly allocated to a target with equal probability. A successful attack rewards the attacker with instant revenue

zR and $(1-z)R$. The expected reward from attacking effort is therefore given by the following equations

$$\begin{aligned}A_l\left(\eta_l\right) &= \int_t^T e^{-\gamma t} zR\Psi_l\left(\alpha_l,\eta_l,t\right)\Delta_l\left(x_l,\psi_l\right)dt \\ A_h\left(\eta_h\right) &= \int_t^T e^{-\gamma t}(1-z)R\Psi_h\left(\alpha_h,\eta_h,t\right)\Delta_h\left(x_h,\psi_h\right)dt\end{aligned}$$

Assuming that attackers choose to enter the market for attacks on the audited or un-audtied systems until the cost equals the expected reward. Without much loss of generality we shall assume that each type of attack has the same cost C and that there is an unlimited pool of potential attackers. Therefore the number of attackers $A_l\left(\eta_l^*\right) = A_h\left(\eta_h^*\right) = C$. Therefore the Nash equilibrium values of defensive expenditure (x_l, x_h), allocation z and attacking intensity (η_l, η_h) are the solutions (if they exist) to the following set of equations:

$$\begin{aligned}A_l\left(\eta_l^N; x_h, x_l, z\right) - C = 0 \\ A_h\left(\eta_h^N; x_h, x_l, z\right) - C = 0 \\ v_l\left(x_l^N; \eta_l\right) = 1 \\ v_h\left(x_h^N; \eta_h\right) = 1 \\ v_z\left(z^N; \eta_l, \eta_h\right) = 0\end{aligned}$$

Let us assume that the present value loss function for the target is

$$\begin{aligned}V &= Le^{\beta(-T)}\left(\frac{ze^{-T\alpha_h\eta_h - x_h\psi_h}}{\beta+\alpha_h\eta_h} - \frac{ze^{-x_h\psi_h}}{\beta} + \frac{(z-1)e^{-x_l\psi_l}}{\beta}\right) \\ &\quad + \frac{Lz\alpha_h\eta_h e^{-x_h\psi_h}}{\beta\left(\beta+\alpha_h\eta_h\right)} - \frac{L(z-1)\left(\beta+\alpha_l\eta_l e^{T(\beta+\alpha_l\eta_l)}\right)e^{-T(\beta+\alpha_l\eta_l)-x_l\psi_l}}{\beta\left(\beta+\alpha_l\eta_l\right)}\end{aligned}$$

In this case there are separably additive solutions for x_l^*, x_h^* and z^* jointly satisfying $\partial V/\partial x_l = 0$, $\partial V/\partial x_h = 0$ and $\partial V/\partial z = 0$. Indeed z^* is a constant of the form $z^* = \psi_h/(\psi_l + \psi_h)$. This extremely useful as the analysis of the separate audit and un-audited systems runs in the same manner as the previous example.

However, once we impose rules based constraints on actions in the audited system, therefore x_h is a constant and possibly constrain the proportion of assets in the audited system z. In Figure 22 we see the variation in x_l when x_h is constrained by policy, for a variety of discount rates. The horizontal line represents the Nash equilibrium point of investment (the horizontal points of intersection with the curves reflect optimal choice of x_h from the view of the targets). In this instance increasing the required security investment for audited assets decreases x_l, in this example quite dramatically (the discount rates here are in the range suggested by NGRID).

We can see that policy instruments must take into account a) the time preferences of the target and b) the budget constraint of the target. The substitution effect for over-investment detracts from investment in security of assets not included in the audited list.

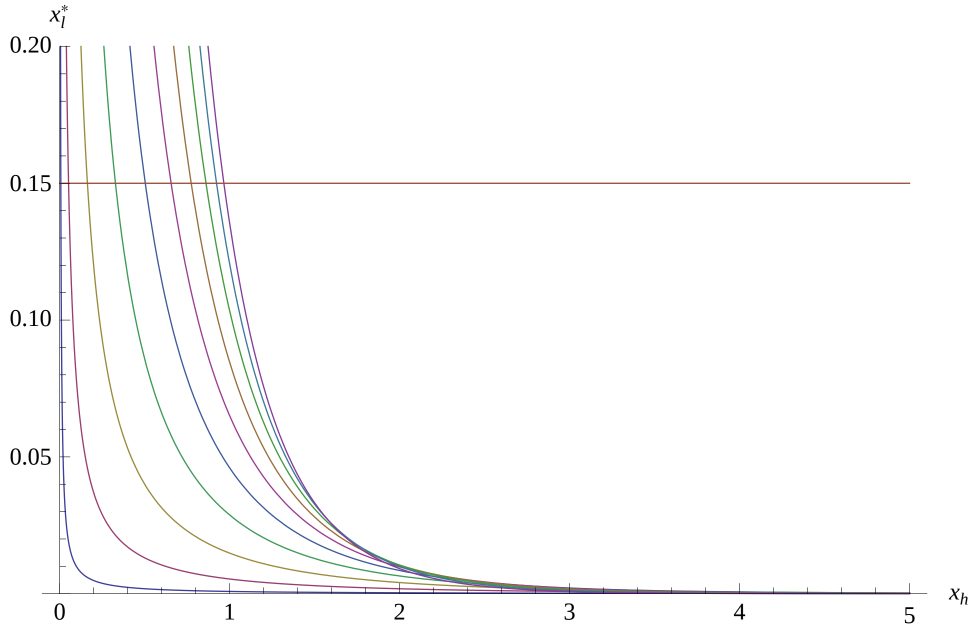

Figure 22: **The variation in un-audited investment x_l^* per dollar of assets at risk $(1-z)L$ when varying the cost of audited security investment. The parameters are consistent with the preceding example ($\psi_l = \psi_h = 0.2, \alpha_l = \alpha_h = 0.2$, $\beta = \{0.2, 1\}$, $\eta = 1$ and $L = 1$).**

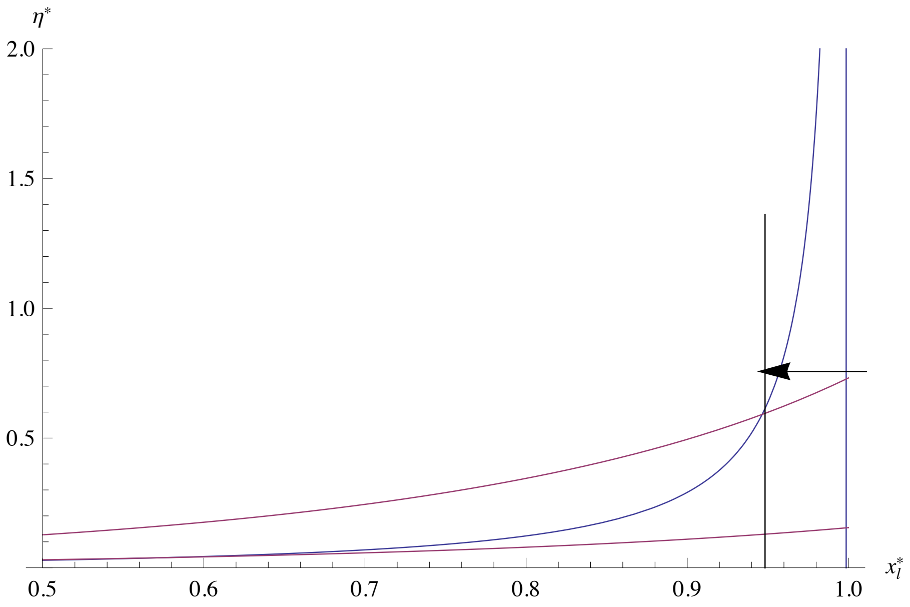

Figure 23: **This model replicates the initial case except we now have a constrained number of assets in the unaudited system. In the first case, both x_h and x_l are in a Nash equilibrium with the choice of attacking intensity η. Now we constrain x_h to a point higher than x_h^* such that x_l is reduced past the discontinuity in the attacker curve. A new equilibrium forms which now has non-zero attacking intensity.**

If the underinvestment in the un-audited assets approaches a critical boundary for attacking behaviour then inappropriately imposed investment constraints could create very large amounts of risk, from Figure 20.

In Figure 23 we repeat the Nash equilibrium game from the preceding example. The first attacker-target curves intersect to the right of the discontinuity and as such the ex-post observed attacking intensity is zero. However, we can keep the attackers constant and impose a constraint on x_h and z. In this case the reaction curve of x_l^* now intersects the attacker curve prior to the discontinuity. Therefore the imposition of the constraint on investment in x_h has now created more risk in the un-audited system.

We know by construction that this risk must be more costly that remediated by increasing x_h as the change in x_h must be to the right (i.e. larger) than the Nash equilibrium. Therefore the risk bearing mechanism must be either just to the left of the discontinuity or is actually approaching it.

6. Conclusion and implementation for other WPs

D8.3 has implemented an economic model to diagnose between policy regimes for critical infrastructure from examples outlined in WP2 D2.3. This is designed as an intermediate demonstration of the SECONOMICS modelling framework. In deliverable D8.2 the visualisation of this model is implemented within the SECONOMICS tool structure. In D8.2 we also discuss examples from WP1 (case study based on this modelling approach) and WP5 (scientific work package and related to WP3 implementation).

The degree of use of systems versus game theoretic economic models (with appropriate technical cost-benefit functions) varies across the case study implementations. The CNI example straddles both modelling domains almost equally, whereas studies base around the airport domain is almost exclusively set in the area of cost-benefit analysis. Analysis of regional transport uses methodologies borrowed from WP4 that balance the trade-off between security, congestion and cost. In each instance we can model the various salient features using a mixture of the tools outlined above.

BIBLIOGRAPHY

[1] Avinash K. Dixit and Robert S. Pindyck. *Investment Under Uncertainty*. Princeton University Press, 1994.

[2] Christos Ioannidis, David J. Pym, and Julian M. Williams. Sustainability in information stewardship. Georgetown University, Washington, 2013. Workshop on the Economics of Information Security.