SECONOMICS

D6.2 — A Report on the Interaction of Systems Models and Models of Economics, Law and Society

Pending of approval from the Research Executive Agency - EC

Document author(s) and Company –
M. Collinson (UNIABDN) (Primary Author Annex 3),
I. Gheyas (UNIDUR) (Primary Author Annex 1),
D. Pym (UCL) (Co Author Annexes 1 – 3),
J. Williams (UNIABDN,UNIDUR) (Primary Author Annex 2),
R. Ruprai (NGRID) (Calibration and Consultation Annex 2 and 3)

Acknowledgements:
Fabio Massacci, Woohyun Shim (UNITN) (Discussions), Petra Guasti (ISASCR) (main review and discussions) Contributing author partners (UNIABDN, UNIDUR, NGRID)

Acknowledged partners (UNITN, ISASCR, NGRID)

Security Economics: Socio economics meets security

Document Number	D6.2
Document Title	A report on the interaction of systems models and models of economics, law and society
Version	4.0
Status	First draft
Work Package	WP 6
Deliverable Type	Report
Contractual Date of Delivery	30.04.2014
Actual Date of Delivery	30.04.2014
Responsible Unit	UNIDUR
Contributors	J. Williams (UNIDUR, UNIABDN), M. Collinson (UNIABDN), I. Gheyas (UNIDUR and UNIABDN), D. Pym (UCL via UNIABDN) and R. Ruprai (NGRID) (see above for contribution breakdown and acknowledgements from ISASCR and UNITN.)
Keyword List	Public Policy, Regulation, Legal Implementation, Legal Instruments, Game Theory
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	Universite 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-Gesellschaft zur Fiorderung der angewandten Forschung e.V., Hansastr. 27c, 80686 Munich, Germany http://www.isst.fraunhofer.de/en/	Contact: Prof. Jan Jurjens jan.juerjens@isst.fraunhofer.de
4	Universidad Rey Juan Carlos	UNIVERSIDAD REY JUAN CARLOS, Calle Tulipileon s/n, 28933, Miostoles (Madrid), Spain. http://www.urjc.es	Contact: Prof. David Rios Insua david.rios@urjc.es
5	1495 UNIVERSITY OF ABERDEEN	THE UNIVERSITY COURT OF THE UNIVERSITY OF ABERDEEN, a Scottish charity (No. SC013683). King's College Regent Walk, AB24 3FX, Aberdeen, United Kingdom http://www.abdn.ac.uk/	Contact: Dr Matthew Collinson matthew.collinson@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 Medina alicia.garcia@atos.net
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. Ruprai Raminder 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
12	Durham University	The Palatine Centre, Stockton Road, Durham, DH1 3LE, UK https://www.dur.ac.uk/	Contact: Prof. Julian Williams julian.williams@abdn.ac.uk

Document change record

Version	Date	Status	Author (Unit)	Description
1.0	25/06/2013	Draft	J. Williams & David Pym (UDUR, UCL via UNIABDN)	Draft table of contents and content for Annex 2.
1.5	04/11/2013	Draft	J. Williams, David Pym (UDUR, UCL via UNIABDN) and R. Ruprai (NGRID)	Draft table of contents and content for Annex 2.
2.0	13/03/2014	Draft	M. Collinson (UNIABDN)	Reimplementation and consolidation in LaTeX
2.0	13/03/2014	Draft	M. Collinson (UNIABDN)	Reimplementation and consolidation in LaTeX
2.1	24/03/2014	Draft	J. Williams (UNIDUR)	Integration of all Annexe material and discussions with UNITN, ISASCR
3.1	Draft	Draft	J. Williams & Iffat Gheyas (UNIDUR)	Main drafting of Annexes 1 and 2 and sections 1 and 2 and corrections.
3.2	30/03/2014	Draft	M. Collinson (UNIABDN)	Minor edits
3.3	01/04/2014	Draft	E. Chiarani (UNITN)	Quality Check
3.4	31/03/2014	Draft	J. Williams (UNIDUR)	Edits following Scientific Review
3.5	31/03/2014	Draft	M. Collinson (UNIABDN)	Edits following Scientific Review
3.6	2/04/2014	Draft	J. Williams (UNIDUR)	Edits following quality check

Index

Executive Summary

Description of Deliverable

D6.2) A report on the interaction of systems models and models of economics, law and society: D6.2 will focus on how to build policy based on observations from research in economics and social policy and combining them with rigorous representations of the security architecture.

Overview

The main aim of this deliverable is to provide a marker stone for the current state of law and economics as applied to the case studies of security within SECONOMICS. This deliverable provides a) a comprehensive summary of the current and near future legal mechanisms for the EU and the US, identified as ket marker points earlier in the project for study. b) the current set of economic models developed within the project that map public policy to firm specific behaviour and c) the specific regulatory model framing for case study 2, of its interaction with various regulatory approaches. This deliverable plays a critical role in providing guidance on how laws interact with incentives to produce economic outcomes.

The document is broken down into sections following the DoW. In §(2.2) we provide an overview of the current future legal states and provide some summary analysis in respect to the EU context. In §(3.2) we provide a detailed analysis of our guiding assumptions on investment and risk within a game theoretic model of public policy specifically designed to capture the reactive antagonists observed in security economics. Finally, in §(4) we provide an overview of the architecturally consistent models use to model regulation for our case studies.

WP – D6.2 provides an overview of the research conducted by the SECONOMICS project on the role of security in society. A particular emphasis of this document is on the mechanism of regulation and the underlying economic and social drivers for the development of regulation. Attached to this deliverable are three research papers that focus on the main requirements as set out in the description of work. However, the research papers in the deliverable provide substantially greater depth than envisioned at the inception of the project and cover a wide range of approaches to designing regulation, from the detailed legal specifications found in ANNEX1 through to the theory of how to design the overview of these legal instruments in ANNEX3. In contrast ANNEX2 attempts to reconcile the high level conceptual approaches and the more specific legal drivers in a strategic framework. This deliverable represents a substantial step-forward in designing an evidence led approach to modelling strategic security situations at the macro-prudential level. In this case, the models that capture macro-prudential considerations represent both the specific design goals and implementation of regulation.

D6.2 contains threads in the technical parts of the Annexes that illustrate how the modelling approaches can be converted into working modelling tools deployed using simulation and analytical mathematics. The main body of the text of the document attempts to minimize the use of technical legal, modelling or economic language. For those interested in the specific implementations of the models the Annexes provide a detailed overview.

1. Deliverable Outline

This deliverable is organised as follows: provides an overview of our work on reviewing the current and proposed legal instruments and draws a series of contrasts between EU and US approaches to security legislation. This section focuses on the characterisation of the legal instruments and provides a summary of the dichotomy between tort (after the fact civil) and proactive audited (preventative) legal mechanisms. provides a non-technical summary of the game-theoretic approaches we have used to model the need for the types of legal mechanisms detailed in , it describes the major mathematical assumptions needed to ensure that the models are a) realistic and b) tractable. provides a brief summary of the results of this analysis and ties the modelling into the work undertaken in each of the case study work packages and the other scientific work packages. In Section 4 we provide an overview of the work undertaken on the direct interface between regulatory policy and firm operations and provide extensible models of firms in the presence varying public-policy and firm-specific policy regimes. ANNEX1 details our legal and regulatory analysis and provides our summary data on the various legal instruments covered within this analysis. ANNEX2 provides the technical summary of our work on the game theory of public policy and provides the main calibration exercises for the examples found in work packages 1 and 2. Finally, ANNEX3 provides a detailed technical overview of models on the interrelationships between regulatory typology and firm behaviour, and includes a detailed summary of the extensive numerical modelling involved in this exercise.

2. Review of Legal Instruments

ANNEX1 provides an overview of the current important pieces of security legislation and their mechanisms of enactment. The key issues that this review addresses are the mechanisms of audit and enforcement for current EU and US legislation in the area of critical infrastructure protection. In slight contrast to the SECONOMICS nomenclature, which identifies critical infrastructure (CI) as specifically relating to bulk electricity transmission, the legal frameworks treat regional and urban transport, air- transport, communications and energy as being under the CI banner. Therefore this review is useful for legal calibration work for models relating to Work-packages 1 – 3. We will refer to the concept of an 'entity' in this section, under the legal definitions set out in ANNEX1. In our context an entity is usually a firm or organisation providing critical infrastructure services.

The role of benevolent public policy is in correcting inefficiencies in allocations provided in the absence of a coordinating actions, via a public policy remit. The action of correction can take several forms.

The first approach to legislation. If inefficient allocations are caused by costly information search than the public policy remit is to enforce channels of information sharing and processing. The role of information sharing is a common theme across the legislative instruments reviewed in ANNEX1. Mandating information sharing and providing information processing capacity (sharing best practice, providing analytic and information search capacity through security agencies) is a well developed aspect of the current EU and US legislative provision.

In ANNEX1, Table ANNEX1.5 provides a comprehensive summary of the relevant legislative instruments useful to the project. The instruments are categorized by date, codifications, area of responsibility, enactment (or proposed in the case of the US), region (EU or US) and an executive summary. For complex legislation a long summary is provided and key points are outlined in **bold**.

The second approach to legislation. When information sharing is unable to provide efficient resource allocations, then regulation is needed to provide constraints on behaviour of individuals and collections of individuals to ensure global welfare improving outcomes. In the security legislative arena the security of air transport has a long lineage of mandated security policies with behavioural constraints and these are documented in Table ANNEX1.5. In this sense, developments post September 11, 2001 have led to a strong convergence in air-transport regulation, with similar specific legal text appearing in transport protection documentation in both US federal and the EU Acquis communautaire documentation reviewed in Table ANNEX1.5.

For critical infrastructure, particularly electricity transmission, there are differences in approach and implementation between the EU and US in the development of enforceable regulatory rules for operation. In general the US legislation has focused on an enforcement mandate, with the department of homeland security, department of justice, department of energy and the department of defence acting as coordinating entities. For energy security the Federal Energy Regulatory Commission is the agency primarily tasked with regulating security resource allocations in critical infrastructure. The mechanisms here involve audit processes relating to a specifically tasked rules based regime.

The key aspects to this legislation is the provision of specific behavioural and investment restrictions on regulated entities (in the case of bulk electricity transmission this is delegated to the National Electricity Reliability Corporation or NERC). NERC provides compliance guidance to state and national governmental structures to and to provide specifications for auditors. From a modelling sense these are specified menus of contracts with compliance penalties and can therefore be modelled using the standard mathematical concepts covered in ANNEX2.

The EU context provides a more eclectic set of regulatory framings and we provide modelling techniques to capture this framework in ANNEX3. We can see from the descriptions in Table ANNEX1.5 that the general approach has been to delegate detailed enforcement implementation to member states. The subsequent examples of implementation detailed in Table ANNEX1.5 provide insight into the varied modalities of implementation pursued by the various EU members. As an interesting aside we can also view the lack of uniformity in implementation from two viewpoints. First, that lack of uniformity ensures that state-wide audit is more difficult to effectively implement. However, an opposite view says that positive externalities may exist; a heterogeneous family of security provisions could reduce the risk of broad, systemic risk. In this case an eclectic set of security provisions can reduce the likelihood of broad systemic risk. We will explore these features in more detail in ANNEX2.

2.1 Tort versus Pre-emption and Liability Sharing: The US Experience

As stated before tort law is the mechanism of redistributing costs after the fact. This is generally considered to be a 'civil' mechanism whereby injured parties are compensated for costs. However, it is obvious from the intent of US legislation that certain costs are non-recoverable (such as death or serious injury) and as such ex-ante liability sharing is imposed and audit used to provide assurance rather than insurance against risks.

Enforcement mechanisms vary considerably from the US to the EU. The uses a mixture of tort based solutions mixed with a pre-emptive penalty structure for violation of audit requirements. The tort law solution is considered an ex-post or civil liability solution. In this sense cost sharing occurs after cost incurring security events. However, for critical infrastructure further levels a greater level of preventative action is demanded in the US system and enforcement is primarily via the audit and compliance method, independent of actual incidents. Liability in this context is usually waived for incidents outside of the audit conditions. However, both at the operational level (see WP2.3) and at the legal level the distinction between liabilities covered under the tort provision versus those covered under the liability protection coverage are not completely transparent.

2.2 Policy Insights

The need for regulation stems both from the need for information sharing and processing, and from the need for the policy-maker to implement behavioural constraints. When individual agents' incentives are not aligned, global social welfare cannot be attained by individual agents even when they are fully informed; hence behavioural constraints are needed .

The legal implementation of desired regulatory policies follows two broad approaches. First, one that sets target levels of risk and provides a broad risk minimization approach, with Tort penalties posted after the fact, based on some broad principles of liability sharing and prior case history. This is in keeping with various comparable environmental and civil legal schemes implemented in similar regulatory areas (such as employment law, natural disaster prevention and recovery and pollution emission schemes). Second, a set of mandated requirements with associated audit and compliance mechanisms. The degree of liability provision depends upon the audit compliance and degree of coverage; however this relationship, as described in legal phrasings and constructions, is highly complex. This analysis provides the core foundations for the mathematical deconstruction of how regulation impacts on behaviour. This follows from the nature of contracts, using their mapping to mathematical artefacts within a game-theoretic set-up.

3. Review of Public Policy Models

Cost-benefit analysis forms a fundamental role in public and firm specific policy making. Actions have to be balanced between expected cost and expected benefit. However, the measurement of cost and benefit for many public policy decisions is not always straightforward, and neither is the task of comparing them. The models that we use often use probabilities (they are stochastic) because of the presence of uncertainties in the underlying scenarios. For example, a modeller cannot always predict in advance exactly which vulnerabilities will be discovered or exploited in a particular time period. In such stochastic models, we typically try to structure the cost-benefit analysis in terms of suitable averages. Technically, this is done in terms of *expected utility* (or *payoff*) values. Finally, this leads to some solvable *loss function* (or equivalently *utility function*) over the possible actions, which is then optimised to provide the best policy choice.

In the present model we assume that the choice of each individual agent corresponds to a single value (often a real number, in the set $\mathbb{R}$). With n individuals, their choices together form a vector $x \in \mathbb{R}^n$. In the case of these models of security, x is a vector of allocations and investments in security. The policy-maker can set policies that influence aggregate choice, x. For example, this can be done either by setting a constraint (such as a lower bound on each of the values chosen by each of the agents, i.e. the components of the vector x), or by choosing a specific value for x (and so for each of the agents) following some optimization procedure.

The most interesting aspect of the analysis is not in the evaluation of specific firms (agents) behaviour; rather it is in how collections of firms come to decisions alongside public policies set by a policy-maker. That is, it is the aggregate social effect that is brought into sharp focus.

Incentive compatibility is an important phenomenon in economics. An important instance of this occurs in the present context: in the absence of regulatory constraints on the values of x, individual choices by firms may lead to an aggregate set of choices that is substantively different from the choice that society as a whole would deem appropriate. We write such an aggregate choice as a vector $x^* \in \mathbb{R}^n$. We write the socially optimal aggregate choice as a vector $x^\dagger \in \mathbb{R}^n$. Societal preferences are reflected in the public policy-maker's loss function.

The policy-maker desires that $x^\diamond$ be adhered to by the firms and as such the optimal contract that the policy-maker imposes on firms is $x^\diamond = x^\dagger$, if monitoring and enforcement are costless. How are the constracts created? This maybe in the form of specific laws such as those in ANNEX1 or in the form of inducements and cost sharing mechanisms, again the table in ANNEX1 provides a summary. We can think of $x^\diamond$ as being the 'first-best' policy attainable given the abilities of the public policy-maker.

Why would individual firms' choices not converge on $x^\dagger$ in the absence of mandated legal action? The simplest case is that firm preferences are societal preferences are divergent, that is, they have different priorities. The second case is that the very action of attempting to achieve $x^\dagger$, results in global deviation from $x^\dagger$, this is due to unequal cost sharing as such the public policy-maker needs to step in to redistribute costs and ensure a fair security allocation.

ANNEX2 provides insight into public policy for collective security: that is, it provides policy insight at the macro-prudential level, and it does so from the perspective of game-theoretic models of collective security behaviour. We have now built a fully functioning partial equilibrium model of economic behaviour at the macro-level with externalities and time preferences providing the key drivers of security investment behaviour.

Our major assumptions in these models are:

- The technology of attack and defence results in *diminishing marginal returns* to security investment (see WP1 – WP3 deliverables X.3 and X.4 for validation of this modelling assumption)
- Attackers are *strategic* (see WP5 results on modelling strategic attackers)
- Firms operate as loss minimizing entities under *risk neutral* measures (see discussion below)
- The public policy-maker has a societal mandate to provide a secure set of firms and has a time horizon for investments decided on by a *social discount rate* (see work in WP4 on societal preferences)
- Regulatory mechanisms are in the form of legal contracts (either implicitly through criminal laws or explicitly through civil laws) and are mediated by audit
- For our most advanced case we shall assume that audit is *incomplete*
- Security threats to attackers arise from a matching of attacker agents to target agents; this is done by a random selection method, following a well-understood probability law
- All agents are *rational* — this is encapsulated by their desire to optimise their (expected) utility functions

3.1 Investment Decision Making

We assume that risk preferences are entirely subsumed within the preference-setting at this time; we work under a risk neutral formulation of the investment model at each current period. Risk neutral decision making is of the form $\tilde{V} = \sum_{i=0}^{N} q_i V_i$, where q_i are risk neutral probabilities and V_i are the current values of the outcomes states associated with each risk neutral probability and there are $N + 1$ states. A key point here is that q_i are not the “true" probabilities, but are adjusted probabilities weighted to provide the agent with an expected pay-off. For instance, if the true probabilities are $p_0 = p_1 = 50\%$ and the value of the pay-off in each state are $V_0 = 0$ and $V_1 = 1$. If the agent is risk averse whereby the utility function is given by $\mathbb{E}(U) = \mathbb{E}(V) - 0.5 \times \mathrm{var}(V)$ (a typical log utility approach adjustment). In this case the payoff is $\mathbb{E}(U) = 0.5 - 0.5 \times 0.5^2 = 0.3750 \times 1$. In this case the payoff should be $q_1 = 0.3750$ and $q_0 = 0.6250$ as $\tilde{V} = 0.3750 = V_0 \times q_0 + V_1 \times q_1$, subject to $q_1 = 1 - q_0$.

We now expand this to a more conventional loss aversion case. Consider an agent faced with the following pay-off (utility) problem:

$$\max_x \mathbb{E}(U(x; p(x), v(x)))$$

where x is a vector of decision variables and p is a probability function and v is a cost function. The simplest version of this is as follows:

$$U(x; p(x), v(x))) = -vp(x) - x$$

where v is constant and $p(x)$ is declining in x. Under a standard measure the utility function is evaluated by

$$\mathbb{E}(U(x;p(x),v(x))) = \int_{t_0}^{T} e^{-\gamma t}U(x;p(x),v(x))ds \rightarrow \int_{t_0}^{T} e^{-\gamma t} - vp(x) - xds$$

where s is a sample space. However, we can determine a new probability measure, $q(x)$ whereby

$$\int_{t_0}^{T} e^{-\gamma t}U(x;p(x),v(x))dt \equiv \int_{t_0}^{T} e^{-\beta t}U(x;q(x),v(x))ds \rightarrow \int_{t_0}^{T} e^{-\gamma t} - vq(x) - xdt$$

note that the integral with respect to q is a deterministic integral over the t_0, T time horizon. Here γ is the observed discount factor and β is the discount factor under the risk neutral probability function q. The importance of this function is algebraic tractability. The utility function requires determining over the complete set of moments of a set of outcomes dependent on the probability function $p(x)$. We can however re-parametrize p to a function q whereby the expected value $v \times q$ provides the point utility function. The new risk neutral discount factor β contains all of the information needed to determine optimal cost-benefit analysis. Therefore we can specify problems in the form $Cost = v \times q(x)$.

This provides an easily analytically tractable framework for dealing with cost-benefit analysis at a local level. As long as the function:

$$\int_{t_0}^{T} e^{-\beta t}U(x;q(x),v(x))dt$$

is convex in x, there is an optimal solution x^* that provides the optimal investment allocation. In Deliverable 8.3 we have provided the one dimensional case for multiple firms in an economy protecting themselves against a strategic set of attackers randomly allocated across firms. We show that under very simple assumptions the optimal level of attacking intensity and the optimal level of defensive expenditure may be characterised in a simultaneous Nash equilibrium (in the sense of Game Theory). From this point we have expanded to a multivariate case whereby targets have a multilateral asset allocation problem with differentiated behavioural restrictions.

This permits the creation of differentially audited assets with varying levels of security criticality. In ANNEX2 we then solve a model where targets can choose to shift assets between a regulated asset class and an unregulated asset class. We show that under certain differentiated conditions investment in security can have counter-intuitive effects. For instance, in the fully-informed public policy case the target firm can switch assets, but the policy-maker can observe the level of security and compute a ‘second best’ outcome to incentivise pro-social welfare outcomes. However, when the policy-maker cannot observe the security investments (for instance because audit is too costly or technically too difficult in one asset class) then public policy choices designed to provide the social optimum my cause more harm than good.

Figure 1: The general landscape of the public policy-maker problem. This figure presents the general set-up of the policy problem. We assume that there is a cloud of attackers that collectively choose a level of attacking intensity. We assume a variety of attacker collaboration types from pure competition to a purely collaborative model. The target firms allocate security across different asset areas, see Figure 2.

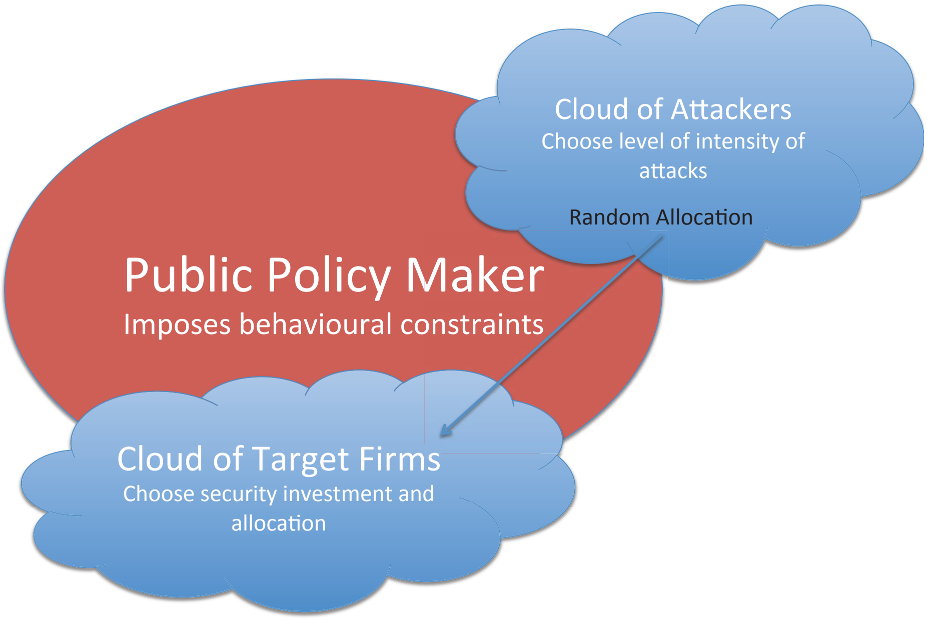
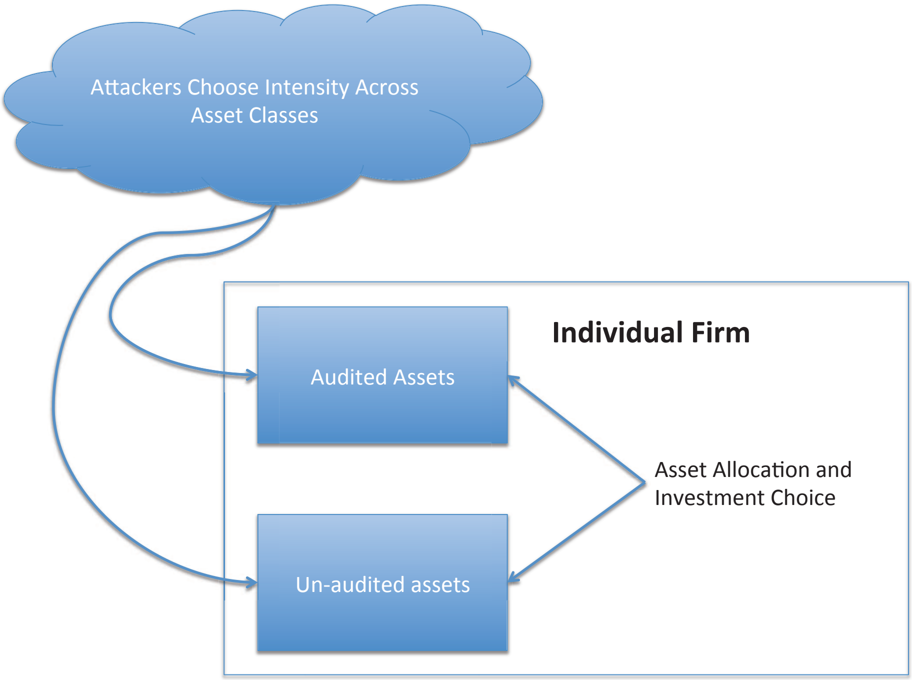

Cloud of Attackers
Choose level of intensity of attacks
Random Allocation
Public Policy Maker
Imposes behavioural constraints
Cloud of Target Firms
Choose security investment and allocation

Figure 2: The asset allocation problem. Target firms choose assets to declare as audited assets, versus those they place (or are forced to place) in the un-audited domain. Attackers choose as a group the level of intensity of attacks they engage in on a particular asset class, however, they are randomly allocated across targets.


Attackers Choose Intensity Across Asset Classes
Individual Firm
Audited Assets
Un-audited assets
Asset Allocation and Investment Choice

The models are designed to capture the issues we have observed in the case study work packages, where there is an incentive incompatibility between policy-makers and targets in terms of cost bearing. In general firms are assume to have higher risk-neutral discount rates than society at large. Ceteris paribus, this means that given identical risk functions, a firm will choose a lower level of investment than that preferred by a police maker. This is simply a result of the risk tolerances and time preferences of target firms.

In this case we can set a social discount factor $\delta < \beta_i \forall i \in \{1, \ldots, N_T\}$, where N_T is the number of target firms and β_i is the firm specific discount rate (that dictates time preferences). As such, on average, firms will tend to under invest in security provision, instead relying on the large number of other firms in the economy to dilute attacking effort or on implicit social liability insurance. Figure 2 presents the firm allocation problem. In ANNEX2 we provide a model whereby firms choose an allocation z between two asset classes, (audited) and (unaudited). In particular, this relates to the question of risk-versus-rules for regulation of electricity transmission discussed in ANNEX3 of this document and WP5 deliverables.

Attackers are randomly allocated, with equal probability $1/N_T$, to target firms. In the most basic case of non- collaborative attackers, an externality of under-investment exists, whereby the diminishing probability of attack success with increasing N_T allows for systematic under-investment. This externality is exacerbated by the differential in discount rates between the public policy-maker acting on behalf of society and the individual target firms.

3.2 Policy insights and calibration to case studies

WP2 provides a set of key calibration parameters for the application of this model to ICS/SCADA systems in bulk electricity transfer (see Deliverable D2.4). In this instance we have the discount rates for the firms and some qualitative record of security incident frequencies as well as degrees of loss.

The models illustrate conditions under which shocks to the technology of security infrastructure protection propagate into the economy of target firms and the potential reaction of those firms in the absence of regulatory intervention, when regulatory intervention is fully informed and when regulatory interventions are only partially informed. We illustrate that in the absence of full information the decision to not regulate can sometimes be the optimal choice of the social policy maker.

In Deliverable D6.3 we present another specific case of the multi-asset allocation problem for assessing principal agent issues in airport security (a detailed analysis is also applicable to regional transport, however an even more detailed appraisal of this is found in D5.2). In this instance we again have a policy-maker, target airports and strategic attackers.

The key concept here is the presence of incentive incompatibility between the target airports and the social policy coordinator. The structure of audit in this case is also incomplete, however, the airports have a higher level of synchronisation in terms of discount rates (time preferences and risk preferences) than the bulk electricity providers. The attacker model in the airport case is also slightly different as their objective functions contain stochastic elements that allow for non-survivable-attacks. Our current set of results give indicative investment and security allocation patterns for local airports and regional hubs.

The models in ANNEX2 are fully analytic — as such we do not provide code as the solutions are in the form of worked equations that we can sketch using standard approaches. These are discussed in WP8 D8.4 and D8.3.

4. Review of Regulatory Models

4.1 Introduction to the Key Policy Problem: Rules-versus-Risk

ANNEX3 is concerned with models of regulation for critical infrastructure, particularly bulk electricity transmission. A key issue highlighted by (project partner) NGRID is the effect that different regulatory regimes can have on a transmission operators security strategy and operations. Moreover, the need to operate in multiple countries where fundamentally different regimes apply (and potentially in other industrial sectors, for example gas supply) can mean that the effects of regulatory policy on effective security protection can be hard to understand or predict.

In electricity transmission (and indeed, in generation and supply) there two forms of regulation are commonly contrasted, these being known as *risk-based* and *rules-based*. In *rules-based* (sometimes known as *bright line*) regulation, the regulator specifies — sometimes very detailed — controls (on people, process, technology) that are required of the operator, the operator is audited for compliance with these controls, and then some kinds of incentives (often negative, in the form of punishments or liabilities) are applied. In *risk-based* regulation, the operator is allowed to evaluate the risks, to define its own strategy and apply its own controls. It is usually required, through some process, to justify its posture to the regulator, and then rewards or punishments may be applied. These rewards and punishments may be very indirect, for example, potential exposure to damages from torts, or potential non-renewal of contracts.

Clearly, the rules-based system appears to have an advantage in that it provides assurance to the regulator that certain controls will be applied. On the other-hand, risk-based regulation would appear to allow operators to apply security controls that are more appropriate to their own risks. It would also appear to allow for greater agility in reacting to new threats. Further advantages and disadvantages of each could be enumerated.

There are real examples of both regulatory regimes in current operation. In the UK, essentially, the approach is largely risk-based and not highly-structured or codified. In the USA, there is a more rules-based system, particularly since the move from version 3 to version 4 of the NERC CIP (NorthAmerican Electric Reliability Corporation, Critical Infrastructure Protection) framework[1]. The importance of the mode of regulation has been recognized by policy-makers at the highest level [2, 3].

Which of the two modes of regulation is better is a matter of current intense debate [4, 5]. Much of this is stimulated by the risk-based methodology advocated in drafts of the (National Institute for Standards and Technology (USA)) Cybersecurity Framework, now formally released [6]. However, most of this discussion is based on expert opinion rather than objective evidence. In line with the goals of Seconomics, in ANNEX3 we advocate the use of models to tackle such questions.

4.2 Structure and Status of Our Models

At present, our models in ANNEX3 simply try to describe the structure and interplay of types of economic incentive for security (risk-based or rules-based) and to explore the general kinds of behavioural effects that can arise from this, rather than to be tightly fitted to numerical data and to make detailed predictions. It may be that such refinement can be done at some later date, but for now we confine ourselves to theoretical models grounded in our intuition for economic effects and in what our interactions with domain experts (in conjunction with WP5) have told us about the structure of the problem.

Note that even when data arises that purports to answer the question of which is better, risk or rules, the complexity of the situation is likely to mean that models will be required to intepret the meaning and significance of that data, and to provide sensible hypotheses for potential refutation. That is to say, this is unlikely to be a question that a naive ‘big’ data-gathering exercise and statistical analysis can answer alone in the absence of some understanding of the underlying economics.

The underlying view of our models is that they are games in the sense of Game Theory. Put simply, this is the best modelling framework for handling questions about the strategic interaction of multiple agents — that is to say, situations in which agents may have conflicting desires for different outcomes and may react, or even anticipate, each other’s choices of how to influence outcomes.

In order to make progress we make numerous abstractions and simplifications in our work — these in no way preclude generalization to more ‘realistic’ models. In the present work we confine ourselves to situations in which a single policy-maker attempts to regulate the behaviour of a single transmission operator (known as ‘the firm’ throughout).

The policy-maker can make various choices such as: a quantity of spend, a set of security rules, and a scheme that trades-off how it rewards the firm for its performance in terms of both auditable compliance and actual performance for its core function — safe, secure, reliable transmission of electricity. The firm can also make various choices: how much it spends, how it allocates its resources to complying with rules and to directly mitigating risks to supply. The actual quality of the job of transmission is dependent upon the latter. Thus we see that the outcome for the policy-maker (representing society) and the outcome for the firm are deeply intertwined.

This is encapsulated in our models through the use of a pair of interdependent *loss functions* (also known as payoff functions), L_F and L_P. The interdependent nature of these function is shown schematically in Figure 3. This figure is reproduced and explained fully in ANNEX3.

In ANNEX3, models that are simple numerical instantiations of this general framework are subjected to preliminary investigation. Such simplified models are amenable to mathematical, analytic methods. However, the general framework has been specifically designed to encompass more general models (for example, with structured sets of rules) and internal loss calculations that are not simple equations. Such models would need to be explored within a simulation tool, rather than exactly solved, as discussed in D6.1.

4.3 Context of the Work

There is a significant body of literature on regulation and transmission, some of which focusses on *reliability* of transmission and some of which involves the construction of models [7, 8, 9, 10, 11]. However, there appears to be little on modelling threats to reliability via information security problems where there is the presence of attack agents (rather than natural hazards) with particular characteristics. The work contained in ANNEX3 thus appears to be

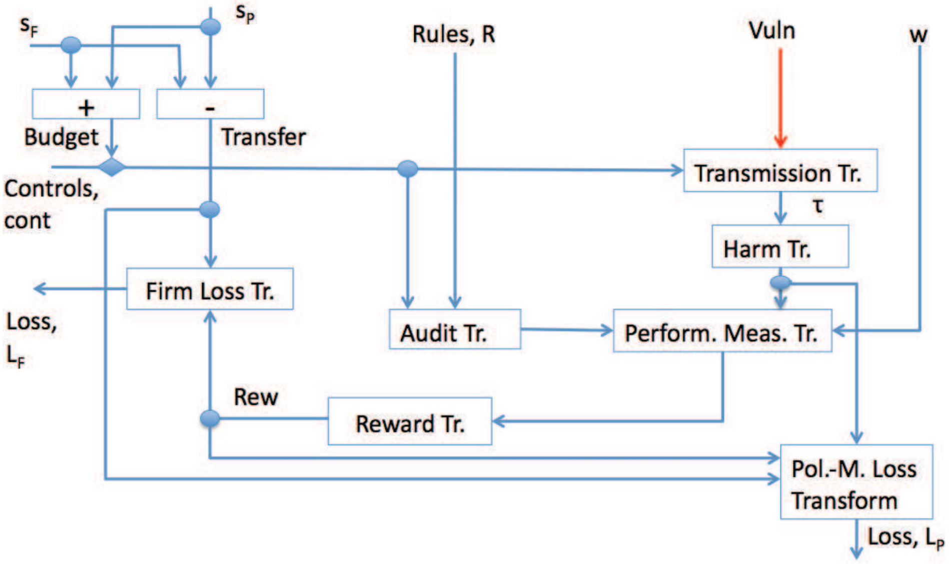


Figure 3: Policy-maker Loss Calculations: Before Stackelberg Equilibriation

timely and well-positioned, but the models and methodology clearly need further refinement.

4.4 Policy Insights

The models that we have are theoretical and have not yet been fully-explored. The insights available at this stage are therefore necessarily somewhat abstract. Briefly, they are:

1. That models *can* capture (interesting and relevant aspects of) the fundamental structure of the objects of policy debate in this area

2. That apparently simple incentive schemes (combining aspects of both risk and rules) set by the policy-maker can lead to complex optimization problems for the firm. This may inadvertently lead to behaviour by the firm which is decidedly not 'pro-social'

3. That the properties of the environment are key to answering the question of rules-versus-risk: for example, the rapidity (or unpredictability) of the evolving threat environment can have a significant impact upon which is more appropriate, since this is material to the informational advantage that the firm has regarding true security risk.

BIBLIOGRAPHY

[1] NERC. Standard CIP-002-4—Cyber Security— Critical Cyber Asset Identification. Available at http://www.nerc.com/files/cip-002-4.pdf (Accessed 12th March 2014).

[2] The President. Executive Order 13636 — Improving Critical Infrastructure Cybersecurity, February 19, 2013. Federal Register, Volume 78, Number 33, Part III http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf. Signed by Barack Obama and dated February 12th 2013. (Accessed 10th March 2014).

[3] Executive Office of the President and President's Council of Advisors on Science and Technology. Immediate opportunities for strengthening the nation's cybersecurity. November 2013. Available at http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf (accessed 3rd March 2014).

[4] R. Langner and P. Pederson. Bound to fail: Why cyber security risk cannot simply be "managed" away. The Brookings Institution. February 2013. Available at http://www.brookings.edu/~/media/research/files/papers/2013/02/cyber-security-langner-pederson/cybersecurity_langner_pederson_0225.pdf and http://www.langner.com/en/wp-content/uploads/2013/06/Bound-to-fail.pdf (both accessed 10th March 2014).

[5] Russell Cameron Thomas. Mr Langner is wrong. Risk management isn't 'bound to fail'. But it does need improvement and innovation., September 8, 2013. Posted to http://exploringpossibilityspace.blogspot.co.uk/2013/09/mr-langner-is-wrong-risk-management.html (accessed 18th March 2014).

[6] NIST. Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014. Version 1.0. Available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (accessed 18th March 2014).

[7] The Regulatory Assistance Project (RAP). Electricity Regulation In the US: A Guide, March 2011. Available at http://www.raponline.org/Fdocs/RAP_Lazar_ElectricityRegulationInTheUS_Guide_2011_03.pdf (accessed 18th March 2014).

[8] Paul L. Joskow. Incentive Regulation in Theory and Practice: Electricity Distribution and Transmission Networks. In Nancy L. Rose, editor, *Economic Regulation and Its Reform: What Have We Learned?* University of Chicago Press, 2014. To appear. Draft paper available at http://www.nber.org/chapters/c12566.pdf and draft of the book http://papers.nber.org/books/rose05-1 (both accessed 18th March 2014).

[9] I. Vogelsang. Electricity transmission pricing and performance-based regulation, May 2005. CESifo Working Paper No. 1474 Category 9: Industrial Organization. Available at http://hdl.handle.net/10419/18838 (accessed 18th March 2014).

[10] MIT Energy Initiative. *The Future of the ElectricGrid: An Interdisciplinary MIT Study*. MIT, 2011. ISBN 978-0-9828008-6-7. Available at http://mitei.mit.edu/system/files/Electric_Grid_Full_Report.pdf (accessed 18th March 2014).

[11] T. Jamasb and R.Nepal. Issues and Options in the Economic Regulation of European Network Security. Technical report, 2014. (Energy Policy research Group) EPRG Working Paper 1405. Cambridge Working Paper in Economics. EC FP7 SESAME

Project. Available at http://www.eprg.group.cam.ac.uk/wp-content/uploads/2014/03/1405-PDF.pdf (accessed 8th March 2014).

[12] EU Communication from the Commission to the Council and Brussels. the European Parliament. Critical Infrastructure Protection in the Fight against Terrorism. Technical Report COM(2004) 702 final.

[13] Brussels EU Green Paper on Energy Policy, Commission of the European Communities. A European Strategy for Sustainable, Competitive and Secure Energy. Technical Report Com SEC(2006), 2006.

[14] Communication on a European Programme for Critical Infrastructure Protection. Technical Report [COM/2006/786], .

[15] Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Technical report, . URL Availableat:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

[16] Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection. Technical report, 2012. URL http://ec.europa.eu/energy/infrastructure/doc/20121114_tnceip_eupolicy_position_paper.pdf.

[17] the European Economic Joint Communication to the European Parliament, the Council, Social Committed, and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Technical report, 2013. URL http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.

[18] Summaries of EU legislation. Technical report, . URL http://europa.eu/legislation_summaries/transport/air_transport/tr0026_en.htm.

[19] US Govt. Executive Order 13636–Improving Critical Infrastructure Cybersecurity. Technical Report Federal Register, Vol. 78 No. 33, February 19, 2013, 2013.

[20] HR 3696 the National Cybersecurity and Critical Infrastructure Protection Act of 2013. Technical report, . URL http://www.loc.gov/search/?q=security+infrastructure+protection&in=original-format%3Alegislation.

[21] D. J. Pym, J. Swierzbinski, and J. Williams. The need for public policy in information security. Working draft at http://www.cs.ucl.ac.uk/staff/D.Pym/InfoSecPubPol.pdf, 2013.

[22] C. Ioannidis, D. J. Pym, and J. M. Williams. Sustainability in information stewardship: Time preferences, externalities, and social co-ordination. In *The Twelfth Workshop on the Economics of Information Security (WEIS 2013)*, 2013. Available at: http://weis2013.econinfosec.org/papers/IoannidisPymWilliamsWEIS2013.pdf.

[23] H. Kunreuther, J. Linnerooth, P. Knez, and R. Yaksick. *Risk Analysis and Decision Processes: The Siting of Liquified Energy Gas Facilities: in Four Countries*. Springer–Verlag, London, 1985.

[24] K. Arrow. *Behavior Under Uncertainty and Its Implications for Policy*. Institute for Mathematical Studies in the Social Sciences, Stanford University, 1983.

[25] H. Bohn and R. T. Deacon. Ownership risk, investment, and the use of natural resources. *American Economic Review*, 90(3):526–549, 2000.

[26] R. Benabou and J. Tirole. Incentives and prosocial behavior. *American Economic Review*, 96(5):1652–1678, 2006.

[27] J. Baldwin, G. Gellatly, M. Tanguay, and A. Patry. Estimating depreciation rates for the productivity accounts. Technical report, OECD Micro-Economics Analysis Division Publication, 2005.

[28] NERC Publications. Second draft 2014 business plan and budget. Technical report, North American Electric Reliability Corporation, 2013.

[29] FERC Policy Statement. Smart grid policy. Technical report, Federal Energy Regulatory Commission, 2009.

[30] Executive Office of the President. Economic Benefits of Increasing Electric Grid Resilience to Weather Outages. Prepared by the President's Council of Economic Advisers and the U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability, with assistance from the White House Office of Science and Technology. August 2013. Available at http://energy.gov/sites/prod/files/2013/08/f2/Grid Resiliency Report_FINAL.pdf (Accessed 10th March 2014).

[31] R. Gold. Cybersecurity for critical infrastructure, or 'how to break into a nuclear power station for fun & profit'. Slides from a talk given at the University of Andrews School of Computer Science on 18th February 2014. Available at http://saleem.host.cs.st-andrews.ac.uk/seminars/20140218_richard_gold/20140218_richard_gold.pdf (accessed 3rd March 2014).

[32] C. Bronk. Hacks on Gas (and the Grid): Cybersecurity, Energy and National Defense. *Forbes*, 2014. http://www.forbes.com/sites/thebakersinstitute/2014/02/05/hacks-on-gas-and-the-grid-cybersecurity-energy-and-national-defense/ (Accessed 10th March 2014).

[33] ENTSO-E. Network code on operational security, 24 September 2013. Available at https://www.entsoe.eu/fileadmin/user_upload/_library/resources/OS_NC/130924-AS-NC_OS_2nd_Edition_final.pdf.

[34] ENTSO-E. Supporting document for the network code on operational security, 24 September 2013. 2nd Edition Final. Available at https://www.entsoe.eu/fileadmin/user_upload/_library/resources/OS_NC/130924-AS-NC_OS_Supporting_Document_2nd_Edition_final.pdf.

[35] Ross Anderson and Shailendra Fuloria. Security economics and critical national infrastructure. In *Economics of Information Security and Privacy*, pages 55–66. Springer, 2010.

[36] ISO/IEC 27000:2014. Information technology — Security techniques — Information security management systems — Overview and vocabulary, 2014. http://www.iso.org/.

[37] IT Governance Institute. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. ISACA, 2012. ISBN 978-1-60420-237-3. http://www.isaca.org/cobit.

[38] Matlab2012a. MATLAB and Statistics Toolbox Release 2012a, The MathWorks, Inc., Natick, Massachusetts, United States.

[39] Simulink. The MathWorks, Inc., Natick, Massachusetts, United States. Available at http://www.mathworks.co.uk/products/simulink/.

[40] C. Ioannidis, D. Pym, and J. Williams. Investments and trade-offs in the economics of information security. In *Proc. Financial Cryptography and Data Security 2009*, volume 5628 of *LNCS*, pages 148–162. Springer, 2009.

[41] C. Ioannidis, D. Pym, and J. Williams. Fixed costs, investment rigidities, and risk aversion in information security: A utility-theoretic approach. In Bruce Schneier, editor, *In Economics of Security and Privacy III*, pages 171–192. Springer, 2012.

[42] C. Ioannidis, D. Pym, and J. Williams. Security trade-offs and optimal patching policies. *European Journal of Operational Research*, 216(2):434–444, 2012.

[43] C. Ioannidis, D. Pym, and J. Williams. Sustainability in information stewardship: Time preferences, externalities, and social co-ordination. Presented at The Twelfth Workshop on the Economics of Information Security (WEIS 2013). Manuscript available at http://www0.cs.ucl.ac.uk/staff/D.Pym/sustainability.pdf (Accessed 10th March 2014).

[44] I. Gheyas, C. Ioannidis, D. Pym, and J. Williams. Resilience in information stewardship. Available at: http://www0.cs.ucl.ac.uk/staff/D.Pym/IoannidisPymWilliamsGheyas-Resilience.pdf (accessed 10th March 2014), 2014.

[45] D. Pym, J. Swierzbinski, and J. Williams. The Need for Public Policy Interventions in Information Security. Available at http://www0.cs.ucl.ac.uk/staff/D.Pym/InfoSecPubPol.pdf (accessed 10th March 2014).

Annexes

ANNEX1. Review of Current Legal Instruments for Protecting Critical Infrastructure

In the post-war period the development of regulation for the protection of national infrastructure has developed at an astounding pace. The core set of regulations that led to the development of FERC and NERC in the 1960s and 1970s have been almost completely overhauled since September 11, 2001 and most national regulatory mechanisms in the European Union have been restructured since the Lisbon Treaty in December 2007. This paper reviews the current set of regulatory instruments in the US and the EU and their mechanisms of action. The critical aspects of this review is in documenting clearly the various important developments in this area. We focus on legal instruments that have mandated actions rather than those which set out advisory or coordination roles for governmental bodies.

A tenet of the work in WP6 is in identification of areas of regulatory authority and characterising their modality of operation relative to the Annexes in this document. Current approaches to aviation security are covered in D6.3. The discussion in this Annex will focus on Energy regulation, however much of the regulatory instruments reviewed are applicable to transport and Appendix ANNEX1.5 outlines the full set of legal structures considered in this summer. The remainder of this paper is organised as follows: §(ANNEX1.1) provides an overview of legal topics related to critical infrastructure. §(ANNEX1.2) relates the current EU approach to protecting critical infrastructure and the manner in which these regulatory mechanisms are filtered to individual members. §(ANNEX1.3) presents an overview of the US approach to Energy infrastructure protection and provides motivation for the other Annexes in this document. Finally, §(ANNEX1.4) provides some comparison and concluding remarks. An Appendix ANNEX1.5 that covers: all of the relevant legal instruments in this area for the US and the EU for five years, plus relevant legacy laws dating back to 1996 is also provided.

ANNEX1.1 Securing Critical Infrastructure

Damage to or discontinuity of critical energy infrastructure (CEI) can have far reaching catastrophic economic, political and social repercussions. Hence, Critical infrastructure protection against all types of hazards has become a major issue in modern society. Critical infrastructure consists of physical and information technology assets. Physical security and cyber security are often intertwined in modern CEI. Since the 1980s utilities increasingly have been using computerized communication systems and networks, primarily SCADA (Supervisory Control and Data Acquisition) and DA (Distribution Automation), to communicate with and control many remote devices on electrical grids. Many of the early SCADA and DA systems that are still in service today were built with legacy or outdated IT systems that lack inbuilt cybersecurity. Hence SCADA and DA honeypots attract swarm of sophisticated hackers with modern tools to breach and manipulate.

Recent technology trends have emphasized the "networking" of all utility computers and control systems for efficiency and collaboration. As more networks are linked, the pathways for cyber spies become myriad and the means of protecting such networks becomes increasingly difficult to maintain. CEI can be an easy target for terrorists. Since post–9/11, both the EU and U.S. have taken on Critical Infrastructure Protection (CIP) initiatives that involve security strategies including prevention, preparedness, and response approach to security incidents. The EU follows a central approach relied on the European Programme for Critical Infrastructure Protection (EPCIP) in CIP in Europe, whereas the US follows voluntary and mandatory guidelines from a range of government and industry agencies.

ANNEX1.2 The EU Approach to Critical Energy Infrastructure Protection (CEIP)

In 2004, the European Commission drafted a communication entitled "Critical Infrastructure Protection in the fight against Terrorism" which offers guidelines and suggestions for prevention of, preparedness for and response to terrorist attacks involving critical infrastructure (CI). Its proposals for Critical Infrastructure Protection (EPCIP) and a Critical Infrastructure Warning Information Network (CIWIN) were adopted by the European Council later that same year. Following a number of seminars and informal expert meetings in 2005, the Commission produced a Green Paper on a European Programme for Critical Infrastructure Protection (EPCIP) in November 2005.

The Green Paper recognized the need for action to address systemic vulnerabilities in critical infrastructures. The threats are seen in terrorism, natural disasters and accidents. Consequently, while the initial focus of the emerging Critical Infrastructure Policy (CIP) was on terrorism, the policy evolved into an all-hazards approach. In December 2006 a policy package on EPCIP was adopted. The package consists of (i) a proposal for a directive – a key element of the EPCIP–on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection.

The Council adopted the Directive in question on 8 December 2008. (ii) a (nonbinding) Communication on a European Programme for Critical Infrastructure Protection, which contains nonbinding measures designed to facilitate the implementation of EPCIP, including an EPCIP Action Plan, the CIWIN (Critical Infrastructure Warning Information Network) network, CIP (Critical Infrastructure Protection) expert groups, CIP information sharing, identification and analysis of sectorial and geographical interdependencies. (iii) Support for Member States concerning National Critical Infrastructure, (iv) Contingency Planning, (v) the development of an External Dimension– External cooperation on CIP will primarily focus on the EU's neighbours, and (v) Accompanying financial measures.

In 2010, the European Commission established the Thematic Network on Critical Energy infrastructure Protection (TNCEIP) as part of the EPCIP in order to ensure a high level of protection for CEI against external threats. This thematic network consists of Europe's energy operators from the gas, electricity and oil sectors. The TNCEIP enables collaboration and common understanding among the energy operators from the gas, electricity and oil sectors. The TNCEIP meets on quarterly basis and discusses topics such as contingency planning in the energy sector, threat assessment, risk management, cyber security and others to facilitate common understanding. The TNCEIP network's basic philosophy is to adopt a common and holistic approach on protecting energy infrastructure of trans-European scale. TNCEIP urges that the convergence of cyber and physical security is essential to set the framework for a unified approach for securing physical and cyberspace. TNCEIP's recommendations include:

(i) the setting up of the Critical Infrastructure Warning Information Network (CIWIN) as a multilevel communication/alert system and an electronic forum for the exchange of CEIP (CEI Protection) ideas and best practices, (ii) continuing and strengthening public-private partnership in general between the European Commission, its member states MS) and relevant stakeholders and operators, (iii)fostering cooperation among MS on emerging security challenges, (iv) development of a common methodology for assessing risks and threats to the energy infrastructure within Europe.

However, the scope of the final Directive (The Directive 2008/114/EC) is limited to the energy and transport sectors. ICT sector is not only a sector in its own right but also a vital support for almost all industries. Hence on 30 March 2009, the Commission adopted its communication on CIIP (Critical Information Infrastructure Protection) under the general framework of the EPCIP. The overall goal of the communication is protecting Europe from large scale cyber-attacks and disruptions. This communication includes an action plan that covers five areas:

(i) preparedness and prevention by creating European Forum for MS to share information and policy practices; by promoting European public private partnership for resilience; and by adopting baseline of capabilities and services for National/Governmental CERTs (Computer Emergency Response Teams), (ii) detection and response through the development of a European Information Sharing and Alert Systems–EISAS dedicated to EU citizens and SMEs, (iii) mitigation and recovery through the following activities: national contingency planning and exercises, Pan-European exercises on large-scale network security incidents, and reinforced cooperation between National/Governmental CERTs, (iv) international cooperation by defining European priorities, principles and guidelines for the long term resilience and stability of the Internet; by promoting the principles and guidelines at global level; and by enhancing global cooperation on exercises on large-scale Internet incidents. (v) Definition of criteria for the identification of European Critical Infrastructures in the ICT sector.

Two years later, in 2011, the commission analysed the results achieved that far and announced follow-up actions in the Communication on CIIP on "Achievements and next steps: towards global cyber-security". In the follow-up communication, the commission calls on member states (MS) to establish a network of well-functioning National/Governmental CERTs, a European cyber-incident contingency plan and regular National and pan-European cyber exercises by 2012 to enhance EU preparedness, security and resilience against major attacks. The commission highlighted the pressing need to make ICT systems and networks resilient and secure to all possible disruptions whether accidental or intentional, and demanded greater European coordination of Internet security and resilience policies. In June 2012, the European Parliament endorsed a resolution on the 2011 communication entitled "Critical Information Infrastructure Protection: towards global cyber security".

On July 4, 2013, the European Parliament adopted new EU legislation to fight cybercrime. At the beginning of 2013 the European Commission launched two major initiatives on cyber security–the EU Cyber Security Strategy and a proposal for a Directive on network and information security. On July 4, 2013, the European Parliament adopted new legislation on the EU cybersecurity strategy. The Directive has yet to be approved by the EU council. The EU cybersecurity strategy promotes Europe's values and interests around the world, establishes norms for responsible behaviour, and fosters the application of existing international laws in cyberspace.

This strategy is also aimed at assisting countries outside the EU with cyber security capacity-building and promoting international cooperation in cyber issues. The proposed directive, along with the Cyber Security Strategy, identifies ?critical infrastructure' sectors that require more protection against cyber threats, including the energy, transport, banking and healthcare sectors. The directive builds on rules that have been in force since 2005 and incorporates into new legislative instruments designed to combat emerging threats including the emergence of large-scale attacks against information systems, and increased criminal use of so-called "botnets", networks of infected computers that can be remotely controlled to stage large-scale, coordinated attacks.

The proposed directive sets tougher penalties for cyber criminals in the EU. For example, the directive sets up a penalty of at least three years' imprisonment for using botnets. In addition the Directive aims to improve European criminal justice and police cooperation by (i) strengthening the existing structure of 24/7 contact points by obliging the EU Member States to react to urgent requests within eight hours, and (ii) requiring the EU Member States to collect basic statistical data on cybercrimes. However there are several important weaknesses in the proposed directive. Two internal memoranda drafted by the European Network and Information Security Agency (ENISA) said that the response teams, or CERTs, are not spreading their detection nets as widely as possible and are failing fully to share their information with one another. Another major problem is that Europe and the United States implement different approaches to cybersecurity, with Washington adopting voluntary reporting mechanisms against Brussels' compulsory measures. The different approaches threaten to create problems for companies across the two major trade blocs.

ANNEX1.3 The US Approach to Critical Energy Infrastructure Protection (CEIP)

In February 2013, the Obama Administration issued an Executive Order (EO) called Improving Infrastructure Cybersecurity, with the ultimate goal of engaging CI owners and operators in developing, promoting and implementing cybersecurity best practices. The EO calls for the development of a voluntary risk-based Cybersecurity Framework–a set of industry standards and best practices to help organizations manage cybersecurity risks. The White House is also considering a series of incentives such as cybersecurity insurance, grants, and liability limitation to encourage the quick adoption of the framework. On February 5, 2014, the House Homeland Security Committee unanimously approved a cybersecurity bill (H.R.396) entitled the National Cybersecurity and Critical Infrastructure Protection Act of 2013 ("NCCIP Act").

The NCCIP builds on many of the ideas set forth in February 2013 Presidential EO on cybersecurity. The bill directs NIST (National Institute Standards and Technology) to develop voluntary best practices that include individual privacy and civil liberty protections. The bill funds the National Cybersecurity and Communication Integration Center (NCCIC). The NCCIC serves as DHS'24 hour cyber and communications watch and warning center. It facilitates situational awareness among all partner organizations and serves as a constantly available cyber incident response and management centre. With approximately 85 percent of critical US infrastructure under private sector control, alliances between government and business are essential for homeland security. Hence, the NCCIP Act establishes an equal partnership between private industry and DHS and ensures that DHS properly recognizes industry-led entities to facilitate critical infrastructure protection and incident response. The NCCIP also amends the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (SAFETY ACT) to provide liability protections for those selling or providing agency-approved cybersecurity technology to customers.

Canada, Mexico and the United States share much of their critical infrastructure. Hence, on December 12, 2001, the U.S. and Canada signed the Smart Border Declaration and the 32-point action plane which is based on four pillars: the secure flow of people, the secure flow of goods, secure infrastructure, and information sharing and coordination in the enforcement of these objectives. Similarly the U.S. and Mexico signed The U.S.-Mexico Border Partnership Declaration on March 22, 2002, in Monterrey, Mexico, to develop the Framework of Cooperation for Critical Infrastructure Protection (CIP). Under this framework, the government of Mexico and the United States share the commitment to protect their populations and critical infrastructure from terrorist attacks, natural disasters and any other eventuality that may compromise their integration and operation.

Following the Northeast Blackout of 2003, the North American Electric Reliability Corporation (NERC) was established to ensure the reliability of the bulk power system in North America. NERC develops and enforces reliability standards; monitors the bulk power system; assesses and reports on future transmission and generation adequacy; and educates trains and certifies industry personnel. It coordinates critical infrastructure protection and cybersecurity and facilitates the exchange of information among the eight regional reliability organizations. The members of the eight regional organizations come from all segments of the electricity industry, including investor-owned utilities; federal power agencies; rural electric cooperatives; state, municipal and provincial utilities; independent power producers; power marketers, and end-user customers. These entities account for virtually all the electricity supplied in the United States, Canada and a portion of Mexico. If a power company is found to be non-compliant with NERC reliability standards, enforcement actions include NERC-overseen rectification of the non-compliant company's issues, as well as fines levied on a sliding scale, proportional to the company's degree of non-compliance.

ANNEX1.4 Conclusions

EU and US legislation have many of the same objectives, however the threat balance is somewhat different and as such this has impacted the legislative approaches to infrastructure legislation. The objective of this section is to provide a comprehensive summary of the current state of the these legal instruments and their deployment across the areas of interest. We see that the EU structure has tended to be state led, and has a high level of coordination and best practice associated with it. The actual implementation tends to happen at the member state level. The US approach tends to set high level across the board rules and then set states with the task of providing audit of those rules. The EU approach to liability is unclear and as such unless or until a major event occurs the mechanisms for distribution and recovery are based on the relatively narrow risk assessment within the various directives. US legislation is very different. In Table ANNEX1.5 we document many pieces of primary US legislation with security either as the main focus or one of the key elements. Liability definitions are very specific and costings are incorporated into the legal framework, therefore contractual elements have been built in to provide cost sharing of risks. This may prove an interesting domain of research for future application of US style regulation to the EU.

ANNEX1.5 Appendix: List of Legal and Regulatory Instruments

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2001	Directive 2001/77/EC of the European Parliament and of the Council of 27 September 2001 on the promotion of electricity from renewable energy sources in the internal electricity market	Energy security	Enacted regulation	EU	The promotion of electricity from renewable energy sources (RES) is a high European Union (EU) priority for several reasons, including the security and diversification of energy supply, environmental protection and social and economic cohesion. The Directive follows up the 1997 White Paper on renewable energy sources which set a target of 12% of gross inland energy consumption from renewables for the EU-15 by 2010, of which electricity would represent 22.1%. With the 2004 enlargement, the EU?s overall objective became 21%. The Directive also constitutes an essential part of the package of measures needed to comply with the commitments made by the EU under the Kyoto Protocol on the reduction of greenhouse gas emissions. European companies are currently among the world leaders in developing new technologies connected with RES electricity. The Directive aims to give a boost to stepping up the contribution of these energies while respecting the principles of the internal market. The Directive concerns electricity produced from non-fossil renewable energy sources such as wind, solar, geothermal, wave, tidal, hydroelectric, biomass, landfill gas, sewage treatment gas and biogas energies. The definitions in Directive 96/92/EC concerning common rules for the internal market in electricity are also applicable to this Directive. **The Member States which joined the EU in 2004 must apply the provisions of Directive 2001/77/EC on producing electricity from renewable energy sources. Their Accession Treaty sets national indicative targets for the proportion of electricity produced from RES (RES-E) in each new Member State the result of which is an overall objective of 21% for the EU-25.** The Member States must adopt and publish, initially every five years, a report setting the indicative Member State targets for future RES-E consumption for the following ten years and showing what measures have or are to be taken to meet those targets. The Member State targets must take account of the reference values set out in the Annex to the Directive for Member States' indicative targets concerning the share of electricity produced from renewable energy sources in gross electricity consumption in 2010. They must also be compatible with all the national commitments entered into as part of the commitments accepted by the Community in Kyoto.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2003	1230/2003/EC	Energy security	Enacted regulation	EU	**Energy and transport play a large part in climate change since they are the leading sources of greenhouse gas emissions; this is why energy policy is particularly important in the European Union's sustainable development strategy.** The EU is increasingly dependent on energy imported from Non-EU Member Countries, creating economic, social, political and other risks for the Union.The EU therefore wishes to reduce its dependence and improve its security of supply by promoting other energy sources and cutting demand for energy. Consequently, it is putting the accent, above all, on improving energy efficiency and promoting renewable energy sources. This programme ensures the continuity of EU action as developed in the previous energy framework programme (1998-2002).This new programme is aimed at providing financial support for local, regional and national initiatives in the field of renewable energy, energy efficiency, the energy aspects of transport, and international promotion. The budget is 200 million for the period 2003-2006.The specific aims are: (i)- to provide the necessary factors to promote energy efficiency and develop renewable energy sources with a view to reducing energy consumption and CO2 emissions; (ii)- to develop resources and instruments which can be used by the Member States to monitor and evaluate the impact of the measures adopted by the Member States; (iii)- to promote efficient and intelligent schemes for the production and consumption of energy, based on solid and sustainable foundations, through awareness-raising and education.To achieve these aims, the programme must ensure that there is a real change in energy behaviour in the EU on the part of individuals as well as industry and enterprise. **It must also develop instruments to ensure effective follow-up, monitoring and evaluation. The programme is divided into four fields, some of which match the earlier programmes to provide and reinforce continuity: (1) The SAVE field, which is concerned with improving energy efficiency and the rational use of energy, in particular in the construction sector and industry. Budget: 69.8 million; (2)The ALTENER field, which is concerned with the promotion of new and renewable energy for the centralised and decentralised production of electricity and heat, and their integration into the local environment and energy systems. Budget: 80 million; (3)The STEER field, which is concerned with supporting initiatives relating to the energy aspects of transport and fuel diversification by using renewable energy sources. Budget: 32.6 million;(4)The COOPENER field, which is concerned with supporting initiatives for the promotion of renewable energy and energy efficiency in developing countries. Budget: 17.6 million.** The programme is structured around key actions for each field of action and funding is directed towards measures or projects concerned with: (i)promotion of sustainable development, security of energy supply, competitiveness and environmental protection. Projects may include the development of standards and of labelling and certification systems and the monitoring of developments on the markets and energy trends; (ii)creation, enlargement and promotion of structures and instruments for sustainable energy development, such as local and regional energy management, and the development of financial products; (iii)promotion of systems and equipment in order to speed up market penetration by the best available technologies; (iv)development of information, education and training structures to raise public awareness and dissemination of know-how and best practices; (v)monitoring of the implementation and impact of EU sustainable energy policy; (vi)evaluation of the impact of projects funded under the programme.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2003	Directive 2003/55/EC	Energy security	Enacted regulation	EU	Directive 2003/55/EC provides for the complete opening of national gas markets to competition and therefore helps create a true internal gas market within the European Union (EU). Completion of the internal gas market increases competitiveness and improves service quality, guarantees fair prices for consumers, establishes rules on public service obligations, improves interconnection and bolsters security of supply. Directive 2003/55/EC lays down the right of third parties to non-discriminatory access to transmission and distribution systems and to liquefied natural gas (LNG) facilities. Consequently, new suppliers can now enter the market and consumers are free to choose their gas supplier. For the internal gas market to operate properly, all the companies, even the smallest ones, such as those which invest in renewable energy sources, must be able to enter the market. Fair competition conditions must be put in place to prevent the risk of dominant positions, in particular of the traditional operators, and predatory behaviour. A gradual approach has been adopted so that companies can adapt whilst guaranteeing the protection of consumers? interests. Since 1 July 2004, industrial consumers have been able to choose their supplier. Domestic consumers have had had this opportunity since 1 July 2007. Access to storage facilities is covered by specific provisions by virtue of which access may be either negotiated or regulated. In each Member State, system operators are appointed for the transmission system on the one hand, storage, liquefied natural gas and the distribution system. Their mission is the operation, maintenance and development of transmission and distribution, storage and liquefied natural gas (LNG) facilities. They are obliged to ensure the safety, reliability, efficiency and interconnection of facilities with due regard for the environment. System operators must guarantee non-discriminatory and transparent access to the system for all users. Access must therefore be based on fair tariffs that are applied objectively. **System operators may not favour certain companies, in particular any with which they are associated. In order to avoid any discrimination relating to network access and enable equal access for new entrants, when companies are vertically integrated, the transmission and distribution activities must be legally and functionally separate from other activities, such as production and supply. This separation does not, however, mean ownership unbundling.** System operators are also obliged to provide other operators with the information necessary for safe and effective running of the interconnected system. The internal gas market can only become a reality if consumers play an active role and actually exercise their right to free choice of their gas supplier. It is therefore essential for operation of the internal gas market to inform consumers of their rights and to ensure their effective protection. Directive 2003/55/EC lays down common minimum standards to ensure a high level of consumer protection (the right to change supplier, transparent contract conditions, general information, dispute settlement mechanisms, etc.) and takes particular care to provide adequate protection of vulnerable consumers (for example, by taking the appropriate steps to avoid disconnection of the gas supply). Gas supply is considered as a public interest service that citizens have the right to access in return for payment. Therefore, the Directive provides for the possibility for Member States to impose public service obligations to guarantee security of supply, economic and social cohesion objectives, regularity, quality and price of the gas supply and protection of the environment.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2006	Mobilising public and private finance towards global access to climate-friendly, affordable and secure energy services: The Global Energy Efficiency and Renewable Energy Fund" [COM(2006) 583 final - Not published in the Official Journal].	Energy security	proposed regulation	EU	The Global Energy Efficiency and Renewable Energy Fund (GEEREF) proposed by the European Commission will help mobilise private investments in energy efficiency and renewable energy projects. Boosting such projects will substantially contribute towards sustainable development. It will provide benefits in terms of the environment, climate change and air quality and will also have social and economic benefits in terms of business, job and income creation at local level. It will also help to stabilise energy supply in the poorest regions of the world. Boosting renewable energy and energy efficiency technology calls for investment, in particular in developing countries and emerging economies. Although the prospects are promising, several factors block the participation of private-sector investors and projects and businesses have major difficulties in raising risk capital, which provides vital collateral for lenders. One of the key reasons causing this block to investments is the significantly higher cost of initial investment in renewable energy generation than for conventional energy. While these costs are compensated by much lower running costs, private-sector investors still regard the longer repayment periods as too risky. The various risks in developing countries are another hurdle, which means that investors look for additional reassurances. Moreover, renewable energy technologies are often suited to small and medium sized projects with less than 5-10 million in total capital, whilst international finance institutions and the private sector traditionally do not invest in such small-scale projects. The GEEREF will establish a public-private partnership by offering ways of risk sharing and co-financing for projects investing in renewable energy and energy efficiency. It will mainly target the raising of "patient" risk capital, in other words, capital invested with a long-term prospect of return on the investment. GEEREF participation will range from between 25 and 50 % for medium to high-risk operations to 15 % for low-risk operations. Provision will also be made for dedicated technical assistance funds. Rather than providing finance directly to projects, GEEREF will help create and fund regional sub-funds or scale up similar existing initiatives. Sub-funds will accommodate the specific conditions and needs of each region.
2006	The support of electricity from renewable energy sources" [COM(2005) 627	Energy security	Enacted regulation	EU	The Commission stresses that the market is dominated by one or several power companies that are too often vertically integrated. The existence of distribution and transport grid operators should guarantee all generators fair grid access, respecting the rules of competition. That is why the independence of these grid operators is vital to the proper functioning of the support schemes. Governments must also ensure that consumers are informed of the way in which these support schemes for renewable energies affect consumers. A distinction needs to be made between the physical trade in electricity and the green value of the electricity. **RES-E is subject to the same restrictions as conventional electricity, including the mandatory disclosure system. This system makes it compulsory to inform consumers of the contribution of each energy source to the overall fuel mix. The support covered by the Community framework for State aid for environmental protection may distort competition. These economic effects may however be justified and compensated for by the beneficial effects for the environment. Since the use of renewable energy sources is a priority for Community policy, the mentioned framework tends to favour support schemes. Some sixty support schemes for RES-E were already approved by the Commission during the period 2001 to 2004.**

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2007	COM(2006) 848	Energy security	Enacted regulation	EU	The Road Map sets out the Commission's long-term strategy for renewable energy in the European Union (EU). The aim of this strategy is to enable the EU to meet the twin objectives of increasing security of energy supply and reducing greenhouse gas emissions. An assessment of the share of renewable energy in the energy mix and the progress made in the last 10 years shows that more and better use could be made of renewables. In the Road Map, the Commission proposes setting a mandatory target of 20% for renewable energy's share of energy consumption in the EU by 2020 and a mandatory minimum target of 10% for biofuels. It also proposes creating a new legislative framework to enhance the promotion and use of renewable energy.
2008	Regulation (EC) No 216/2008 of the European Parliament and of the council of 20 Feb 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency	Civil Aviation	Enacted regulation	EU	The regulation applies to the production, maintenance and operation of aircraft, as well as to personnel and organisations involved in these activities. **It aims to: (1) establish common rules on aviation safety in order to guarantee a high level of passenger security and ensure that the environment is protected; (2) ensure a level playing field for all stakeholders in the internal aviation market and facilitate the free movement of goods, persons and services through the recognition of certificates issued by the competent authorities; (3) simplify and enhance the efficiency of the certification process, by centralising activities at European level where possible; (4) promote the European Union's (EU) views on civil aviation safety standards and rules all over the world.**
2008	2008/98/EC	Environmental Protection	Enacted regulation	EU	This Directive establishes a legal framework for the treatment of waste * within the Community. It aims at protecting the environment and human health through the prevention of the harmful effects of waste generation and waste management. **It applies to waste other than: (i)gaseous effluents;(ii)radioactive elements;(iii)decommissioned explosives; (iv) faecal matter; (v)waste waters; (vi)animal by-products;(vii)carcasses of animals that have died other than by being slaughtered;(viii)elements resulting from mineral resources.** Any producer or holder of waste must carry out their treatment themselves or else must have treatment carried out by a broker, establishment or undertaking. Member States may cooperate, if necessary, to establish a network of waste disposal facilities. This network must allow for the independence of the European Union with regard to the treatment of waste. Dangerous waste must be stored and treated in conditions that ensure the protection of health and the environment. They must not, in any case be mixed with other dangerous waste and must be packaged or labelled in line with international or Community regulations. Any establishment or undertaking intending to carry out waste treatment must obtain a permit from the competent authorities who determine notably the quantity and type of treated waste, the method used as well as monitoring and control operations. Any incineration or co-incineration method aimed at energy recovery must only be carried out if this recovery takes place with a high level of energy efficiency.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2009	Directive 2009/28/EC	Energy security	Enacted regulation	EU	This Directive establishes a common framework for the production and promotion of energy from renewable sources. Each Member State has a target calculated according to the share of energy from renewable sources in its gross final consumption for 2020. This target is in line with the overall '20-20-20' goal for the Community. Moreover, the share of energy from renewable sources in the transport sector must amount to at least 10 % of final energy consumption in the sector by 2020. **The Member States are to establish national action plans which set the share of energy from renewable sources consumed in transport, as well as in the production of electricity and heating, for 2020. These action plans must take into account the effects of other energy efficiency measures on final energy consumption (the higher the reduction in energy consumption, the less energy from renewable sources will be required to meet the target). These plans will also establish procedures for the reform of planning and pricing schemes and access to electricity networks, promoting energy from renewable sources.** Member States can ?exchange? an amount of energy from renewable sources using a statistical transfer, and set up joint projects concerning the production of electricity and heating from renewable sources. It is also possible to establish cooperation with third countries. The following conditions must be met: (i)the electricity must be consumed in the Community; (ii)the electricity must be produced by a newly constructed installation (after June 2009); (iii)the quantity of electricity produced and exported must not benefit from any other support.
2010	Regulation (EU) No 996/2010 of the European Parliament and of the Council of 20 October 2010 on the investigation and prevention of accidents and incidents in civil aviation and repealing Directive 94/56/EC.	Civil Aviation	Enacted regulation	EU	This regulation establishes an obligation for each EU country to investigate every accident or serious incident which occurs on its territory and involving an aircraft. The sole objective of this investigation is to prevent future accidents and incidents in civil aviation and not not to apportion blame or liability. A national safety investigation authority from one EU country may request the assistance of other EU national safetyinvestigation authorities.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2011	Setting up an Aviation Safety Management System for Europe [COM(2011)670]	Civil Aviation	proposed regulation	EU	The current system for ensuring aviation safety in the European Union (EU) is predominantly based on a set of rules, overseen by the European Aviation Safety Agency (EASA) and National Aviation Authorities (NAA). These rules have evolved over many years of experience and have delivered a very good safety record for aviation in Europe. **However, the International Civil Aviation Organisation (ICAO) has recognised that as the aviation system becomes more complex and more is understood about the limitations of human performance and the impact of organisational processes, simple regulation is no longer sufficient. It is necessary to evolve from a reactive system where regulations are changed as a result of experience towards a pro-active system which attempts to anticipate potential safety risks in order to reduce the likelihood of an accident. The ICAO therefore introduced the need for a safety management system. A safety management system is a pro-active system that identifies the hazards to the activity, assesses the risks those hazards present, and takes action to reduce those risks to an acceptable level. It then checks to confirm the effectiveness of the actions and works continuously to ensure any new hazards or risks are quickly identified and mitigated.** The EU safety management system will support the efforts of the EU countries and not replace them. It will depend on the assistance, cooperation and contributions of the EU countries and the EU aviation industry.Requires the Assistant Secretary to chair an interagency working group, which shall: (1) develop risk- and performance-based cybersecurity requirements for civilian federal agency computer networks and federally owned critical infrastructure, to be enforced by the Assistant Secretary through the Director; (2) develop remedies for noncompliance with such requirements, to be executed by the Director of the Office of Management and Budget (OMB); (3) recommend budgets for security of such networks; and (4) propose updates for the Common Criteria for Information Technology Security Evaluation.
2011	Energy Efficiency Plan 2011 [COM(2011) 109	Energy security	Enacted regulation	EU	The Energy Efficiency Plan 2011 forms part of the European Union?s (EU) 20 % target (aimed at reducing primary energy consumption) and the 2020 Energy strategy. It aims at: (i)promoting an economy that respects the planet?s resources;(ii)implementing a low carbon system;(iii)improving the EU?s energy independence;(iv)strengthening security of energy supply.In order to meet these objectives, the European Commission proposes to act at different levels.
2013	Cyber Security Directive	Cyber security	proposed regulation	EU	The strategy aims to create an open, safe and secure cyberspace and combat cubercrime by introducing minimum requirements for NIS (Network and Information Security) across Europe. Unlike existing security breach notification requirements for the telecoms sector, the proposed Cyber Security Directive will require notification of potential security risks. It will also require actual incidents to be reported to cyber security authorities that will be established across Europe.
1995	H.R,564– Infrastructure Protection Act 0f 1995	Infrastructure Protection	Enacted regulation	U.S.	Infrastructure Protection Act of 1995 - Prohibits the receipts and disbursements of the Highway Trust Fund (for both the Federal aid highway program and the Mass Transit Account), the Airport and Airway Trust Fund, the Inland Waterways Trust Fund, and the Harbor Maintenance Trust Fund which are allocable to the transportation-related operations of such Funds from being included in either the Federal budget as submitted by the President or in the congressional budget. Exempts such Trust Funds from any general statutory budget limitation.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
1996	S.982–National Information Infrastructure Protection Act of 1996	Infrastructure Protection	Enacted regulation	U.S.	National Information Infrastructure Protection Act of 1996 - Revises Federal criminal code provisions regarding fraud and related activity in connection with computers. Sets penalties with respect to anyone who having knowingly accessed a computer without authorization or exceeding authorized access, obtains specified restricted information or data, and, with reason to believe that such information could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, or transmits it to any person not entitled to receive it (or causes or attempts such communication) or willfully retains it and fails to deliver it to the U.S. officer or employee entitled to receive it. Sets penalties for: (1) intentionally accessing a computer without authorization or exceeding authorized access and thereby obtaining information from any U.S. department or agency, or from any protected computer if the conduct involved an interstate or foreign communication; (2) intentionally accessing, without authorization, any nonpublic computer of a U.S. department or agency that is exclusively for use by or for the U.S. Government or, in the case of a computer not exclusively for such use, that is used by or for the U.S. Government if such conduct affects the use of the Government's operation of such computer; (3) knowingly and with intent to defraud, accessing a protected computer without authorization, or exceeding authorized access, and furthering the intended fraud and obtaining anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any one-year period; (4) knowingly causing the transmission of a program, information, code, or command, and, as a result, intentionally causing damage without authorization to a protected computer, intentionally accessing a protected computer without authorization and recklessly causing damage, or intentionally accessing a protected computer without authorization and causing damage; and (5) with intent to extort from any person or legal entity any thing of value, transmitting in interstate or foreign commerce any communication containing a threat to cause damage to a protected computer. Increases penalties for fraud and related activity in connection with computers. (Sec. 3) Amends the Federal criminal code to authorize the transfer of all persons who have been found not guilty by reason of insanity and who have been committed to a hospital for the mentally ill under the District of Columbia Code and for whom the United States has continuing financial responsibility to the custody of the Attorney General, who shall hospitalize such persons for treatment in a suitable facility. Authorizes the Attorney General to establish custody over such persons by filing an application in the United States District Court for the District of Columbia, subject to specified requirements. Requires the court, upon such application, to order the transfer of custody unless it finds that the proposed transfer would violate such person's rights under the Constitution. Sets forth provisions regarding: (1) the transfer of records pertaining to such persons from the District of Columbia or St. Elizabeth's Hospital to the Attorney General; and (2) certain testimonial privileges (not affected by this Act). (Sec. 4) Requires the Director of the Bureau of Justice Assistance to provide grants to the Boys and Girls Clubs of America to establish Boys and Girls Clubs in public housing projects and other distressed areas. Grants the Secretary of Housing and Urban Development contracting authority to establish such clubs. Sets forth reporting requirements. Authorizes appropriations. Makes sums authorized to be appropriated under this section available from the Violent Crime Reduction Trust Fund.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2000	S.2448 - Internet Integrity and Critical Protacol Infrastructure Protection Act of 2000	Infrastructure Protection	Enacted regulation	U.S.	Internet Integrity and Critical Infrastructure Protection Act of 2000 - Directs the Attorney General (AG) to appoint a Deputy Assistant Attorney General for Computer Crime and Intellectual Property (Deputy Assistant) to: (1) advise Federal prosecutors and law enforcement personnel regarding computer and intellectual property crime; (2) coordinate national and international activities for combating such crime; (3) guide and assist Federal, State, and local law enforcement agencies and personnel, as well as appropriate foreign entities, regarding responses to threats of such crimes; and (4) undertake related coordinating, training, and legislative recommendation activities. Requires the individual who holds the position of head of the Computer Crime and Intellectual Property Section of the Department of Justice to act as the Deputy Assistant until the AG appoints another individual to that Section position. Authorizes appropriations for such Section.(Sec. 3) Amends the Federal criminal code to apply the protection from computer extortion provisions only to persons (currently, also to many other institutions and entities). Provides criminal penalties for engaging in fraudulent access and related activities in connection with protected computers, including: (1) when the offense causes aggregate losses of at least $5,000; (2) when the offense causes the modification or impairment of medical diagnosis, treatment, or care; (3) when the offense causes a physical injury to any person; (4) when the offense causes a threat to public health or safety; or (5) when the offense damages a computer system used by or for a government entity in the administration of justice, national defense, or national security. Increases the prison term for a succeeding conviction of the same offense.(Sec. 4) Requires the criminal and civil forfeiture of any property used in committing such offenses, as well as any property constituting or derived from proceeds from such offense.(Sec. 6) Includes such offenses when committed by juveniles as offenses under which the Attorney General may certify to the appropriate district court a substantial Federal interest in exercising Federal prosecution.(Sec. 7) Includes as a defense against prosecution for a computer offense by a telecommunications provider, subscriber, or other aggrieved person that the person providing the information was responding to the request of a governmental entity.(Sec. 8) Authorizes the Federal interception of wire, oral, or electronic communications for a suspected felony violation relating to computer fraud and abuse.(Sec. 9) Provides for the criminal forfeiture of any replicator or other device used to copy a computer program or computer program documentation or packaging.(Sec. 10) Directs the U.S. Sentencing Commission to amend Federal sentencing guidelines to provide guidelines relating to computer fraud and abuse and the use of encryption in connection with the commission or concealment of criminal acts.(Sec. 11) Requires the Director of the Federal Bureau of Investigation to construct and equip a National Cyber Crime Technical Support Center to serve as the centralized technical resource for Federal, State, and local law enforcement and to provide technical assistance in the investigation of computer-related criminal activities. Requires the Director to develop at least ten regional computer forensic laboratories, and to provide support, education, and assistance for such existing laboratories. Authorizes appropriations.
2001	Aviation and Transportation Security Act (ATSA)	Civil Aviation	Enacted regulation	U.S.	ATSA was created to oversee civil aviation security. The central feature of ATSA is federalization of the nation's transportation security system. According to the provisions contained in ATSA, the under secretary of transportation for security shall provide for the screening of all passengers abd property that will be carried aboard an aircraft. In addtion, for flights and flight segments iriginating in the U.S., the screening shall take place before boarding and such screening shall be carried out by a federal government employee. The screening activity at airports in the U.S. shall be supervised by uniformed federal personnel of TSA. Additionally, to ensure passenger safety and national security, the government shall order the deployment of law enforcement personnel authorized to carry firearms at each airport security screening location.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2001	S.1593–Water Infrastructure Security and Research Development Act	Infrastructure Protection	Enacted regulation	U.S.	Water Infrastructure Security and Research Development Act - Requires the Administrator of the Environmental Protection Agency to establish a program of grants to, and enter into cooperative agreements with, research institutions to improve the protection and security of public water supply systems by carrying out eligible projects concerning technologies and processes that address physical and cyber threats to water supply systems. Requires such projects to: (1) assess security issues; (2) protect systems from a potential threat by developing technologies, processes, guidelines, standards, procedures, real-time monitoring systems, and educational and awareness programs; (3) develop technologies and processes for addressing biological, chemical, and radiological contamination; (4) implement a specified Presidential Decision Directive regarding information sharing; or (5) test and evaluate new technologies and processes. Requires the Administrator to: (1) disseminate information to water supply system s on the results of a project as soon as practicable after they have been evaluated; and (2) report to Congress periodically on this program. Authorizes appropriations. Directs the Administrator, for each of FY 2002 and 2003, to use $20 million to assist small water supply systems in complying with requirements concerning arsenic in drinking water.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2001	H.R.3166 – Rebuild America: Financing Infrastructure Renewal and Security for Transportation Act of 2001	Infrastructure Protection	Enacted regulation	U.S.	Rebuild America: Financing Infrastructure Renewal and Security for Transportation Act of 2001 - Amends the Internal Revenue Code to allow a limited tax credit to holders of qualified Amtrak bonds. Requires Secretary of Transportation approval of qualified Amtrak projects funded by such bonds. Amends Federal rail transportation law to authorize appropriations to the Secretary for Amtrak capital expenditures, including specified tunnel life safety projects, bridges, tracks, and other improvements, and equipment, including acquisition of trainsets and rolling stock. Directs the Secretary to establish a program of capital grants to class II and class III railroads (or with the concurrence of such railroads, to a State or local government) to rehabilitate, preserve, or improve certain railroad track. Amends the Railroad Revitalization and Regulatory Reform Act of 1976 to set forth additional requirements with respect to cohorts of direct loans and loan guarantees for certain railroad rehabilitation and improvement projects. Amends the Federal Water Pollution Control Act to remove certain requirements for States with respect to construction of treatment works under capitalization grant agreements. Directs the Administrator of the Environmental Protection Agency to assist States in establishing simplified procedures for small water systems to obtain assistance under this Act. Requires revolving funds to be used only for providing assistance for activities which have as a principal benefit the improvement or protection of water quality. Provides for an extended repayment period and additional subsidization with respect to loans from revolving funds to financially distressed communities. Amends the Transportation Equity Act for the 21st Century to increase the Federal-Aid Highway program obligation ceiling for FY 2002. Authorizes additional appropriations from the Mass Transit Account and the Highway Trust Fund for FY 2002 for certain formula grants for mass transportation projects, including projects for special needs of elderly individuals and individuals with disabilities and non-urbanized areas. Amends the Internal Revenue Code to raise the $100 transportation fringe benefit limitation (applicable to commuter highway vehicles and transit passes) to $175. Amends Federal aviation law to increase appropriations from the Airport and Airway Trust Fund for FY 2002 for airport planning and airport development, including airport noise compatibility planning and programs. Authorizes additional appropriations for FY 2002 and 2003 for guaranteed loans for ferries using a streamlined process. Authorizes the Secretary to make grants to U.S. port or maritime cargo terminal operators to acquire the best available technology, equipment, or infrastructure. Amends the Public Works and Economic Development Act of 1965, the Appalachian Regional Development Act of 1965, and the Consolidated Farm and Rural Development Act to authorize additional FY 2002 appropriations, respectively, for public works and economic development, Appalachian regional development, and Delta, Mississippi regional development. Authorizes additional FY 2002 appropriations to: (1) carry out construction, operation, and maintenance activities (including security measures) for Corps of Engineers projects; and (2) enhance the security of General Services Administration properties. Amends the John F. Kennedy Center Act to authorize additional appropriations for FY 2002 to enhance the security of: (1) the John F. Kennedy Center for the Performing Arts; and (2) the Smithsonian Institution.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2003	S.1212–A bill to identify certain sites as key resources for protection by the Directorate for Information Analysis and Infrastructure Protection of the Department of Homeland Security, and for other purposes.	Infrastructure Protection	Enacted regulation	U.S.	Amends the Homeland Security Act of 2002 to include under the definition of "key resources," for purposes of protection by the Directorate for Information Analysis and Infrastructure Protection of the Department of Homeland Security, National Park Service sites identified by the Secretary of the Interior as being so universally recognized as symbols of the United States and so heavily visited by the American and international public that such sites would likely be identified as targets of terrorist attacks, including: (1) the Statue of Liberty National Monument in New York Harbor; (2) Independence Hall and the Liberty Bell in Philadelphia, Pennsylvania; (3) the Gateway Arch in St. Louis, Missouri; (4) Mount Rushmore National Memorial in Keystone, South Dakota; and (5) memorials and monuments in the District of Columbia.
2003	S.1043–Nuclear Infrastructure Security Act of 2003	Nuclear Infrastructure Security	Enacted regulation	U.S.	Amends the Internal Revenue Code of 1986 to authorize importation of a machine gun or short-barreled shotgun for transfer to a licensee or certificate holder for purposes of establishing and maintaining an on-site physical protection system and security organization required by Federal law. (Sec. 6) Amends the Atomic Energy Act of 1954 to direct the NRC to: (1) evaluate the security of sensitive radioactive material against security threats; (2) recommend to Congress and the President on actions to provide an acceptable level of security against such threats; (3) revise the system for licensing sensitive radioactive materials; and (4) delegate its authority to implement regulatory programs and requirements to States that enter into agreements with the NRC to perform inspections and other functions on a cooperative basis. (Sec. 7) Redefines byproduct material to include: (1) any discrete source of radium-226 produced, extracted, or converted after extraction for use in a commercial, medical, or research activity; (2) specified material that has been made radioactive by use of a particle accelerator for use in such an activity; and (3) any discrete source of naturally occurring radioactive material, other than source material extracted or converted after extraction for use in such an activity that the NRC determines would pose a threat similar to that posed by a discrete source of radium-226 to the public health and safety or the common defense and security. Instructs the NRC to: (1) promulgate final implementing regulations governing such byproduct material; and (2) prepare and give public notice of a transition plan for State assumption of regulatory responsibility for such material. (Sec. 8) Authorizes the NRC to issue regulations on the unauthorized introduction of dangerous weapons into or upon any facility, installation, or real property subject to NRC licensing or certification. (Sec. 9) Subjects to a criminal penalty any attempt or conspiracy to commit sabotage of nuclear facilities or fuel. (The current standard is intentional or willful attempt.). Establishes a criminal penalty for sabotage: (1) committed during construction of certain NRC facilities if the sabotage could adversely affect public health and safety during facility operation; (2) to any primary facility or backup facility from which a radiological emergency preparedness alert and warning system is activated; or (3) to any radioactive material or other property subject to NRC regulation that, before the date of the offense, the NRC determines is of significance to the public health and safety or to common defense and security. (Sec. 10) Instructs the Attorney General and the NRC to report to Congress on the adequacy of criminal enforcement provisions in the Atomic Energy Act of 1954. (Sec. 11) Amends the Energy Reorganization Act of 1974 to extend whistleblower protections to an employee of an NRC contractor or subcontractor. (Sec. 13) Authorizes appropriations.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2006	H.R.5004 - To amend the Homeland Security Act of 2002 to provide for an Office of Intelligence and Analysis and an Office of Infrastructure Protection, and for other purposes.	Infrastructure Protection	Enacted regulation	U.S.	Amends the Homeland Security Act of 2002 to: (1) rename the Directorate for Information Analysis and Infrastructure Protection as the Office of Intelligence and Analysis and the Under Secretary for such Directorate as the Under Secretary for Intelligence and Analysis; (2) expand the intelligence-related duties of the Under Secretary; (3) establish within the Office of Intelligence and Analysis an Internal Continuity of Operations (COOP) Plan to assure the continuation of intelligence operations during emergencies; (4) specify the responsibilities of each intelligence component of the Department of Homeland Security (DHS); and (5) establish an Office of Infrastructure Protection within DHS to be headed by an Assistant Secretary for Infrastructure Protection.
2006	S.2380 - U.S. National Security Protection Act of 2006	National Security Protection	Enacted regulation	U.S.	U.S. National Security Protection Act of 2006 - Revises the structure of the Committee on Foreign Investment in the United States (CFIUS) to: (1) add the Director of National Intelligence and the Director of Central Intelligence as members; (2) designate the Secretaries of Homeland Security and of Defense as vice chairs; and (3) require the President to establish a Subcommittee on Intelligence. Amends the Defense Production Act of 1950 to charge the Subcommittee with the tasks of providing review and comment both before and after investigations authorized or required under the Act to determine the national security effects of mergers, acquisitions, and takeovers ("takeovers," for purposes of this Act) involving foreign persons or foreign government-controlled entities that could result in foreign control of persons engaged in interstate commerce. Includes ownership, control, or operation of critical infrastructure as interstate commerce activity that could affect national security. Requires certification by the President or by the chair of CFIUS (when CFIUS is acting as the President's designee) of a final determination not to proceed with an investigation by the President of a takeover action. Requires persons controlled by or acting on behalf of a foreign government or person to notify the President (or the President's designee) in writing of any proposed takeover of critical infrastructure, providing information necessary to assess national security effects. Requires notice to Congress within 15 days of such notification and at the commencement of an investigation. Requires the President to report quarterly to Congress on all takeovers that were subject to investigation or review during the quarter. Makes CFIUS the President's designee for purposes of the takeover investigation provisions.
2006	H.R.4986 - To amend title 46, United States Code, to require the Secretary of Homeland Security to prioritize maritime transportation security grants based on the risks and vulnerabilities of ports and the proximity of ports to critical infrastructure or urban or sensitive areas.	Infrastructure Protection	Enacted regulation	U.S.	Amends federal shipping law to require the Secretary of Homeland Security to prioritize maritime transportation security grants awarded to port authorities, facility operators, and state and local government agencies required to provide port security based on the risks and vulnerabilities of ports and the proximity of such ports to critical infrastructure or to urban or sensitive areas.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2007	H.R.4177–Airport Security Enhancement Act of 2007	Airport Srcurity	Enacted regulation	U.S.	Amends federal transportation law to authorize the Assistant Secretary of Homeland Security (Transportation Security Administration) to: (1) designate certain airport areas as Federal Security Zones; (2) issue a badge authorizing certain qualified individuals access to suce zones. Restricts access to a Federal Special Security Zone to individuals who require access because of their employment and who have obtained a badge. Prohibits the use of a state issued badge to gain access to Federal Special Security Zone.
2007	H.R.534–Rail Transit Security and Safety Act of 2007	Rail Transit Security and Safety	Enacted regulation	U.S.	Directs the Under Secretary for Border and Transportation Security to complete a vulnerability assessment of freight and passenger rail transportation, and develop specific prioritized recommendations for improving rail security. Diects the Under Secretary to establish the position of Federal Rail Security Manager. Authorizes the Secretary of Transportation to make grants to Amtrack for certain fire and life-safety improvements and infrastructure upgrades to tunnels on the Northeast Corridor. Directs the Secretary of Homeland Security to award grants directly to public transportation agencies for allowable capital and operational security improvements based on the prioritized rail security recommendations. Sets forth whistleblower protections for rail employees or other persons who have provided information or otherwise assisted in any investigation regarding certain conduct, or who have refused to violate or assist in the violation of any regulation related to public transportation security. Directs the Secretary of Homeland Security to make grants to railroad carriers for costs incurred in instituting a rail worker emergency training program.
2007	H.R.535–Rail Worker Emergency Training Act of 2007	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	Directs the Secretary of Homeland Security, in coordination with the Secretary of Transportation, to make grants to railroad carriers for costs incurred in instituting a rail worker emergency training program. Directs the Secretary of Homeland Security to issue detailed guidelines for a rail worker emergency training program to enhance rail worker training in preparation for and response to potential or actual terrorist attacks, natural disasters, and other emergencies. Authorizes the Secretary of Homeland Security to issue a letter of noncompliance to rail carriers that fail to comply with the requirements of this Act.
2007	H.R.33o5–Anti-Terrorism Act of 2007	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	Provides that no federal agency shall prohibit an airline pilot, copilot, or navigator, or law enforcement person specifically detailed for protection of an aircraft, from carrying firearm.
2007	H.R.1079: Professional Driver Background Check Efficiency Act of 2007	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	Amends federal transportation law to revise background records check requirements with respect to the issuance of a moto vehicle license for the transportation of hazardous materials: (1) impose a fee of not more than $50 upon the applicant to cover the costs of the background check, and (2) authorize the costs for such background checks to reimbursed to the state.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2007	H.R.1690–Guaranteeing Airport Physical Screening Standards Act	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	Guaranteeing Airport Physical Screening Standards Act - Directs the Assistant Secretary of Homeland Security (Transportation Security Administration) to: (1) implement a pilot program at five commercial service airports to physically screen all airport workers with access to sterile areas of the airport; (2) issue regulations, directives, or other appropriate measures to implement requirements directing airport perimeter screening of all individuals, goods, property, vehicles, and other equipment before entry into a secured airport area; and (3) set a schedule for requiring airports to update their airport security plans to comply with such perimeter screening requirements. Requires, with respect to the pilot program: (1) at least two of the participating airports to be large hub airports, with each of the remaining airports representing a different airport security risk category; (2) screening to be conducted under the same standards as apply to individuals at airport security screening checkpoints and to be carried out by contract screeners at a minimum of two airports; and (3) that it shall be carried out for not less than 180 days. Authorizes the Secretary of Homeland Security to hire the necessary number of passenger and baggage screeners to ensure aviation security.
2007	H.R.2603–High Threat Helicopter Flight Area Act	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	High Threat Helicopter Flight Area Act - Directs the Secretary of Homeland Security (Secretary) to designate an area at high risk for an attack by one or more terrorists as a high threat helicopter flight area. Directs the Secretary to provide screening of all passengers and property transported from a high threat flight helicopter area on a passenger helicopter equivalent to that provided for passengers and property carried aboard a domestic passenger aircraft. Requires the Secretary to develop a plan for acquiring and training personnel, including acquiring equipment, to provide such screening. Directs the Secretary of Transportation to take necessary action to ensure that: (1) no passenger helicopter flies in a high threat flight area, except on approach for landing, or departure after takeoff, in such area; (2) a passenger helicopter when flying in such area, to the maximum extent practicable, flies over water; and (3) a helicopter pilot when in flight over such area remains in contact with the Federal Aviation Administration (FAA) regarding its flight path, irrespective of its altitude. Exempts from such requirement helicopters carrying out military, police, medical, or other operations as the Secretary of Transportation deems appropriate.
2007	S.575 - Border Infrastructure and Technology Modernization Act of 2007	Infrastructure Protection	Enacted regulation	U.S.	Border Infrastructure and Technology Modernization Act of 2007 - Directs the Under Secretary for Border and Transportation Security (Under Secretary) of the Department of Homeland Security (DHS) to: (1) increase, during FY2008-FY2012, the number of agents and inspectors in the Bureau of Immigration and Customs Enforcement of the DHS; and (2) provide such agents and inspectors new technology training to a level of proficiency acceptable to protect U.S. borders. Directs the Administrator of the General Services Administration (GSA) to update, and submit to Congress, the Port of Entry Infrastructure Assessment Study. Directs the Under Secretary to prepare annually, and submit to Congress, a National Land Border Security Plan that includes a vulnerability assessment of each port of entry located on the U.S. northern and southern borders. Authorizes the Under Secretary to establish one or more port security coordinators at such ports of entry. Directs the Commissioner of the United States Customs and Border Protection of the DHS to: (1) develop a plan to expand Customs-Trade Partnership Against Terrorism programs along the U.S. northern and southern borders; and (2) establish a demonstration program to develop a cooperative trade security system to improve supply chain security. Directs the Under Secretary to carry out a technology demonstration program to test and evaluate new port of entry technologies that enhance port of entry inspections and the detection of weapons of mass destruction, and to train personnel in its use.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2007	H.R.3220 - New Direction for Energy Independence, National Security, and Consumer Protection Act	Workforce Protection	Enacted regulation	U.S.	Amends the Workforce Investment Act of 1998 to direct the Secretary of Labor to: (1) establish an energy efficiency and renewable energy worker training program; (2) collect and analyze labor market data to track workforce trends resulting from energy-related initiatives under this Act; and (3) award National Energy Training Partnerships Grants to community based nonprofit organizations to carry out training programs that lead to economic self-sufficiency and develop an energy efficiency and renewable energy industries workforce. Establishes the International Clean Energy Foundation to promote projects outside the United States for reducing greenhouse gas emissions and to work with foreign governments and private entities to address climate change issues.
2008	H.R.6606–To direct the Secretary of Homeland Security to impose requirements for the improvement of security camera and video surveillance systems at certain airports, and for other purposes.	Security Camera and video surveillance systems at certain airports	Enacted regulation	U.S.	Directs the Secretary of Homeland Security (Secretary), acting through the Assistant Secretary of Homeland Security (Transportation Security Administration), to require category X or category 1 airport operators to modify their airport security programs to provide for the installation of airport security camera and video surveillance systems. Requires airport operators to submit their modifications to the Secretary for approval. Prohibits the use of images from such cameras and surveillance systems against an airport employee involved in an employment disciplinary matter, except in a criminal investigation or prosecution of criminal acts.
2008	H.R.535–Rail Worker Emergency Training Act of 2008	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	Directs the Secretary of Homeland Security, in coordination with the Secretary of Transportation, to make grants to railroad carriers for costs incurred in instituting a rail worker emergency training program. Directs the Secretary of Homeland Security to issue detailed guidelines for a rail worker emergency training program to enhance rail worker training in preparation for and response to potential or actual terrorist attacks, natural disasters, and other emergencies. Authorizes the Secretary of Homeland Security to issue a letter of noncompliance to rail carriers that fail to comply with the requirements of this Act.
2008	H.R.5915–Screening Applied Fairly and Equitably to Truckers Act of 2008	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	Amends the Homeland Security Act of 2002 to require the Secretary of Homeland Security to: (1) designate security sensitive material; and (2) prohibit an individual from operating a motor vehicle in commerce while transporting such material, unless the operator of the motor vehicle holds a transportation security card issued by the Secretary. Directs the Secretary to prohibit a person (shipper) from offering a security sensitive material for transportation by motor vehicle, or causing the transportation of such material by motor vehicle, unless the operator of the motor vehicle holds a transportation security card. Sets forth both civil and criminal penalties for persons who violate the requirements of this Act. Prohibits a motor vehicle registered in Mexico or Canada from transporting security sensitive material in U.S. commercial motor vehicle operators licensed to transport security sensitive materials in U.S. commerce. Requires the Secretary to conduct periodically a named-based background check against the U.S. integrated terrorism watch list of all individuals licensed to operate a motor vehicle to transport a hazardous material in commerce. Establishes task forces on: (1) highway security, and (2) crimes disqualifying individuals from certain transportation-related employment.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2009	the American Clean Energy and Security (ACES) Act of 2009	Energy security	Enacted regulation	U.S.	This act is a comprehensive national climate and energy legislation that would establish an economy-wide, greenhouse gas (GHG) cap-and-trade system and critical complementary measures to help address climate change and build a clean energy economy. The bill contains five distinct titles: I) Clean energy,II) energy efficiency, III) reducing global warming pollution, IV) transitioning to a clean energy economy and V) agriculture and forestry related offsets. Title I contains provisions related to a federal renewable electricity and efficiency standard, carbon capture and storage technology, performance standard for new coal-fueled power plants, R&D support for electric vehicles, and support for deployment of smart grid advancement. Title II includes provisions related to building, lighting, appliance, and vehicle energy efficiency programs. Title IV includes provisions to preserve domestic competitiveness and support workers, provide assistance to consumers, and support for domestic and international adaptation initiatives.
2009	H.R.261–Chemical Facility Security Improvement Act of 2009	Chemical Facility Security	Enacted regulation	U.S.	Prohibits federal funds from being used by the Secretary of Homeland Security to approve a site security plan for a chemical facility unless the facility meets or exceeds security standards and requirements to protect it against terrorist acts established by the state or local government for the area where it is located. Amends the Department of Homeland Security Appropriations Act, 2007 to: (1) repeal a provision prohibiting the Secretary from disapproving a site security plan based on the presence of absence of a particular security measure; (2) require vulnerability assessments and site security plans to be treated as sensitive security information; and (3) repeal a provision limiting to the Secretary any right of action against a chemical facility owner or operator to enforce security measures.
2009	H.R.3o93–General Aviation Security Enhancement Act of 2009	Aviation Security	Enacted regulation	U.S.	Prohibits the Secretary of Homeland Security, except when an emergency exists based on a credible and urgent threat, from issuing a rule regarding the proposed rulemaking entitled "Large Aircraft Security Program, Other Aircraft Operator Security Program, and Airport Operator Security Program (Transportation Security Administration (TSA)–2008-0021)" unless the Secretary: (1) establishes a nogotiated rulemaking committee; and (2) receives a written report from it detailing findings and recommendations.
2009	H.R.2216–To amend title 49, United States Code, to direct the Assistant Secretary of Homeland Security (Transportation Security Administration) to transfer unclaimed money recovered at airport security checkpoints to United Service Organizations, Incorporated, and for other purpose.	Transportation security administration	Enacted regulation	U.S.	Directs the Assistant Secretary of Homeland Security (Transportation security administration [TSA]) to transfer annually, without further appropriation, unclaimed money recovered at airport security checkpoints to United Service Organization (USO), incorporated, for funding its activities.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2009	H.R.535–Rail Worker Emergency Training Act of 2009	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	Directs the Secretary of Homeland Security, in coordination with the Secretary of Transportation, to make grants to railroad carriers for costs incurred in instituting a rail worker emergency training program. Directs the Secretary of Homeland Security to issue detailed guidelines for a rail worker emergency training program to enhance rail worker training in preparation for and response to potential or actual terrorist attacks, natural disasters, and other emergencies. Authorizes the Secretary of Homeland Security to issue a letter of noncompliance to rail carriers that fail to comply with the requirements of this Act.
2009	H.R.2503–To amend title 49, United States Code, to require inclusion on the no fly list certain detainees housed at the Naval Air Station, Guantanamo Bay, Cuba	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	Requires the Assistant Secretary of Homeland Security (Transportation Security Administration), in coordination with the Terrorist Screening Center, to include on the no fly list any individual who was a detainee housed, on or after January 1, 2009, at the Naval Station in Guantanamo Bay, Cuba.
2009	H.R.2464–COVERT Act of 2009	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	Requires the Secretary of Homeland Security to make sure that avance notice of a covert test of a transportation security system is not provided to any individual (including any security screener) before completion of the test, except: (1) that such information may be provided to certain federal, state, and local government employees, officers, and contractors (including military personnel); and (2)an individual conducting such a test may disclose his or her status if a security screener or other non-covered employee identifies such tester as a potential threat. Requires the head of each covert testing office to make sure that a covert testing person or group is accompanied by a cover team to monitor the test and confirm the identity of personnel involved. States, however, that a cover team is not required to be present during a test of the screening of persons or baggage at an aviation security checkpoint if the test: (1) is approved by the Federal Security Director for the airport, and (2) is administered under an aviation screening assessment program of the Department of Homeland Security. Directs the Secretary to study the impact of implementing covert testing procedures under this Act of the Department's efforts to improve transportation security.
2009	H.R.2870–Security Cabin Baggage Act	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	Securing Cabin Baggage Act - Directs the Secretary of Homeland Security, acting through the Assistant Secretary of Homeland Security (Transportation Security Administration) (TSA), to issue regulations to limit: (1) the size of baggage and personal items carried on board a passenger aircraft; and (2) a passenger to only one carry-on bag and one personal item. Directs the Administrator of the Federal Aviation Administration (FAA) to modify certain federal regulations regarding carry-on baggage to require air carrier carry-on baggage programs to limit each passenger boarding an aircraft to one piece of carry-on baggage and one personal item. Authorizes air carriers to establish smaller size limitations for such items. Specifies items and persons to be excluded from TSA and FAA carry-on baggage limitations, including cockpit and cabin crew in uniform. Requires the TSA and FAA to notify passengers via their websites of federal carry-on baggage and personal item limitations. Requires the TSA to: (1) to install a template with a maximum depth and width to prevent the conveyor belt passage at each checkpoint of carry-on baggage or personal items that exceed federal size limitations; and (2) require passengers with carry-on baggage or personal items that exceed such limitations to check them in.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2010	H.R.6423–111th Congress (2009-2010)–Homeland Security Cyber and Physical Infrastructure Protection Act of 2010	Homeland Security Cyber and Physical Infrastructure Protection	Enacted regulation	U.S.	Amends the Homeland security Act of 2002 to establish within the Department of Homeland Security (DHS) an office of Cybersecurity and Communications, which shall be headed by the Assistant Secretary for Cybersecurity and Communications and which shall include: (1) the United States Computer Emergency Readiness Team; (2) a Cybersecurity Compliance Division (established by this Act); and (3) Other DHS components with primary responsibility for emergency or national communications or cybersecurity. Directs the Secretary of DHS, acting through the Assistant Secretary or the Director of such Division, to establish and enforce cybersecurity requirements for civilian nonmilitary and non-intelligence community federal systems to prevent, deter, respond to, and recover from cyber attacks and incidents.
2010	H.R.5684–Maritime Infrastructure Security and Counterterrorism Act—11th Congress (2009-2010)	Maritime Infrastructure Security and Counterterrorism	Enacted regulation	U.S.	Directs the Secretary of Homeland Security (DHS), acting through the Commandant of the Coast Guard, to commission an independent review of : (1) the threats of terrorist attack posed to offshore energy infrastructure in the Gulf of Mexico, the vulnerabilities of such infrastructure, and consequences of such attacks; and (2) whether the Coast Guard can adequately secure such infrastructure. Directs the Secretary: (1) every two years, to review all vessel security plans approved for mobile offshore drilling units and other vessels used for exploration, development, or production of energy in the Gulf of Mexico; (2) to assess whether such plans take into account the threats of trrorist attack; and (3) to recommend countermeasures.
2010	H.R.6410-Air Cargo Security Act	Air Cargo Security	Enacted regulation	U.S.	Directs the Secretary of Homeland Security (DHS) to establish systems to inspect cargo to ensure the security of all cargo transported in domestic or foreign all-cargo aircraft, including the intrastate air transportation. Requires such systems to meet minimum stansards that ensure eqipment, technology, procedures, or personnel used to screen cargo provide a level of security commensurate with the security level for the screening of passenger checked baggage.
2010	H.R.6275–Air Cargo Security Act of 2010–111th Congress (2009-2010)	Air Cargo Security	Enacted regulation	U.S.	Directs the Secretary of Homeland Security (DHS),acting through the Assistant Secretary of Homeland Security (TSA), to: (1) establish at each U.S airport federal air cargo screening centers to screen cargo transported on domestic and foreign passanger aircraft that operate in air transportation, including intrastate air transportation; (2) establish minimum standards for equipment, technology, procedures, personnel, and methods used to conduct such screening;and (3) ensure that air cargo screening is coordinated with the Certified Cargo Screening Program and any other established air cargo security program.
2010	H.R.5186–Continuing Chemical Facilities Antiterrorism Security Act of 2010	Chemical Facility Security	Enacted regulation	U.S.	Amends the Department of Homeland Security Appropriations Act, 2007 to extend until October 4, 2015, the authority of the Security of Homeland Security (DHS) to issue interim final regulations establishing risk-based performance standards for security of chemical facilities and requiring vulnerability assessments and the development and implementation of site security plans for such facilities. Requires the Secretary, acting through the Administrator of the Federal Emergency Management Agency (FEMA) and in coordination with the Under Secretary for National Protection and Programs, to: (1)establish a voluntary chemical security training program to enhance the capabilities of high-risk chemical facilities to prevent, prepare for, respond to, mitigate against, and recover from acts of terrorism , natural disasters, and other man-made disasters, and (2) develop a voluntary chemical security exercise program to offer voluntary testing and evaluation of the capabilities of the federal government, state governments, commercial personnel and management, emergency response providers, and the private sector to prevent, prepare for, mitigate against, respond to, and recover from acts of terrorism, natural disasters, and other emergencies at chemical facilities.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2010	H.R.6o47–Guaranting Airport Physical Screening Standard Act	Airport Srcurity	Enacted regulation	U.S.	Directs the Assistant Secretary of Homeland Security (Transportation Security Administration) to: (1) issue regulations, directives, or other appropriate measures to implement requirements directing airport perimeter screening of all individuals, goods, property, vehicles, and other equipment before entry into a secured airport area; and (2) set a schedule for requiring airports to update their airport security plans to comply with such perimeter screening requirements.
2010	H.R.6326–Fair and Impartial Requirement Act of 2010	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	Directs the Assistant Secretary of Homeland Security (Transportation Security Administration [TSA]) to issue: (1) issue regulations to establish a waiver process to allow an air carrier, airport operator, or government to to hire an individual who has been disqualified for employment for a position as an airport security screener or in which an individual has unescorted access to a sterile airport area because of conviction of a specified crime; and (2) establish an appeals process for a disqualified individual that includes notice and an opportunity for a hearing before an impartial third party. Requires the Assistant Secretary to issue a waiver to an individual: (1) who, based on certain criteria, does not pose a terrorism risk; and (2) without regard to whether that individual would otherwise be disqualified by reason of a felony conviction, if the employer establishes acceptable alternate security arrangements.
2010	H.R.535–Rail Worker Emergency Training Act of 2010	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	Directs the Secretary of Homeland Security, in coordination with the Secretary of Transportation, to make grants to railroad carriers for costs incurred in instituting a rail worker emergency training program. Directs the Secretary of Homeland Security to issue detailed guidelines for a rail worker emergency training program to enhance rail worker training in preparation for and response to potential or actual terrorist attacks, natural disasters, and other emergencies. Authorizes the Secretary of Homeland Security to issue a letter of noncompliance to rail carriers that fail to comply with the requirements of this Act.
2010	H.R.575o–FAMS Augmentation Act of 2010	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	Directs the Assistant Secretary of Homeland Security (DHS) for the Transportation Security Administration (TSA) to increase the number of federal air marshals by at least an additional 1,750 above the number of such marshals as of January 31, 2010, to ensure increased transportation security for inbound international flights. Declares the goal of this Act is to increase the number of inbound flights with federal marshals onboard while maintaining federal marshal presence on domestic point-to-point flights at or above December 25, 2009, levels. Directs the Federal Air Marshal Service (FAMS) to establish a policy requiring newly hired federal air marshals to complete as part of their basic training the criminal investigative training program at the Federal Law Enforcement Training Center.
2010	H.R.4442–Planes Act of 2010	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	Directs the Secretary of Homeland Security (DHS) , acting through the Assistant Secretary of Homeland Security (DHS), acting through the Assistant Secretary of Homeland Security (Transportation Security Administration[TSA]) to: (1) study and report to Congress on the use and effectiveness of explosives detection technologies, including whole-body imaging technology, and explosives detection canine teams, for screening cargo , passenger checked an carry-on baggage, and air passangers on domestic and foreign aircraft, (2)submit to Congress an explosive detection technologies rapid deployment plan; and (3) ensure that each U.S. commercial service airport has at least one explosives detection canine team, and that is a sufficient number of such teams be deployed to meet 100% of federal air cargo screening requirements for domestic and foreign passanger aircraft.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2010	H.R.6122–Federal Protective Service Improvement and Accountability Act of 2010	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	Directs the Secretary of Homeland Security (DHS) to maintain no fewer than 1,350 full-time equivalent positions in the Federal Protective Service inspector force, who shall be fully tained federal law enforcement officers. Directs the Secretary to classify the positions in the following categories: (1) Federal Protective Service Contract oversight force; and (2) minimum training and certification standards for security guard services at facilities protected by the Service. Express the sense of Congress that specified security standards for federal facilities established by the Interagency Security Committee should be implemented for all federal facilities for which they were issued. Directs the Secretary, through the Director of the Federal Protective Service to: (1) commence a one-year pilot program to research the advantages of converting guard positions at the highest-risk federal facilities protected by the Service from contract guard positions to positions held be federal employees; and (2) establish and hire individuals for a federal facility security guard position. Directs the Controller General to: (1) periodically review and report to Congress on the performance by federal facility security guards under the pilot program, and upon its completion submit a final report evaluating whether or not the performance of individuals in such positions was satisfactory (if so, directs the Secretary to replace contract guards at all highest risk facilities protected by the Service with federal employees); and (2) submit a review of the fee-based funding system in use by the Service and issue any recommendations for alternative approaches.
2010	S.3538–National Cyber Infrastructure Ptotection Act of 2010	Cyber security	Enacted regulation	U.S.	National Cyber Infrastructure Protection Act of 2010 - Establishes within the Department of Defense (DOD) a National Cyber Center, headed by a Director who shall report directly to the President. Includes among the Director's duties: (1) coordinating federal government defensive operations, intelligence collection and analysis, and activities to protect and defend government information networks; (2) acting as the principal adviser to the President, the National Security Council, and the heads of federal agencies on matters relating to the protection and defense of such networks; and (3) keeping appropriate congressional committees fully informed of the Center's activities. Grants the Director access to all intelligence relating to cyber security collected by any federal agency, with specified exceptions. Provides for annual submissions to the Director of cyber budget requests by the head of each federal agency with responsibilities for matters relating to the protection and defense of federal information networks. Establishes within the National Cyber Security Program Budget a National Cyber Defense Contingency Fund. Directs the Secretary of Energy (DOE) to determine the appropriate location for, and to establish within a National Laboratory, a public and private partnership for sharing cyber threat information and exchanging technical assistance, advice, and support, to be known as the Cyber Defense Alliance. Sets forth guidelines regarding the uses of shared information. Requires the Director of National Intelligence (DNI) to: (1) facilitate certain information sharing and declassification activities; and (2) establish uniform procedures for the receipt, care, and storage by agencies of information that is voluntarily submitted to the government through the Alliance. Establishes penalties for federal officers or employees who knowingly disclose cyber threat information protected from disclosure by this Act. Authorizes the federal government to provide warnings regarding potential threats to information networks. Terminates the Alliance on December 31, 2020.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2011	The Cyber Intelligence Sharing and Protection Act(CISPA)	Cyber security	proposed regulation	U.S.	CISPA would allow for the sharing of Internet traffic information between the U.S. Government and technology and manufacturing companies. The stated aim of this bill is to help the U.S. Government investigate cyber threats and ensure the security of networks against cyberattacks. CISPA has been criticized by advocates of Internet privacy and civil liberties. Those groups argue CISPA contains too limits on how and when the government may monitor a private individual's Internet browsing information. Additionally they fear that such new powers could be used to spy on the general public rather than to pursue malicious hackers. CISPA had garnered favour from corporations and lobbying groups such as Microsoft, IBM and Apple, which look on it as a simple and effective means of sharing important cyber threat information with the government.
2011	H.R.535–Rail Worker Emergency Training Act of 2011	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	Directs the Secretary of Homeland Security, in coordination with the Secretary of Transportation, to make grants to railroad carriers for costs incurred in instituting a rail worker emergency training program. Directs the Secretary of Homeland Security to issue detailed guidelines for a rail worker emergency training program to enhance rail worker training in preparation for and response to potential or actual terrorist attacks, natural disasters, and other emergencies. Authorizes the Secretary of Homeland Security to issue a letter of noncompliance to rail carriers that fail to comply with the requirements of this Act.
2011	H.R.71–FAMS Augmentation Act of 2011	Transportation Security and Infrastructure Protection	Enacted regulation	U.S.	FAMS Augmentation Act of 2011 - Directs the Assistant Secretary of Homeland Security (DHS) for the Transportation Security Administration (TSA) to increase the number of federal air marshals by at least an additional 1,750 above the number of such marshals as of January 31, 2010, to ensure increased transportation security for inbound international flights. Declares the goal of this Act is to increase the number of inbound flights with federal marshals onboard while maintaining federal marshal presence on domestic point-to-point flights at or above December 25, 2009, levels. Directs the Federal Air Marshal Service (FAMS) to establish a policy requiring newly hired federal air marshals to complete as part of their basic training the criminal investigative training program at the Federal Law Enforcement Training Center. Requires federal air marshals hired before enactment of this Act who have not completed such program to attend an alternative training program. Directs the Assistant Secretary to establish in FAMS an Office of the Ombudsman.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2011	H.R.2937–Pipeline Infrastructure and Community Protection Act of 2011	Infrastructure Protection	Enacted regulation	U.S.	Pipeline Infrastructure and Community Protection Act of 2011 - Prescribes or revises requirements for safety and environmental protection in pipeline transportation. (Sec. 2) Defines the term "major consequence violation" to mean a violation that contributed to a pipeline incident resulting in: (1) one or more deaths or injuries or illnesses requiring in-patient hospitalization; or (2) environmental harm exceeding $250,000 in estimated damages, including property loss (other than the value of natural gas or hazardous liquid lost or damage to pipeline facility equipment). Subjects to a civil penalty of $250,000 per day any person that the Secretary of Transportation (DOT) has found to have committed a major consequence violation of a pipeline marking or excavation notification requirement, pipeline safety standard or regulation, or order. Authorizes the Secretary to impose a civil penalty on a person who obstructs or prevents an inspection or investigation of a gas pipeline or hazardous liquid pipeline. Prescribes a maximum civil penalty of $2.5 million for a related series of major consequence violations. (Sec. 3) Prohibits a state one-call notification program from exempting mechanized excavation, municipalities, state agencies, or their contractors from its one-call notification system requirements. Directs the Secretary to study the impact of third party damage on pipeline safety. (Sec. 4) Requires the Secretary to issue regulations subjecting offshore hazardous liquid gathering lines (except production pipelines or flow lines) as well as those located within Gulf of Mexico inlets to the same standards and regulations as other hazardous liquid pipelines. (Sec. 5) Directs the Secretary to prescribe a regulation to require the use of automatic or remote-controlled shut-off valves (or equivalent technology) on pipelines. Directs the Secretary to review the ability of a transmission pipeline operator to respond to a hazardous liquid or gas release from a pipeline segment located in a high consequence area, including an analysis of the costs, risks, and benefits of installing automatic and remote-controlled shut-off valves. (Sec. 6) Requires the Secretary to prescribe regulations to require the use of excess flow valves, or equivalent technology, on new or entirely replaced distribution branch services, multi-family facilities, and small commercial facilities located in high-density population areas and environmentally sensitive areas. **(Sec. 7) Directs the Secretary to evaluate specified questions with respect to integrity management safety system requirements, taking certain factors into consideration. Directs the Secretary to prescribe regulations that: (1) expand integrity management system requirements, or elements of them, beyond high consequence areas; and (2) remove redundant class location requirements for gas transmission pipeline facilities regulated under an integrity management program.**
2011	H.R.1505 - National Security and Federal Lands Protection Act	National Security and Land Protection	Enacted regulation	U.S.	National Security and Federal Lands Protection Act - Prohibits the Secretary of the Interior or the Secretary of Agriculture (USDA) from prohibiting or restricting activities on land under their respective jurisdictions by U.S. Customs and Border Protection to achieve operational control over the international land borders of the United States. Grants U.S. Customs and Border Protection access to such lands to conduct the following activities: (1) construction and maintenance of roads and fences; (2) use of patrol vehicles and aircraft; (3) installation, maintenance, and operation of surveillance equipment and sensors; and (4) deployment of temporary tactical infrastructure, including forward operating bases. States that a waiver by the Secretary of Homeland Security (DHS) of specified laws regarding sections of the international border between the United States and Mexico and between the United States and Canada shall apply to all land under the jurisdiction of the Secretary of the Interior or the Secretary of Agriculture within 100 miles of the international land borders of the United States with respect to U.S. Customs and Border Protection activities under this Act. States that this Act shall not be construed to restrict legal use (grazing, hunting, or mining) on, or legal access to, land under the jurisdiction of the Secretary of the Interior or the Secretary of Agriculture. Terminates this Act five years after enactment.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2012	S.3450–Coal Miner Employment and Domestic Energy Infrastructure Protection Act	Infrastructure Protection	Enacted regulation	U.S.	Coal Miner Employment and Domestic Energy Infrastructure Protection Act - Prohibits the Secretary of the Interior, before December 31, 2013, from issuing or approving any proposed or final regulation under the Surface Mining Control and Reclamation Act of 1977 that would: (1) adversely impact employment in coal mines in the United States; (2) cause a reduction in revenue received by the federal government or any state, tribal, or local government, by reducing through regulation the quantity of coal in the United States that is available for mining; (3) reduce the quantity of coal available for domestic consumption or for export; (4) designate any area as unsuitable for surface coal mining and reclamation operations; or (5) expose the United States to liability for taking the value of privately owned coal through regulation.
2012	H.R.3792 - Clean Water Infrastructure and Security Improvement Act of 2002	Infrastructure Protection	Enacted regulation	U.S.	Clean Water Infrastructure and Security Improvement Act of 2002 - Amends the Federal Water Pollution Control Act to remove certain requirements for States with respect to construction of treatment works under capitalization grant agreements. Requires architectural and engineering contracts to be awarded consistent with procedures under the Federal Property and Administrative Services Act of 1949 or an equivalent State qualifications-based requirement. Directs the Administrator of the Environmental Protection Agency to assist States in establishing simplified procedures for small water systems to obtain assistance under the Act. Requires revolving funds to be used only for providing assistance for activities which have as a principal benefit the improvement or protection of water quality of navigable waters. Makes revisions concerning uses of funds for: (1) innovative technologies; (2) administrative expenses; (3) small system technical, planning, and management assistance; and (4) financially distressed communities. Revises requirements related to consistency with plans and eligibility of treatment works not considered publicly owned. Requires States to make grants to financially distressed communities in any fiscal year in which the Administrator has more than $1.4 billion available for obligation and allows a State to give priority to such communities in making loans. Allows a recipient of assistance from a State revolving fund to use the design-build project delivery (single contract) method. Reauthorizes appropriations for FY 2003 through 2007 for the revolving fund program.
2012	S.2111 - Cyber Crime Protection Security Act	Cyber security	Enacted regulation	U.S.	Cyber Crime Protection Security Act - Amends the federal criminal code to make fraud in connection with the unauthorized access of personally identifiable information (in electronic or digital form) a predicate for instituting a prosecution for racketeering. Increases penalties for fraud and related activity in connection with computers. Expands the prohibition against trafficking in passwords to include trafficking through any means by which a protected computer may be accessed without authorization. Imposes criminal penalties for attempts and conspiracies to commit fraud and related activity in connection with computers. Modifies criminal and civil forfeiture provisions, including requiring certain civil forfeiture seizures and forfeitures to be performed by persons designated for that purpose by the Secretary of Homeland Security (DHS) or the Attorney General (DOJ). Prohibits, during and in relation to a felony violation of provisions regarding fraud and related activity in connection with computers, intentionally causing or attempting to cause damage to a critical infrastructure computer if such damage results in (or, in the case of an attempt, would, if completed have resulted in) the substantial impairment of the operation of that computer or of the critical infrastructure associated with the computer. Imposes a prison term of between 3 and 20 years, a fine, or both. Prohibits probation for any person convicted of such a violation. Provides for concurrent sentences under specified circumstances. Excludes from the definition of "exceeds authorized access" for purposes of the prohibition against fraudulent use of computers, access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or nongovernment employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized.

Year	Legislation code	Area	Proposed or enacted	State	Summary of key points relating to security
2013	S.831 - Coal Miner Employment and Domestic Energy Infrastructure Protection Act of 2013	Infrastructure Protection	Enacted regulation	U.S.	Coal Miner Employment and Domestic Energy Infrastructure Protection Act of 2013 - Prohibits the Secretary of the Interior, before December 31, 2017, from issuing or approving any proposed or final regulation under the Surface Mining Control and Reclamation Act of 1977 that would: (1) adversely impact employment in coal mines in the United States; (2) cause a reduction in revenue received by the federal government or any state, tribal, or local government, by reducing through regulation the quantity of coal in the United States that is available for mining; (3) reduce the quantity of coal available for domestic consumption or for export; (4) designate any area as unsuitable for surface coal mining and reclamation operations; (5) expose the United States to liability for taking the value of privately owned coal through regulation; or (6) cause further time delays to permitting or increase costs.

ANNEX2. Public Policy and Information Security

ANNEX2.1 Public Policy

This paper reviews some theoretical results in the area of public policy related to security. Broadly, we assume that there are three types of players in a strategic game: targets (usually thought to be firms or individuals), attackers (an unknown typology, but assumed to have some form of consistent preferences) and a public-policy maker that has responsibility for the aggregate security of the targets subject to their own set of preferences.

The models presented in this paper tend to assume ex-ante identical targets and attackers this is for reasons of analytical tractability. However, the core ideas are easily extensible to a simulated example, that permits variation in attacker and target behaviour. Of course, this variation results in the solutions having to be computed numerically rather than analytically (with an explicit mathematical formulation).

ANNEX2.1.1 Background

The key question for this deliverable is: how do firms choose investments in security? We then construct a dynamic model of investment and solve for an individual firms optimal choice. Next we outline a set of assumptions on how attackers choose to involve themselves in attacks on targets. As this is a public policy decision we do not look at the fine structure of the interaction between specific attackers and targets, however we assume some form of statistical matching. The main results are in the form of analytic equilibrium solutions for investment and risk.

Our results are calibrated to qualitative and quantitative data provided by NGRID summarised in the validation section of Deliverable 2.4. Our quantitative model provides an approach for assessing the impact of sudden changes in the capabilities of attackers and targets, using a nested cost-benefit analysis.

ANNEX2.2 The Model

We follow [21] and [22] in formulating an equilibrium model with attacker externalities. We consider a set of N_T ex-ante identical targets choosing to allocate defensive resources that mitigate the harm from attacks.

In a departure from previous models the targets need to solve, simultaneously, a multidimensional resource allocation problem. Let the subscripts h and l represent to potential areas of allocation of assets and let $x_h \geq 0$ and $x_l \geq 0$ be one off investments made at time t_0 in securing those areas. Let z be a switching variable such that a fraction $0 \leq z \leq 1$ of assets are allocated between h and l.

Let $\tilde{\sigma}_{i\in\{l,h\}} : \mathbb{R}_+ \rightarrow [0, 1]$ be a function that determines the instantaneous, time t risk for a fixed time horizon where $(t_0, T) = \{t | t_0 < t < T\}$. When properly specified we can interpret $\tilde{\sigma}$ as the instant probability of a successful attack. We will refer to z as the 'asset allocation' and to two further quantities x_l and x_l as the 'investment allocation' stated combinations are referred as 'allocation bundles'.

A reasonable assumption is that increased investment $x_{i\in\{l,h\}}$ reduces the probability of a successful attack, i.e. $\partial\tilde{\sigma}_{i\in\{l,h\}}/\partial x_{i\in\{l,h\}} < 0$, ceteris paribus. However, with increasing investment is a decreasing marginal reduction in the probability of a successful attack $\partial^2\tilde{\sigma}_{i\in\{l,h\}}/\partial x^2_{i\in\{l,h\}} > 0$. Similarly, with increased attacking intensity $\eta_{i\in\{l,h\}}$ on the particular area of allocation there should be a corresponding increase in the probability of a successful attack $\partial\tilde{\sigma}_{i\in\{l,h\}}/\partial\eta_{i\in\{l,h\}} > 0$. A functional form for $\tilde{\sigma}$ that satisfies these conditions is the following multiplicative model:

$$\tilde{\sigma}_i = e^{-\psi_i x_i}\eta_i^{\alpha_i}, \quad i \in \{l, h\} \tag{1}$$

under this formulation there is an upper bound on $\eta_{i\in\{l,h\}}$ of $\eta_i^* < e^{\alpha_i^{-1} x_i \psi_i}$ for $i \in \{l, h\}$ such that $\tilde{\sigma}_i$ may still be interpreted as probability of a successful attack. Here $\psi_{i\in\{l,h\}}$ is relative marginal decrease in $\tilde{\sigma}_{i,i\in\{l,h\}}$ for a unit increase in $x_{i\in\{l,h\}}$. Analogously, $\alpha_{i\in\{l,h\}}$ is the elasticity of attack.

Let $L > 0$ be an instantaneous value of assets at risk from attack and $\beta \in \mathbb{R}$ be a subjective discount rate determining the time preferences of all targets. The risk neutral expected loss over the time horizon $t_0 < t < T$, is given by

$$\tilde{V}_L = \int_{t_0}^{T} e^{-\beta t} \left(z\tilde{\sigma}_l\left(x_l, \eta_l\right) L + (1 - z)\,\tilde{\sigma}_h\left(x_h, \eta_h\right) L\right) dt + x_l + x_h. \tag{2}$$

The optimal allocation bundle $(z^\diamond, x_l^\diamond, x_h^\diamond)$, when attacking intensity is exogenous, is the simultaneous solution of $\{\partial\tilde{V}_L/\partial x_l = 0, \partial\tilde{V}_L/\partial x_h = 0, \partial\tilde{V}_L/\partial z = 0\}$. By construction, if $\alpha_{i\in\{l,h\}} > 0$, $\psi i \in \{l, h\} > 0$, $L > 0$, $\beta > 0$ and $z \in (0, 1)$ a minima of this function exists. By assumption we set that the optimal allocation must be either $(x_{i\in\{k,h\}}) \in \mathbb{R}_+$ when $(\eta_{i\in\{k,h\}}) \in \mathbb{R}_+$, or if the minima lies at $x_{i\in\{l,h\}} < 0$, then $x^\diamond_{i\in\{l,h\}} = 0$. Similarly we impose the inequality constraint that $0 \leq z^\diamond \leq 1$.

In this model we assume that attacker externalities are driven by the diffuse-attacking-mass approach first suggested in [21] and refined in [22]. In this approach attackers are assumed to be ex-ante identical and randomly allocated to targets with identical probability $1/N_T$. Attackers are assumed to be able to make independent decisions on the type of attacks (analogous to entering the market for a given the asset area (l, h)).

A useful interpretation of the attacker cost per unit is that attackers need to develop an attacking tool at cost c each time they engage a target. The attacker then chooses the medium by which they seek to monetize (in the case of terrorists monetization is via utility equivalents) their attacking effort. An example could be corporate network information channels versus industrial control systems. Attackers at inception may not know which target they intend to attack or from the viewpoint of the policy-maker, in this setting, it is irrelevant who is attacking the targets, from the target-attacker transaction viewpoint, the salient point is the aggregate level of loss incurred in the presence of attacking intent.

What is important, to the policy-maker, is the overall mass of attacks against systems containing assets under the type l and type h and this will be influenced by the aggregate behaviour of targets and attackers, rather than the microstructure of individual attack-defence interactions. The more attractive the ecosystem is to attackers then the greater the mass of attacks against its individual components.

Let the number of attackers for each asset area is $N_{A,i\in\{l,h\}}$ and the ratio of attackers per target is the attacking intensity $\eta_{i\in\{l,h\}} = N_{A,i\in\{l,h\}}/N_T$. Let the reward $R > 0$ for a successful attack be proportional to the assets allocated in each area h and l and for notational compactness let $\zeta_{i=l} = z$ and $\zeta_{i=h} = 1 - z$. Set $\gamma = c/R$ to be the cost ratio of attack, where c is the unit cost of a single attack. When attacker time preferences are described by the δ the profit function for a single attacker is:

$$\tilde{\Pi}_{A,i} = \int_{t_0}^{T} e^{-\delta t}\zeta_i\eta_i^{-1}\tilde{\sigma}_i\left(x_i,\eta_i\right)dt - \gamma, \quad i \in \{l,h\} \tag{3}$$

in this case we assume that attackers do not coordinate attacks (or are commissioned by a single attacker) and rewards are claimed on a first-winner-takes-all basis. Attackers are assumed to be drawn from a pool and make one-off entry decisions until marginal cost and marginal benefit are equal and hence $\tilde{\Pi}_{A,i} = 0$.

Assuming that targets and attackers have positive discount rates the appropriate time horizon, T, for empirical analysis, maybe determined endogenously. Let λ be an arbitrarily large, but not infinite, number. For a given discount factor, $\tilde{\theta} = \min(\delta,\beta)$, by construction $\lim_{T\to\infty}\int_{t_0}^{T}\tilde{\theta}^{-1}e^{-\theta t}dt = 1$. Therefore, the approximation of the time horizon $\tilde{T}$ covering the $1 - 1/\lambda$ proportion of the future losses is derived from $\tilde{T} = \log(\lambda)/\tilde{\theta}$. In §(ANNEX2.3) of this paper we shall follow [22] and assume that $\beta > \delta$ and that $\tilde{T} = \log(\lambda)/\delta$, such that the interval t_0 to $\tilde{T}$ covers 90% of the expected present value, i.e. $\lambda = 10$.

Proposition 1a: Existence of Nash equilibrium target allocations

Following the preceding assumptions, when $\tilde{\sigma}_i = e^{-\psi_i x_i}\eta_i^{\alpha_i}$ for $i \in \{l,h\}$, the Nash equilibrium allocations of x_h, x_l and z denoted x_h^*, x_l^* and $z*$ are

$$\begin{aligned} x_i^* &= \frac{\alpha_i}{\psi_i}\log\left(\frac{L\psi_i\psi_j^2\left(e^{\delta T}-1\right)^2}{\gamma\delta\beta\left(\psi_j+\psi_i\right)^2}\right) - \frac{\alpha_i\delta T}{\psi_i}, \quad i \in \{l,h\}, j \in \{l,h\}, j \neq i \\ z^* &= \frac{\psi_l}{\psi_h+\psi_l} \end{aligned} \tag{4}$$

Proof is in § ANNEX2.5.1. Note that in the multiplicative separably additive form of $\tilde{\sigma}_{i\in\{l,h\}}$ the Nash equilibrium allocation z^* is a simple function of $\psi_{i\in\{l,h\}}$ and when $\psi_l = \psi_h$ the allocation is equal. If we add a constraint $x_l + x_h = \tilde{x}$, where $\tilde{x}$ is a hard budget constraint then the attacking effort in each asset area enters the function for z. We will demonstrate in §§(ANNEX2.2.5) that in this modelling approach we do not have to place an arbitrary constraint on $x_l + x_h$ to create conditions similar to the standard results obtained when optimising under a hard budget restriction.

Proposition 1b: Existence of Nash equilibrium attacker intensities

Following from Proposition 1a the Nash equilibrium attacker intensities, denoted η_l^* and η_h^* are

$$\eta_i^* = \left(\frac{\psi_j(e^{\delta T}-1)e^{-x_i^*\psi_i-\delta T}}{\gamma\delta(\psi_i+\psi_j)}\right)^{\frac{1}{1-\alpha_l}}, \quad i \in \{l,h\}, j \in \{l,h\}, j \neq i \tag{5}$$

where $x^*{}_{i,\in\{l,h\}}$, is the functional forms of the Nash equilibrium given in Proposition 1a.

Proof is given in § ANNEX2.5.1. This solution is subject to the upper bound of $\eta_i^* < e^{\alpha_i^{-1} x_i \psi_i}$ for $i \in \{l, h\}$.

ANNEX2.2.1 Introducing the Public Policy-Maker

The subject of this paper is resilience and why a system might not be resilient to security shocks through the choices of the individual components. The first policy action we will evaluate replicates our previous work by postulating a Stackelberg policy framework in which the policy maker setting rules relative to a target level of global welfare. When the policy-maker is fully informed our model reverts to a standard mechanism design problem whereby the policy-maker is able to set a mandatory investment bundle (denoted by the lower bar) on the individual targets $(\bar{x}_l, \bar{x}_h)$ as well as imposing a specific asset allocation $\bar{z}$ and maximise global welfare (by minimize total loss).

The Nash equilibrium allocations for the N_T targets assumes no social coordination. Therefore, the Nash equilibrium allocation (x_l^*, x_h^*, z^*) of defensive effort and corresponding attacking intensities (η_l^*, η_h^*) will not necessarily be the first best solution for Pareto efficiency. Let $(x_l^\dagger, x_h^\dagger, z^\dagger)$ be the Pareto efficient allocations for a given set of model parameters $(\alpha_{i\in\{l,h\}}, \beta, \gamma, \delta, \lambda, \psi_{i\in\{l,h\}}, L)$.

For a classical efficiency a public policy maker imposing $(\bar{x}_l, \bar{x}_h, \bar{z})$ Pareto efficiency is only achieved when the subjective discount rate of the policy-maker is equal to β for a single allocation, this is relatively simple and is illustrated in the next subsection. Indeed, the subjective viewpoint of the targets heterogeneous discount rates, the chosen values of $(\bar{x}_l, \bar{x}_h, \bar{z})$ cannot be the Pareto efficient allocation $(x_l^\dagger, x_h^\dagger, z^\dagger)$, when $\beta \neq \bar{\beta}$.

ANNEX2.2.2 The Fully Informed (x_l, x_h, z) setting Public-Policy-Maker

Let the social discount rate be $\bar{\beta}$. A fully informed public policy sets a mandatory level of $(\bar{x}_l, \bar{x}_h, \bar{z})$ by minimizing the following loss function

$$\tilde{V}_P = \int_{t_0}^{T} e^{-\bar{\beta} t} \left(z \tilde{\sigma}_l \left(x_l, \eta_l^\diamond \right) L + (1 - z) \tilde{\sigma}_h \left(x_h, \eta_h^\diamond \right) L \right) dt + x_l + x_h \tag{6}$$

where $\eta_i^\diamond(x_i, z)$ for $i \in \{l, h\}$ is the solution to

$$\int_{t_0}^{T} e^{-\delta t} \zeta_i \eta_i^{-1} \tilde{\sigma}_i \left(x_i, \eta_i \right) dt = \gamma, \quad i \in \{l, h\} \tag{7}$$

in terms of (x_l, x_h, z). We can see that by internalizing the attacker reaction curve the fully informed policy maker with identical time preferences to the homogenous targets $\bar{\beta} = \beta$ will set an allocation bundle $(\bar{x}_l, \bar{x}_h, \bar{z})$. In the multi-allocation form of the model, when $\tilde{\sigma}_i = e^{-\psi_i x_i} \eta_i^{\alpha_i}$ for $i \in \{l, h\}$ proof that $(\bar{x}_l, \bar{x}_h, \bar{z}) = (x_l^\dagger, x_h^\dagger, z^\dagger)$ when $\bar{\beta} = \beta$ for all parameter combinations, is not possible as $\bar{z}$ does not have an analytically tractable form, other than in certain special cases, for instance $\alpha_l = \alpha_h = \alpha$.

However, let us now consider a constraint on weighting aspect of the bundle z across asset areas. A logical constraint would be to set $z = \psi_h/(\psi_h + \psi_l)$, the Nash equilibrium allocation. However, other constraints on z can be reasonably justified as we will demonstrate subsequently.

Proposition 2a: The Fully Informed Public-Policy-Maker Investment Allocation

When $\tilde{\sigma}_i = e^{-\psi_i x_i}\eta_i^{\alpha_i}$ and let $\bar{z} = \psi_h/(\psi_h + \psi_l)$, the policy-maker's optimal investment allocation $(\bar{x}_l, \bar{x}_h)$ is

$$\begin{aligned}\bar{x}_i \;&=\; \frac{1}{\psi_i}\log\left(\psi_j(\psi_i+\psi_j)^{\frac{1}{1-\alpha_i}}\right) + \frac{\alpha_i}{\psi_i}\log\left(\frac{1}{\gamma}\delta\left(e^{\delta T}-1\right)\right) + \\ &\left(\frac{\bar{\beta}T\left(\alpha_i-1\right)}{\psi_i} - \frac{\delta T\alpha_i}{\psi_i}\right) + \frac{(\alpha_i-1)}{\psi_i}\log\left(\frac{-\bar{\beta}\left(\alpha_j-1\right)}{L\psi_i\left(e^{\bar{\beta}T}-1\right)}\right), \\ &i \in \{l,h\}, j \in \{l,h\}, j \neq i \qquad (8)\end{aligned}$$

Proof: Is given in § ANNEX2.5.2.

Proposition 2b: Attacking Intensity with a Fully informed Public-Policy-Maker

Following from Proposition 2a the attacker intensity $\eta_{i\in\{l,h\}}$ is

$$\bar{\eta}_i = \left(\frac{\psi_i\left(e^{\delta T}-1\right)e^{-\bar{x}_i\psi_i-\delta T}}{\gamma\delta\left(\psi_j+\psi_i\right)}\right)^{\frac{1}{1-\alpha_i}}, \quad i \in \{l,h\}, j \in \{l,h\}, j \neq i \qquad (9)$$

where $\bar{x}_i$ is given in Equation 8.
Proof: Is also given in § ANNEX2.5.2. The solution is again subject to an upper bound of upper bound of $\eta_i^* < e^{\alpha_i^{-1}x_i\psi_i}$ for $i \in \{l,h\}$. We can compare the solutions in Equations 8 and 9 for the fully informed policy-maker versus those in Equations 4 and 5. This leads us to a further Proposition as follows.

Proposition 2c: The Public-Policy-Maker Improvement

When $\tilde{\sigma}_i = e^{-\psi_i x_i}\eta_i^{\alpha_i}$ with $\beta \geq \bar{\beta}$ and $\alpha_{i\in\{l,h\}} > 0, \psi_{i\in\{l,h\}} > 0, \gamma > 0, \delta > 0, L > 0$ and the asset allocation is constrained to $\bar{z} = \psi_h/(\psi_h + \psi_l)$, the Policy-makers mandated investment $\bar{x}_{i\in\{l,h\}}$ is always greater than or equal to the Nash equilibrium investment bundle $x^*{}_{i\in\{l,h\}}$.
Proof: is obtained by substituting the expressions $\bar{x}_{i\in\{l,h\}}$ and $x^*{}_{i\in\ l,h\}}$ in Equations 4 and 8 into the functional form $\bar{x}_{i\in\{l,h\}} \geq x^*{}_{i\in\{l,h\}}$ and subject to the constraint $\beta \geq \bar{\beta}$. By solving the two inequalities simultaneously for each parameter relative to its own constraint i.e. $\alpha_{i\in\{l,h\}} > 0, \psi_{i\in\{l,h\}} > 0, \gamma > 0, \delta > 0, L > 0$ by inspection the constraint $\beta > \bar{\beta}$ is never violated. The complete set of steps of the proof are relatively simple albeit algebraically long and is available from the authors on request.

A useful by product of the comparison between Propositions 1 and 2 is that we can define an upper bound on $\beta \geq \bar{\beta}$ such that the policy-maker does at least as well as the Nash equilibrium even when the policy-maker weights potential near term losses more than the targets (non-progressive bound on policy-maker ability). Again this is covered in more detail for the one dimensional case in [22].

The attacker intensities follow from the functional form of the Nash equilibrium, except with $\bar{x}_{i\in\{l,h\}}$ replacing $x^*_{i\in\{l,h\}}$ as in Equation 9, from the chosen functional form of $\tilde{\sigma}_{i\in\{l,h\}}$, $\bar{\eta}_{i\in\{|,h\}}$ we know that overall loss decreases with increasing $x_{i\in\{l,h\}}$, ceteris paribus, and we know by construction that $\bar{x} > x^*$ when we constrain $\bar{z} = \psi_h/(\psi_h + \psi_l)$ and $\beta \geq \bar{\beta}$.

Following [22] we also consider an non-discounted metric $\tilde{V}_A$ that measures total cost from attacks and investment, we shall consider a detailed functional form in §§(ANNEX2.2.6). When $x_{i\in\{l,h\}}$ is set by the fully informed policy-maker minimising the objective function set out in Equation 6 and $\tilde{\sigma}_{i\in\{l,h\}}$, $\bar{\eta}_{i\in\{|,h\}}$ with $\bar{z} = \psi_h/(\psi_h + \psi_l)$ and $\beta \geq \bar{\beta}$ then $\tilde{V}_A(\bar{x}_{i\in\{l,h\}})$ will be lower than $\tilde{V}_A(\bar{x}^*_{i\in\{l,h\}})$ for all combinations of $\alpha_{i\in\{l,h\}} > 0, \psi_{i\in\{l,h\}} > 0, \gamma > 0, \delta > 0$ and $L > 0$. It should be noted that by construction $\tilde{V}_A$ is not an objective function (its minima is unbounded in $x_{i\in\{l,h\}}$). However, the functional form of $\tilde{V}_A$ is useful in measuring the effect of the transition from $x^*_{i\in\{l,h\}}$ to $\bar{x}_{i\in\{l,h\}}$ free from the subjective discount rates β and $\bar{\beta}$.

ANNEX2.2.3 Reducing the Policy-maker's Abilities

The preceding notion of the policy-maker assumed that he/she had the ability to impose $(\bar{x}_l, \bar{x}_h, \bar{z})$ on the targets and thus achieve a lower loss in $\tilde{V}_P$ than the Nash equilibrium allocation of (x^*_l, x^*_h, z^*). This result is useful is unsurprising, the policy-maker acts as a classic public policy maker and sets the mechanism so that any attacking externalities are internalised by the targets. A less intuitive fact is that it is the policy-makers discount rate $\bar{\beta}$ that determines if, from the viewpoint of the targets with discount rate β, a Pareto efficient solution has been achieved.

Therefore when $\beta \neq \bar{\beta}$ a natural antagonism will exist between the targets and the policy-maker and if the policy-maker requires, periodically for instance, to have their power to set $(\bar{x}_l, \bar{x}_h, \bar{z})$ ratified by the targets then it is likely that $\bar{\beta} \to \beta$, however if the individual targets have heterogeneous discount rates then the policy-maker will never be able to attain the Pareto efficient solution, unless each target is allowed to state their own discount rate. The issue occurs that targets may overstate their discount rates (we can consider the security resource allocation to be part of a wider investment bundle for the targets) and as such the targets will simply tend back to the Nash equilibrium. We leave extended discussion of this effect to future work.

Moving back to the simplified ex-ante identical targets example, further interesting cases can be analysed by restricting either the action set and/or the information set of the policy-maker. Indeed, these cases present the type of situations where the policy-maker is unable to maintain the resilience of the ecosystem of targets in the presence of shocks to specific parameters (we will focus on shocks to the technology parameters $\alpha_{i\in\{l,h\}}$ and $\psi_{i\in\{l,h\}}$. We will focus on the fully informed policy-maker with limited action and finally the partially informed policy-maker with limited action.

ANNEX2.2.4 Full Information with Limited Action: Majority and Minority Cases

First, let us consider the case whereby the policy-maker can observe $x_{i\in\{l,h\}}$ and z, but can only impose constraints on x_h and z. We designate this the *majority-action-case*, i.e. the policy-maker controls the majority of variables affecting the allocation bundle (two variables) and the individual agents control a minority of it (one variable).

A similar case occurs when the the policy-maker can only impose constraints on x_h and x_l, but observes z, the results are intuitively identical). In this case targets x_h and z are now exogenous and their problem reduces to a one dimensional optimisation problem that seeks to minimize

$$\tilde{x}_l(z, x_h, \eta_l, \eta_h) = \arg\min_{x_l} \int_{t_0}^{T} e^{-\beta t} \left(z\tilde{\sigma}_l\left(x_l, \eta_l\right) L + (1-z)\tilde{\sigma}_h\left(\bar{x}_h, \eta_h\right) L\right) dt + x_l + x_h \tag{10}$$

where $\tilde{x}_l(z, x_h, \eta_l, \eta_h)$ is the targets optimal solution to x_l as a function of the now imposed values of x_h, z and the attacker intensity choices η_l and η_z. The intuition behind this approach is that the policy-maker sets some collection of rules that identify the allocation z and then impose some investment on that allocation x_h. The optimal bundle of (x_h, z) from the view-point of the policy-maker is denoted $(\bar{x}_h, \bar{z})$. The policy-maker therefore solves the other two thirds of the allocation using the following objective function

$$(\bar{x}_h, \bar{z}) = \arg\min_{x_h, z} \int_{t_0}^{T} e^{-\bar{\beta} t} \left((1-z)\tilde{\sigma}_l\left(\tilde{x}_l\left(z, x_h, \eta_l^\diamond, \eta_h^\diamond\right), \eta_l^\diamond\right) L + z\tilde{\sigma}_h\left(x_h, \eta_h^\diamond\right) L\right) dt + \tilde{x}_l\left(z, x_h, \eta_l^\diamond, \eta_h^\diamond\right) + x_h \tag{11}$$

where $\eta^\diamond_{i\in\{l,h\}}$ is the solution to the attacker intensities give in Equation 7, however the policy-maker anticipates the reaction of the target into the objective function for x_l.

In this instance almost all of the policy-maker objectives in (x_l, x_h, z) from can be achieved as the policy-maker can impose themselves on two out of the three degrees of freedom in the model. We can also see implicitly that when $\bar{\beta} = \beta$, i.e. the policy-maker and targets have aligned time preferences, then the policy-maker will achieve a broadly similar risk profile to the case when the policy-maker controls all of the degrees of freedom (x_l, x_h, z). Whilst the policy-maker can attain their risk trade-off they do so at a lower level of efficiency (in terms of total initial cost $x_l + x_h$) than if the policy-maker controlled (x_l, x_h, z). Unless an arbitrary upper bound is placed on $x_h + x_l$ the policy-maker can achieve a global minima for any given combination of $\alpha_{i\in\{l,h\}}$ and $\psi_{i\in\{l,h\}}$, by imposing a shift of assets (if necessary) into their domain. In the extreme case when $\bar{z} \to 1$, the policy-maker has control over all assets and sets an unbounded investment in protection of $\bar{x}_h$ as essentially one dimensional optimization problem.

Reducing the policy-makers action space to only one of the three allocation variables (designated the minority action case) provides a far greater limitation to their action space and now substantially impairs the policy-makers' ability to internalise the attacker externalities and adjust the total level of risk in response to a change in $\alpha_{i\in\{l,h\}}$ or $\psi_{i\in\{l,h\}}$. However, the circumstances under which a policy-maker would be able to observe, but have no direct influence on behaviour violates one of the previously stated roles of the policy-maker in the ecosystem. We leave the motivation and analysis of this fully informed, but substantively limited policy-maker to future work.

ANNEX2.2.5 The Partially Informed policy-maker with Limited Action: Minority Case

We skip the fully informed policy-maker with limited action case and move directly to a partially informed policy-maker with minority-action. This, in theory, is the most interesting case as it illustrates the limitations of the policy-makers actions in response to changes in $\alpha_{i\in\{l,h\}}$ or $\psi_{i\in\{l,h\}}$ and also illustrates that with limited information the policy-maker can in fact provide a worse global outcome than the Nash equilibrium without the policy-maker.

Let the policy-maker observe and enforce only x_h. The policy-maker can observe and internalise the externality in η_h, but cannot observe or enforce z and x_l. The targets then choose the investment and allocation bundle (x_l, z) following:

$$(\tilde{x}_l, \tilde{z}; x_h, \eta_l, \eta_h) = \arg\min_{x_l,z} \int_{t_0}^{T} e^{-\beta t} \left(\bar{z}\tilde{\sigma}_l\left(x_l, \eta_l\right) L + (1-\bar{z})\tilde{\sigma}_h\left(\bar{x}_h, \eta_h\right) L\right) dt + x_l + x_h \tag{12}$$

the policy-maker now solves the following minority optimization given the policy-makers information set:

$$\bar{x}_h(\eta_h) = \arg\min_{x_h} \int_{t_0}^{T} e^{-\beta t} \left(\hat{L}\tilde{\sigma}_h\left(\bar{x}_h, \eta_h^{\diamond}\right)\right) dt + x_h \tag{13}$$

where $\eta_h^{\diamond}$ is the solution to the attacker entry problem from Equation 3, but only for the h asset class, from the policy-makers point of view this is now:

$$\int_{t_0}^{T} e^{-\delta t}\tilde{\zeta}_h\eta_h^{-1}\tilde{\sigma}_h\left(x_h, \eta_h\right) dt = \gamma \tag{14}$$

Note that the policy-maker now takes $\hat{L}$ as the value of losses, this is because the policy-maker can no longer identify zL and $(1-z)L$, the policy-maker is simply given $\hat{L}$ by the targets at an a-priori stage and is assumed to be exogenous. Similarly, whilst $\tilde{\zeta}_h$ is equal to z from the viewpoint of attackers and targets it is simply a parameter unrelated to the overall asset allocation of the targets from the point of view of the policy-maker. The policy-maker is now unwittingly, not a Stackelberg policy maker, but in a Nash equilibrium with the targets and attackers.

The attackers are also solving their entry and exit decision for assets in allocation l, following $\int_{t_0}^{T} e^{-\delta t}\tilde{\zeta}_l\eta_l^{-1}\tilde{\sigma}_l\left(x_l, \eta_l\right) dt = \gamma$ this is unobserved from the point of view of the policy-maker, but is accounted for as part of a Nash equilibrium by the targets. For tractability we assume that from the viewpoint of the attackers $\tilde{\zeta}_h$ is set exogenously and at a fixed ratio to $\hat{L}$. There is no loss of generality ($\hat{L}$ is exogenous by construction and $\tilde{\zeta}_h$ are already set in a pre-optimisation between the attackers and the policy-maker) and we are specifically interested in the reaction of targets setting x_l and attackers choosing η_l, to demonstrate the natural limits that appear in the game.

Proposition 3a: Attackers and policy-maker in asset class h

When $\tilde{\sigma}_i = e^{-\psi_i x_i}\eta_i^{\alpha_i}$, for $i \in \{l, h\}$, the policy-maker's objective function is as stated in Equation 13 and the attacker dynamics are as those given in Equation 14 the policy-makers optimal mandated investment allocation is

$$\begin{aligned}\bar{x}_h &= \frac{1-\alpha_h}{\psi_h}\log(\hat{L}(e^{bT}-1)\psi_h) - \frac{\alpha_h}{\psi_h}\log(\gamma\delta(\tilde{\zeta}e^{\delta T}-\tilde{\zeta})) \\ & \frac{1}{\psi_h}(\log(\bar{\beta}\alpha_h - \bar{\beta})(1-\alpha_h) + \alpha_h T(\bar{\beta}-\delta) - \bar{\beta}T). \qquad (15)\end{aligned}$$

Following from the policy-maker's choice the attacker intensity given the policy-maker actions $\bar{\eta}_h$ is given by

$$\bar{\eta}_h = \left(\frac{\tilde{\zeta}\left(e^{\delta T}-1\right)e^{-\bar{x}_h\psi_h-\delta T}}{\gamma\delta}\right)^{\frac{1}{1-\alpha_h}} \qquad (16)$$

where $\bar{x}_h$ is as defined in Equation 15.

Proof: is presented in the §. Note, that the policy-makers' choice is effectively determined by three variables $\hat{L}$, $\tilde{\zeta}_h$ and $\bar{\beta}$, we shall assume that these are, a priori, in policy-maker's information set. It is worth reiterating that at this stage decisions regarding z, x_l and η_l are by construction not included in this optimization. However, we do not have to impose these restrictions, as the derivative of the policy-makers objective function given the multiplicative form of $\tilde{\sigma}_i = e^{-\psi_i x_i}\eta_i^{\alpha_i}$, for $i \in \{l, h\}$ with respect to x_h does not include x_l and η_l. So the only implicitly restricted information is replaced by $\hat{L}$, $\tilde{\zeta}_h$. This neat result is of course notreplicated for more complex forms of $\tilde{\sigma}_i$ which affect the behaviour of attackers in asset class h.

Proposition 3b: Attackers and targets in asset class l

We now move to the targets and attackers new equilibrium. When $\tilde{\sigma}_i = e^{-\psi_i x_i}\eta_i^{\alpha_i}$, for $i \in \{l, h\}$ and the targets' objective is as specified in Equation 12 the the equilibrium allocation bundle x_l, z will be

$$\begin{aligned}x_l^{\ddagger} &= -\frac{1}{\psi_l}\log(\bar{\eta}_h^{\alpha_h}) + \frac{\alpha_l}{\psi_l}(\log(\bar{\eta}_h^{\alpha_h}) + \log(\beta(e^{\delta T}-1)\bar{\eta}_h^{-\alpha_h}) - \qquad (17) \\ & \log(\gamma\delta\psi_l(e^{\beta T}-1)L) + \beta T - \delta T) + \bar{x}_h\psi_h \\ z^{\ddagger} &= \frac{\beta\bar{\eta}_h^{-\alpha_h}e^{\bar{x}_h\psi_h+\beta T}}{L\psi_l(e^{\beta T}-1)}, \qquad (18)\end{aligned}$$

and the attacker intensity η_l is given by

$$\eta_l^{\ddagger} = \left(\frac{z\left(e^{\delta T}-1\right)e^{-x_l^{\ddagger}\psi_l-\delta T}}{\gamma\delta}\right)^{\frac{1}{1-\alpha_l}}. \qquad (19)$$

Proof: Is provided in § ANNEX2.5.3. Note that we use the $\ddagger$ to denote this new equilibrium for the targets as it is not strictly a Nash equilibrium solution as that stated in Proposition 1a.

ANNEX2.2.6 Measuring Resilience

Measuring the impact of technological shocks to $\alpha_{i,i\in\{l,h\}}$, $\psi_{i,i\in\{l,h\}}$ and economic shocks to $\bar{\beta}$, β, δ, L and γ is a tricky task and requires creation of an arbitrary metric. In this case we combine the equilibrium values of $x_{i\in\{l,h\}}$, z and $\eta_{i\in\{l,h\}}$, using an total non-discounted loss function for the risk component only, this is given as follows

$$\begin{aligned}
\tilde{V}_A(\tilde{v},\tilde{u}) &= \int_{t_0}^{\tilde{T}} \tilde{z}\tilde{\sigma}_l\left(\tilde{x}_l,\tilde{\eta}_l\right)L + (1-\tilde{z})\,\tilde{\sigma}_h\left(\tilde{x}_h,\eta_h\right)Ldt && (20)\\
\tilde{v} &= (\tilde{z},\tilde{x}_{i\in\{l,h\}},\tilde{\eta}_{i\in\{l,h\}}) && (21)\\
\tilde{u} &= (\alpha_{i,i\in\{l,h\}},\psi_{i,i\in\{l,h\}}) && (22)
\end{aligned}$$

where $\tilde{T} = \log(\lambda)/\theta$ and $\theta = \min(\bar{\beta},\beta,\delta)$, for an arbitrary number λ, we assume this to be ten, so the simulation covers 90% of the future value. $\tilde{v}$ is the collection of choice variables under the various policy options and is detailed below. $\tilde{u}$ is the collection of technology shocks under consideration.

Other sensitivity metrics can be used (for instance the same as above, however discounting at the policy-maker discount rate. However, part of our stress test is to evaluate the impact of varying $\bar{\beta}$, therefore to ensure this is fair experiment we have decided to use the functional form provided in Equation 20.

To derive the sensitivity of the system to technology shocks we substitute the functional forms for $x_{i\in\{l,h\}}$, z and $\eta_{i\in\{l,h\}}$ into Equation 20 and then compute the four partial derivatives with respect to $\alpha_{i,i\in\{l,h\}}$, $\psi_{i,i\in\{l,h\}}$ to give a combined sensitivity metric. We divide the evaluation of these partial derivatives into the three cases covered in the paper, Nash equilibrium in the absence of the policy-maker, the fully informed policy-maker and the partially informed policy-maker with minority action case.

The response function to technology shocks is the numerical evaluation of the following ordinary differential equation

$$\begin{aligned}
\tilde{I}(\tilde{u}) &= \int_{t_0}^{\tilde{T}} \frac{\partial\tilde{z}}{\partial\tilde{u}}\tilde{\sigma}_l\left(\frac{\partial\tilde{x}_l}{\partial\tilde{u}},\frac{\partial\tilde{\eta}_l}{\partial\tilde{u}}\right)L + \frac{\partial(1-\tilde{z})}{\partial\tilde{u}}\tilde{\sigma}_h\left(\frac{\partial\tilde{x}}{\partial\tilde{u}},\frac{\partial\tilde{\eta}}{\partial\tilde{u}}\right)Ldt, && (23)\\
\tilde{u} &= \{\alpha_{i\in\{l,h\}},\psi_{i\in\{l,h\}}\}
\end{aligned}$$

where each case has a set of functional forms for $\tilde{z}$, $\tilde{x}_{i\in\{l,h\}}$ and $\eta_{i\in\{l,h\}}\}$. We have denoted the three cases as follows: $\tilde{v} = v^*$ and $\tilde{u} = u^*$ for the Nash equilibrium, $\tilde{v} = \bar{v}$ and $\tilde{u} = \bar{u}$ for the fully informed policy-maker and $\tilde{v} = \bar{v}^\ddagger$ and $\tilde{u} = \bar{u}^\ddagger$ for the partially informed policy-maker with minority action case.

Let $\tilde{V}_A(v^*,u^*)$ and $\tilde{I}(u^*)$ be, respectively, the total non-discounted loss for the risk component under the Nash equilibrium and the corresponding collection of response functions. Similarly let $\tilde{V}_A(\bar{v},\bar{u}),\tilde{I}(\bar{u})$ and $\tilde{V}_A(\bar{v}^\ddagger,\bar{u}^\ddagger),\tilde{I}(\bar{u}^\ddagger)$ be, respectively, the same pair of function and collection of functions for the fully informed policy-maker and the partially informed policy-maker with minority action cases.

We can measure the effectiveness of the policy-maker by comparing $\tilde{V}_A(v^*,u^*)$ to $\tilde{V}_A(\bar{v},\bar{u})$. We can also evaluate the erosion in risk reduction caused by restricting the policy-makers informations set and action space by pairwise evaluation of $\tilde{V}_A(v^*, u^*)$ and $\tilde{V}_A(\bar{v}, \bar{u})$ with $\tilde{V}_A(\bar{v}^\ddagger, \bar{u}^\ddagger)$

To examine the impact of shocks and measure resilience we compare the response functions $\tilde{I}(u^*)$ and $I(\bar{u}^)$ to evaluate the impact of the fully informed policy-maker. Finally, we can compare the resilience of the system when the policy-makers information set is restricted by comparing $\tilde{I}(u^*)$ and $I(\bar{u}^)$ to $I(\bar{u}^\ddagger)$, for varying sizes of shocks in $\tilde{u}$. In particular we will focus on $\alpha_{i \in \{l,h\}}$.

ANNEX2.2.7 Discussion

The various forms of the model, we have proposed, assumes that targets are ex-ante identical. This is of course a simplifying assumption to lend tractability to the derivation and illustration of the specific effects that we are attempting to identify. However, this is not as limiting an assumption a would initially be presumed.

The issue with heterogeneity of target type (in terms of vulnerability or magnitude of loss) is that once we assume a policy-maker in the role of a policy maker determining mandatory investments this policy-maker would necessarily have to identify each targets Pareto efficient investment. For a large cross section of targets this could potentially be a costly information gathering exercise.

In [21] the need for correct identification of target type is a necessary, but not sufficient, requirement for the policy-maker in determining the Pareto efficient investment allocation. If the policy-maker imposes mandatory investment in response to the voluntary information disclosure of a targets vulnerability characteristics (thus reducing the costly information gathering exercise).

However, targets may be incentivised to under-disclose their characteristics (for instance due to budget pressures) and the remediation action of the policy-maker is therefore rendered ineffective. A standard approach to this is contingent audit, see for instance early research in this area in [23, 24] and later work in [25, 26]

In this case targets are asked to declare their characteristics by the policy-maker, in terms of vulnerability and magnitude of loss. In the event of an incident there is a chance of audit (with known likelihood) and a large penalty (necessarily large enough for incentive compatibility) for incorrect prior identification to the policy-maker. If the target has correctly identified their characteristics then no fine is levied.

For the types of model proposed in [21, 22] this approach would allow the policy-maker to coordinate and mandate investment allocations with targets declaring their own vulnerability and loss characteristics. The allocation would therefore be Pareto efficient from the viewpoint of the policy-maker. However, the allocation will not necessarily be Pareto efficient from the viewpoint of the target as the policy-maker and target time preferences may be divergent.

This is further exaggerated when the targets have the ability to hide assets from the policy-maker. When the policy-makers discount rate is very low relative to the targets then under certain cases of the model targets will move their assets to the class labelled h, by decreasing z substantially towards zero. This leaves very few assets in class h regulated by the policy-maker.

When shocks (say to the elasticity of the technology of attack in class l denoted α_l) result in a higher level of viable attacking intensity in equilibrium, then targets can either choose to shift their assets to h by decreasing z or try to cope with the increasing attacks in I. Unfortunately, the game between attackers and targets in I achieves an equilibrium with externalities. Moreover, for certain versions of the model, the total risk when the policy-maker takes action without observing x_l and z may be substantially higher (by orders of magnitude) than if the targets and attackers achieved a Nash equilibrium in the absence of the policy-maker. We will demonstrate this case in §(ANNEX2.3).

An obvious further question arises, as why the targets do not inform the policy-maker of z and x_l? It might be possible to only recover the target type from explicitly described information systems (such as those regulated under national critical infrastructure legislation). The forced revelation of type argument above, therefore only works for the information asset types covered under the policy-makers mandate.

Several rationales can be put forward to explain why the common knowledge assumption of z and x_l might not be shared with the policy-maker by the targets. First, if β is much larger than $\bar{\beta}$ then the targets do not share the sustainability objectives of the policy-maker defined in terms of their time preferences (the targets are far shorter term than the policy maker), therefore the targets may make a strategic choice, in an initial sub-game, to hide z and x_l from the policy-maker. Second, an alternative explanation that does not require another greater mechanism to explain it, is that the targets and policy-maker initially entered into a Stackelberg arrangement that is binding to the policy-maker (to accomplish some sustainability target and internalize externalities in x_h). The policy-maker sets x_h within the framework of the original agreement and this optimization rule continues through the life of the ecosystem, even when potentially new assets x_l exist.

Indeed, The policy-maker may simply not have the information processing power to supervise all assets and then cover them under relevant tort law liability conditions, for the targets self revelation approach to work. If there are a very large number of targets with highly diverse information assets then the ability to fully audit may not be possible. Obviously the model assumes company types in x_l are ex-ante homogenous.

One can think of a set of regulations (in the form of fixed rules) designed by the policy-maker and requiring the disclosure of targets' assets such that the investment x_h internalises attacker externalities across targets (on the assumption that this is the complete set of assets). However, after a time, new assets not covered by the rules appear, or methods that allow targets to de-recognize these assets from the policy-maker now exist.

We now move onto a worked example that illustrates our modelling approach in a specific business context.

ANNEX2.3 Application to ICS/SCADA and Corporate Networks

Industrial control systems (ICS) are ubiquitous in most large industrial firms and related organisations. A further common type of ICS are supervisory control and data acquisition (SCADA) systems. These systems are designed to automatically or semi-automatically control industrial processes. Examples of such systems can be found in petroleum exploration and processing, gas distribution, bulk electricity transmission, various parts of the nuclear industry and most manufacturing processes. Similar, or identical types of systems may be found in defensive applications, such as automatic air defence systems.

ICS/SCADA systems are often very complex and deal with a large number of different types of sensors and actuators affecting the various aspects of the system in question. IC-

S/SCADA systems and the security of ICS/SCADA systems is not a new topic however, when many of the ICS/SCADA systems were first installed they were viewed as standalone assets and as such the major security concern was physical access to the control system or by physically tapping directly into the data acquisition sensors and/or the control communications to actuators. For our purposes this distinction between ICS and SCADA is non critical and we shall refer generically to ICS/SCADA as a single type of assets within a target organization.

Our main question centres on whether a firm would seek to adjust its declared mix of ICS/SCADA and corporate information assets (we explicitly do not include physical assets in this example) to avoid costly regulation. We will assume that there exists some legacy regulation of certain types of ICS/SCADA systems and that firms can choose to replace some or all of the information architecture of theses systems with analogous technologies run on an unregulated corporate network.

For a closed ICS/SCADA system to inflict damage traditionally an attacker would need a) a-priori information on the function of the ICS/SCADA system and b) if it is an analogue system, knowledge of the individual communication lines between the ICS/SCADA system and the sensors and actuators. The attacker would also need to understand the various states of the system and why and how the ICS/SCADA system adjusted to various different stimuli. As the attack would need to have some form of physical penetration this knowledge would need to be obtained prior to the attack.

However, a recent trend has seen a greater integration of corporate networks and ICS/ SCADA systems. The reasons for this integration are complex, but in most cases are driven by the need for greater flexibility and the cost reduction associated with a more networked organisation. For instance, instead of having operator input from each physical site, system oversight can be run centrally with communications via internet protocol (IP) and cellular data (denoted 3G) communications networks.

With this shift to a networked organisation, where standard corporate network assets and physical ICS/SCADA assets have high levels of interoperability comes obvious security risks. For certain types of industry, for instance bulk electricity transmission, most ICS/ SCADA assets have systematic security controls placed on them by public policy makers acting on behalf of society as a whole (performing the policy-maker role). In the US 1,900 bulk power system operators are regulated by The North American Electric Reliability Corporation (NERC), a not for profit organisation with the role of coordinating the individual operators.

Each operator will have a ICS/SCADA system that manages the bulk electricity transmission in their area. This will be a network of communications that monitor the physical network of power cables, transformers and substations. We can think of this as an information ecosystem with individual information assets and we will assume that this is analogous to our *h* asset class.

In addition to the ICS/SCADA assets, the various operators have corporate networks that provide on-going information services for the normal business activities for each operator. The information assets stored in this information ecosystem are designated the *l* assets. The corporate network has many of the same features as the ICS/SCADA system from an information perspective and there are elements of substitutability between the two. For instance, an operator could phase out using expensive fibre optic cables to communicate between ICS/SCADA systems and substations and replace this with a IP or 3G type communications.

A successful penetration of a corporate network that is integrated with an ICS/SCADA now provides attackers with a potentially more effective means of attacking the ICS/ SCADA system. The attacker can sit an learn the systems properties via sampling and observation of the ICS/SCADA systems normal operation and then use this information to either provide a-priori information to improve the chance of success of a physical attack or actually attack the ICS/SCADA system directly through the corporate network.

As a community of targets, systematic under investment across all targets leads to increased attacking intensity and this provides a negative externality that requires coordination across targets in order to internalise this cost. We will illustrate three cases for this example, first where targets are unregulated and choose investment using the Nash equilibrium approach in §(ANNEX2.2). We will then demonstrate the improvement that can be achieved by the fully informed policy-maker. Finally, we will illustrate the deterioration in security when targets can shift assets from the oversight of the policy-maker and the policy-maker can no longer mandate investment. In each case we will illustrate the change in total risk with shocks to attacker elasticities and why targets may find it attractive to move assets from a regulated to an unregulated environment.

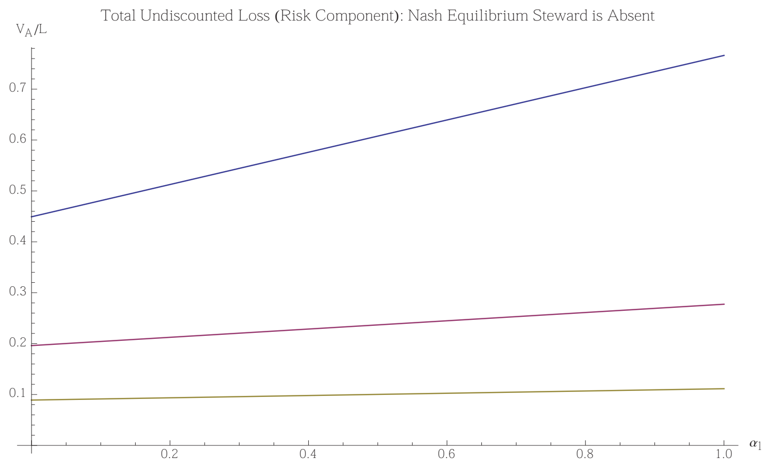


Figure 4: Nash equilibrium total non-discounted loss function $\tilde{V}_A$ as a function of α_l. Note that as attacking technology increases total also increases almost linearly over a reasonable range of α_l.

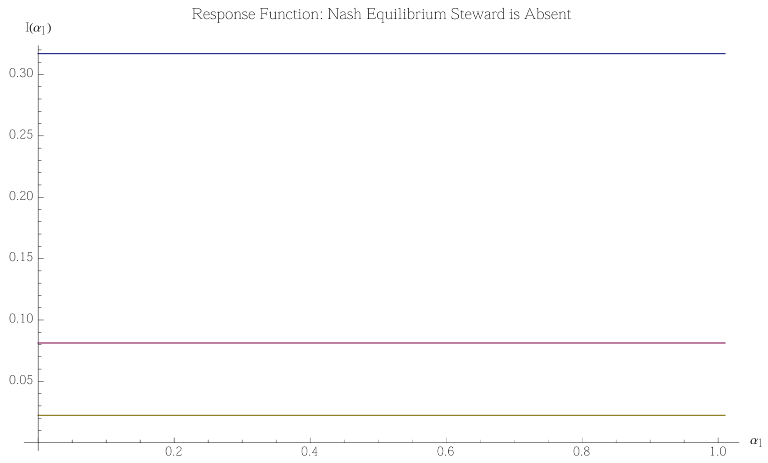


Figure 5: Nash equilibrium response function $\tilde{I}(\alpha_l)$ as a function of an increasing shock in α_l, the abscissa values. The response function represents the transmission rate of the shock in α_l is almost constant for a given $\psi_{i\in\{l,h\}} = \psi$, which effectively determines the order of magnitude of the adjustment.

ANNEX2.3.1 Simulation for Bulk Electricity Transmission

This simulation is designed to provide an overview of the intuition of our model and is not supposed to provide specific quantification for our proposed application. However, we have tried to stay close to real data when possible.

Let us assume that targets have a discount rate of 20% per annum ($\beta = \log(6/5)$ continuous growth rate), in this case when $\lambda = 10$, the target time overall horizon is $T = 12.3$ years. This appears to be a reasonable assumption for the amortisation of information assets within a firm see for an example survey in [27]. For electricity transmission in the United States the dichotomy between physical and information assets can be found in [28, 29].

We will assume that the societal discount rate used by the policy-maker is much lower and ranges from $\bar{\beta} \to 0$ to $\bar{\beta} \to 1/10$. In [22] we outline the various debates on the appropriate social discount factor to be applied in public policy scenarios. For certain areas of public policy debate such as climate change discount rates approaching zero a common for certain economic arguments relating to low carbon policies. For information policy the requirement is not so acute but significant differences between firm discount rates and societal discount rates remain.

For our starting numerical example we shall assume that $\psi_l = \psi_h$, i.e. the relative marginal risk reduction from investment in both asset classes is identical and fixed we shall assume that it is 1/100, 1/10 and 1/2, to represent low, medium and high effectiveness bands. This is a more difficult assumption to justify as there is very little literature on the efficacy of investment in security in this area, therefore our simulation covers a wide range of reasonable bands.

We shall arbitrarily fix $L = \$1\text{Million}$ as an example and divide all losses by L to give a per dollar at risk measure. $\hat{L}$ is assumed to be half L, starting from the Nash equilibrium assumption when $\psi_l = \psi_h$ and it follows that $\tilde{\zeta} = 1/2$.

For the attackers, we set their discount rate $\delta = \log(11/10)$ or a 10% discrete rate of return. From the view point of attackers the discount rate is analogous to an investment rather than the depreciation and amortization viewpoint of the targets. The most difficult parameter to set in the simulation is γ as almost no data exists on the cost per attack to reward ratio. When $\gamma \to 0$ the cost per attack divided by reward indicates that either the rewards are very high or that the cost per attack is very low. When $\gamma = 0$ attacking intensity is infinite, this has not been observed, therefore we stick to finite values of $\gamma = 1/10$ or a 10% cost-reward ratio. The shock of interest is to the elasticity of attack $\alpha_{i\in\{l,h\}}$ and in particular shocks to α_l.

Figures 4 and 5 present the functions $\tilde{V}_A$ and $\tilde{I}$ as a function of α_l, the attacker elasticity. Inspection of the plots affirms the basic logic of the Nash equilibrium version of the model. The most important term in remediating shocks to $\alpha_{i\in\{l,h\}}$ is $\psi_{i\in\{l,h\}}$, of interest when comparing to the fully informed policy-maker is the fact that $\tilde{I}(\alpha_l)$ is almost constant over a variety of adjustments in α_l, this means that even though the shock is increasing linearly the system can only adjust in a linear manner to the new Nash equilibrium.

By contrast Figures 6 and 7 illustrate a different effect. As shocks to the attacking elasticity α_l increases the policy-maker utilizes the collective component to reduce the attacking intensity (rather than keeping the risk down by defensive effort x_l) the derivative of $\partial\bar{\eta}_l/\partial\bar{x}_l$ is now more important than $\partial\tilde{\sigma}_l/\partial\bar{x}_l$, where η_l is constant. The policy-maker therefore finds an optima by driving away all the attackers (as even small numbers are now very effective).

We see that for all values of ψ, the fully informed policy-maker provides a lower total non-discounted loss than the Nash equilibrium. This illustrates the beneficial effect of the policy-maker, however, with larger values of ψ the absolute effect decreases. However, the major benefit of the policy-maker is in suppressing and adjusting the ecosystem to shocks and this effect is demonstrable for all three values of ψ.

Finally, we move to the partially informed policy-maker with minority action, the total non-discounted loss $\tilde{V}_A$ and response function $\tilde{I}$ for shocks in α_l are plotted in Figures 8 and 9. In this case the pattern is similar to the Nash equilibrium for small shocks. The targets, however have costly regulation in the h asset class and under investing in the l asset class.

Unfortunately in this case the there is a discontinuity at α_l = 1, so the total loss spikes, prior to the shift in assets from *l* to *h*. We can see that before the policy-maker can regulate the assets the total risk will traverse the discontinuity, before the policy-maker can actually manage the majority of assets that the targets have not declared. Here, we can see a case of an ecosystem that is not resilient and it lies within the feasible boundaries of our example parameter sets.

ANNEX2.4 Summary

This paper will make grim reading for any governmental, supra-governmental agency or firm that needs to act in a policy-maker capacity over a complex information ecosystem. We illustrate two contrasting issues that complicate the management of this type of ecosystem. First, for almost all conceivable target–attacker interactions the presence of a policy-maker is beneficial to overall risk reduction, by acting as a social coordinator and mandating investment that internalises externalities. Second, it is unlikely, however, that the time preferences of the policy-maker, acting on behalf of society, and the targets will be aligned and as such the targets may not have the correct incentive to reveal their true type to the policy-maker. In our framework this is in the form of hiding assets in an alternative unregulated asset class.

If the policy-maker is able to observe these assets and mandate the majority of the investment bundle then the policy-maker can still perform a beneficial role. However, when the policy-maker acts on minority information and has limited action, the effect can be far worse than the Nash equilibrium when the policy-maker is not present. Targets, maybe incentivized to store assets in increasingly insecure areas and this can substantially degrade the resilience of the ecosystem.

We have also provided a short example of this model using parameters designed to approximate the choice between holding information assets in a regulated ICS/SCADA system versus redeployment to a standard corporate information network. We demonstrate that a catastrophic scenario predicted by the model solutions under certain parameter configurations is possible for the domain of shocks assumed choices in this example.

Our major conclusions are also backed by qualitative analysis of the types of contracts an regulations needed to ensure that the policy-makers information set is sufficient to maintain the information ecosystem. It should be noted that the types of regulatory structures needed, transparent mandatory information sharing, audit in the event of an incident and penalties that compound when prior information sharing has proven to be false, are not commonly observed in the regulation of standard enterprise networks. However, for firms with assets of significant importance or interaction with to the critical infrastructure of nations and groups of nations this type of regulation may need to be commonplace. This could include supply chains to infrastructure providers and cloud service providers for very large groups of firms and individuals.

ANNEX2.5 Nash Equilibrium

ANNEX2.5.1 Proofs of Propositions 1a and 1b

Target Decision Making

Let $\tilde{\sigma}_{i\in\{l,h\}} : \mathbb{R}_+ \to [0,1]$. Evaluating the non stochastic integral of loss over $t_0 = 0$ to T we find an analytic form the the Target loss function:

$$V_L = \frac{1}{\beta} L\left(e^{\beta T} - 1\right) e^{-x_h\psi_h - x_l\psi_l - \beta T}\left(z e^{x_h\psi_h}\eta_l^{\alpha_l} - (z-1)\eta_h^{\alpha_h} e^{x_l\psi_l}\right) + x_h + x_l \tag{24}$$

differentiating with respect to $\tilde{x}_l$, $\tilde{x}_h$ and $\tilde{z}$ yields

$$\begin{aligned}
\frac{\delta \tilde{V}_L}{\delta x_l} &= 1 - \frac{1}{\beta} L z \psi_l \left(e^{\beta T} - 1\right) \eta_l^{\alpha_l} e^{-x_l\psi_l - T\beta} && (25)\\
\frac{\delta \tilde{V}_L}{\delta x_l} &= 1 - \frac{1}{\beta} L(1-z)\psi_h \left(e^{\beta T} - 1\right) \eta_h^{\alpha_h} e^{-x_h\psi_h - T\beta} && (26)\\
\frac{\delta \tilde{V}_L}{\delta z} &= \frac{1}{\beta} L\left(e^{\beta T} - 1\right) e^{-x_h\psi_h - x_l\psi_l - T\beta}\left(e^{x_h\psi_h}\eta_l^{\alpha_l} - \eta_h^{\alpha_h} e^{x_l\psi_l}\right) && (27)
\end{aligned}$$

Setting $\delta\tilde{V}_L/\delta x_l = 0$, $\delta\tilde{V}_L/\delta x_h = 0$ and $\delta\tilde{V}_L/\delta z = 0$ and solving simultaneously we derive the unconstrained optimal allocation $(x_l^\diamond, x_h^\diamond, z^\diamond)$ when attacking intensity (η_l, η_h) is exogenous, this is analytically derived as

$$\begin{aligned}
x_l^\diamond(\eta_l) &= \frac{1}{\psi_l}\log\left(\frac{(\lambda-1)L\psi_h\psi_l\eta_l^{\alpha_l}}{\beta\lambda\left(\psi_h + \psi_l\right)}\right) && (28)\\
x_h^\diamond(\eta_h) &= \frac{1}{\psi_h}\log\left(\frac{(\lambda-1)L\psi_h\psi_l\eta_h^{\alpha_h}}{\beta\lambda\left(\psi_h + \psi_l\right)}\right) && (29)\\
z^\diamond &= \frac{\psi_l}{\psi_h + \psi_l}. && (30)
\end{aligned}$$

Note that $z^\diamond$ is a simple ratio of ψ_h and ψ_l. In this model we apply no total budget constraint on x_h and x_l, e.g. $x_h + x_l = x$, so no Lagrange multiplier needs to be added at this stage.

Attacker Entry Conditions

Following from the target decision making process we derive the attacker function. For Proposition 1b attackers enter the market for attacks in each asset class until they break even problem when $\Pi_l = 0$ and $\Pi_h = 0$, we assume that attackers are randomly assigned targets with identical probability $1/N_T$ for each attack and that the first successful attacker wins the reward R. Let $\gamma = c/R$, the cost of attack to reward when $\tilde{\sigma}_{i\in\{l,h\}} : \mathbb{R}_+ \to [0,1]$, the profit functions for the attacker are as follows:

$$\Pi_l = \frac{1}{\delta} z \lambda^{-\frac{\delta}{\beta}}\left(\lambda^{\delta/\beta} - 1\right)\eta_l^{\alpha_l - 1} e^{-x_l\psi_l} - \gamma \tag{31}$$

$$\Pi_h = \frac{1}{\delta}(1-z)\left(\lambda^{\delta/\beta} - 1\right)\lambda^{-\frac{\delta}{\beta}}\eta_h^{\alpha_h - 1} e^{-x_h\psi_h} - \gamma \tag{32}$$

Solving each function for the break-even attacking intensities $\eta_l^\diamond(x_l)$ and $\eta_h^\diamond(x_h)$ we compute the aggregate attacker reaction functions:

$$\eta_l^\diamond(x_l) = \left(\frac{z\lambda^{-\frac{\delta}{\beta}}\left(\lambda^{\delta/\beta} - 1\right) e^{-x_l\psi_l}}{\gamma\delta}\right)^{\frac{1}{1-\alpha_l}} \tag{33}$$

$$\eta_h^\diamond(x_h) = \left(\frac{(1-z)\lambda^{-\frac{\delta}{\beta}}\left(\lambda^{\delta/\beta}-1\right)e^{-x_h\psi_h}}{\gamma\delta}\right)^{\frac{1}{1-\alpha_h}} \tag{34}$$

The simultaneous Nash equilibrium is the best reply of the target to the best reply of the attacker (and vice versa), which is the simultaneous solution of $\{x_l^\diamond, x_h^\diamond, z^\diamond, \eta_l^\diamond, \eta_h^\diamond\}$. Setting the Nash equilibrium defensive allocation (targets) and attacking intensity (attacker) as $\{x_l^*, x_h^*, z^*, \eta_l^*, \eta_h^*\}$

$$\begin{aligned} x_l^* &= \frac{\alpha_l}{\psi_l}\left(-\log\left(\gamma\delta L\psi_h\psi_l\left(e^{\beta T}-1\right)\right)+\log\left(\beta\psi_h\left(e^{\delta T}-1\right)\right)+\beta T-\delta T\right) \\ &\quad +\frac{1}{\psi_l}\log\left(\frac{L\psi_h\psi_l\left(e^{\beta T}-1\right)}{\beta\left(\psi_h+\psi_l\right)}\right)-T\beta \end{aligned} \tag{35}$$

$$\begin{aligned} x_h^* &= \frac{\alpha_h}{\psi_h}\left(-\log\left(\gamma\delta L\psi_h\psi_l\left(e^{\beta T}-1\right)\right)+\log\left(\beta\psi_l\left(e^{\delta T}-1\right)\right)+\beta T-\delta T\right) \\ &\quad +\frac{1}{\psi_h}\log\left(\frac{L\psi_h\psi_l\left(e^{\beta T}-1\right)}{\beta\left(\psi_h+\psi_l\right)}\right)-T\beta \end{aligned} \tag{36}$$

$$\eta_l^* = \left(\frac{\beta\left(e^{\delta T}-1\right)e^{\alpha_l\left(\log\left(\gamma\delta L\psi_h\psi_l\left(e^{\beta T}-1\right)\right)-\log\left(\beta\psi_h\left(e^{\delta T}-1\right)\right)+\beta(-T)+\delta T\right)+T(\beta-\delta)}}{\gamma\delta L\psi_l\left(e^{\beta T}-1\right)}\right)^{\frac{1}{1-\alpha_l}} \tag{37}$$

$$\eta_h^* = \left(\frac{\beta\left(e^{\delta T}-1\right)e^{T(\beta-\delta)+\alpha_h\left(\log\left(\gamma\delta L\psi_h\psi_l\left(e^{\beta T}-1\right)\right)-\log\left(\beta\psi_l\left(-\left(e^{\delta T}-1\right)\right)\right)-\beta T+\delta T\right)}}{\gamma\delta L\psi_h\left(e^{\beta T}-1\right)}\right)^{\frac{1}{1-\alpha_h}} \tag{38}$$

where $z^* = z^\diamond$. Assuming that $\alpha_{i\in\{l,h\}} > 0$, $\psi_{i\in\{l,h\}} > 0$, $L > 0$, $T > 0$, $\gamma > 0$, $\delta > 0$ and $\beta > 0$, then Equations 35 and 36 simplify to the result given in Proposition 1a and Equations 37 and 38 simplify to the equations given in Proposition 1b ■

ANNEX2.5.2 Proofs of Propositions 2a and 2b

policy-maker Decision Making Function

For the fully informed policy-maker setting $\bar{x}_{i\in\{h,l\}}$ and $\bar{z}$ the objective function is to minimize total aggregate loss for all targets. For our derivation the targets are all assumed to be identical therefore the policy-maker seeks to minimize

$$\tilde{V}_P = N_T\int_{t_0}^{T} e^{-\bar{\beta}t}\left(z\tilde{\sigma}\left(x_l,\eta_l^\diamond\right)+(1-z)\,\tilde{\sigma}\left(x_h,\eta_h^\diamond\right)\right)dt + N_T x_h + N_T x_l$$

when $\tilde{\sigma}_{i\in\{l,h\}}:\mathbb{R}_+\to[0,1]$, ${\eta^\diamond}_{i\in\{l,h\}}$ is derived from Equations 33 and 34. The asset allocation z does not have a tractable analytic solution in this case, so for exposition purposes we focus on x_l and x_h when z is fixed. In this case, let us fix z to the Nash equilibrium solution, therefore $\bar{z} = z^{diamond}$, from the Proof in Proposition 1a. Evaluating the integral from $t_0 = 0$ to

T and eliminating N_T yields:

$$\tilde{V}_P = \frac{L\left(e^{\beta T}-1\right)e^{-x_h\psi_h - x_l\psi_l - \beta T}\psi_h e^{x_l\psi_l}}{\beta\left(\psi_h+\psi_l\right)}\left(\frac{\psi_h\left(e^{\delta T}-1\right)e^{-x_h\psi_h - T\delta}}{\gamma\delta\left(\psi_h+\psi_l\right)}\right)^{\frac{\alpha_h}{1-\alpha_h}}$$

$$+\frac{L\left(e^{\beta T}-1\right)e^{-x_h\psi_h - x_l\psi_l - \beta T}\psi_h e^{x_l\psi_l}\psi_l e^{x_h\psi_h}}{\beta\left(\psi_h+\psi_l\right)}\left(\frac{\psi_l\left(e^{\delta T}-1\right)e^{-x_l\psi_l - \delta T}}{\gamma\delta\left(\psi_h+\psi_l\right)}\right)^{\frac{\alpha_l}{1-\alpha_l}} \tag{39}$$

This is now a two dimensional unconstrained optimization problem, where

$$\frac{\partial\tilde{V}_P}{\partial x_l} = \frac{L\psi_l^2\left(e^{\beta T}-1\right)e^{-x_l\psi_l - \beta T}}{\beta\left(\alpha_l-1\right)\left(\psi_h+\psi_l\right)}\left(\frac{\psi_l\left(e^{\delta T}-1\right)e^{-x_l\psi_l - \delta T}}{\gamma\delta\left(\psi_h+\psi_l\right)}\right)^{\frac{\alpha_l}{1-\alpha_l}} \tag{40}$$

$$\frac{\partial\tilde{V}_P}{\partial x_h} = \frac{L\psi_h^2\left(e^{\beta T}-1\right)e^{-x_h\psi_h - \beta T}}{\beta\left(\alpha_h-1\right)\left(\psi_h+\psi_l\right)}\left(\frac{\psi_h\left(e^{\delta T}-1\right)e^{-x_h\psi_h - \delta T}}{\gamma\delta\left(\psi_h+\psi_l\right)}\right)^{\frac{\alpha_h}{1-\alpha_h}} \tag{41}$$

setting $\partial\tilde{V}_P/\partial x_l = 0$ and $\partial\tilde{V}_P/\partial x_h = 0$ and solving for $\bar{x}_l$ and $\bar{x}_h$ we obtain the policy-makers solution

$$\bar{x}_l = \frac{-\left(1-\alpha_l\right)}{\psi_l}\times \tag{42}$$

$$\log\left(\frac{\left(1-\alpha_l\right)\beta\gamma^{-\frac{\alpha_l}{\alpha_l-1}}\delta^{-\frac{\alpha_l}{\alpha_l-1}}\psi_l^{\frac{1}{\alpha_l-1}-1}\left(\psi_h+\psi_l\right)^{\frac{1}{1-\alpha_l}}\left(e^{\delta T}-1\right)^{\frac{1}{\alpha_l-1}+1}e^{\beta T-\frac{\delta\alpha_l}{\alpha_l-1}T}}{L\left(e^{\beta T}-1\right)}\right)$$

$$\bar{x}_h = \frac{-\left(1-\alpha_h\right)}{\psi_h}\times \tag{43}$$

$$\log\left(\frac{\left(1-\alpha_h\right)\beta\gamma^{-\frac{\alpha_h}{\alpha_h-1}}\delta^{-\frac{\alpha_h}{\alpha_h-1}}\psi_h^{\frac{1}{\alpha_h-1}-1}\left(\psi_h+\psi_l\right)^{\frac{1}{1-\alpha_h}}\left(e^{\delta T}-1\right)^{\frac{1}{\alpha_h-1}+1}e^{T\left(\beta-\frac{\delta\alpha_h}{\alpha_h-1}\right)}}{L\left(e^{\beta T}-1\right)}\right)$$

Simplification of Equations 42 and 43 yield the solutions given in Proposition 2a.

Subsequent Attacker Intensity

By extension the attacker intensities under the fully informed policy-maker are obtained by substituting the optimal expenditures $\bar{x}_l$ and $\bar{x}_h$ into Equations 33 and 34, i.e.

$$\bar{\eta}_l = \left(\frac{\psi_l\left(e^{\delta T}-1\right)e^{\delta(-T)-\bar{x}_l\psi_l}}{\gamma\delta\left(\psi_h+\psi_l\right)}\right)^{\frac{1}{1-\alpha_l}} \tag{44}$$

$$\bar{\eta}_h = \left(\frac{\psi_h\left(e^{\delta T}-1\right)e^{\delta(-T)-\bar{x}_h\psi_h}}{\gamma\delta\left(\psi_h+\psi_l\right)}\right)^{\frac{1}{1-\alpha_h}} \tag{45}$$

Setting $i = \{h, l\}$ and $j = \{h, l\}$ for $j \neq i$ yields Equation 9 in Proposition 2b ■

The analytic forms of Equations 44 and 45 as a function of the model parameters are as follows:

$$\bar{\eta}_l = \left(\frac{\psi_l e^{\delta(-T)}\left(e^{\delta T}-1\right)}{\gamma\delta\left(\psi_h+\psi_l\right)}\right)^{\frac{1}{1-\alpha_l}} \times \tag{46}$$

$$\left(-\frac{\beta\left(\alpha_l-1\right)\gamma^{-\frac{\alpha_l}{\alpha_l-1}}\delta^{-\frac{\alpha_l}{\alpha_l-1}}\psi_l^{\frac{1}{\alpha_l-1}-1}\left(\psi_h+\psi_l\right)^{\frac{1}{1-\alpha_l}}\left(e^{\delta T}-1\right)^{\frac{1}{\alpha_l-1}+1}e^{T\left(\beta-\frac{\delta\alpha_l}{\alpha_l-1}\right)}}{L\left(e^{\beta T}-1\right)}\right)$$

$$\bar{\eta}_h = \left(\frac{\psi_h e^{\delta(-T)}\left(e^{\delta T}-1\right)}{\gamma\delta\left(\psi_h+\psi_l\right)}\right)^{\frac{1}{1-\alpha_h}} \times \tag{47}$$

$$\left(-\frac{\beta\left(\alpha_h-1\right)\gamma^{-\frac{\alpha_h}{\alpha_h-1}}\delta^{-\frac{\alpha_h}{\alpha_h-1}}\psi_h^{\frac{1}{\alpha_h-1}-1}\left(\psi_h+\psi_l\right)^{\frac{1}{1-\alpha_h}}\left(e^{\delta T}-1\right)^{\frac{1}{\alpha_h-1}+1}e^{T\left(\beta-\frac{\delta\alpha_h}{\alpha_h-1}\right)}}{L\left(e^{\beta T}-1\right)}\right).$$

ANNEX2.5.3 Proofs of Propositions 3a and 3b

The final case we consider in this paper considers the case when a policy-maker can only observe and mandate one of the elements of the investment allocation, x_h. The targets have discretion to signal a value $\hat{L}$, however the policy-maker does not know the true value of L or z.

The attackers signal a value $\tilde{\zeta}$, which we assume is actually $1-z$. Targets, still have to choose their asset allocation, but they can potentially hide it from a potentially costly investment allocation. For tractability we will assume this is in two steps, a signal of $\hat{L}$ and $\tilde{\zeta}$ and then an adjustment. This is done for tractable exposition, although the simultaneous model also has an analytic solution and provides a similar result, whilst being algebraically more complex.

The Targets Optimal Allocation Bundle

Let $\tilde{\sigma}_{i\in\{l,h\}} : \mathbb{R}_+ \to [0,1]$ and for the targets let x_h be exogenous. Targets minimize

$$\tilde{V}_T = \frac{1}{\beta}L\left(e^{\beta T}-1\right)e^{-x_h\psi_h-x_l\psi_l+\beta(-T)}\left(ze^{x_h\psi_h}\eta_l^{\alpha_l}-(z-1)\eta_h^{\alpha_h}e^{x_l\psi_l}\right)+x_h+x_l \tag{48}$$

Setting $\partial\tilde{V}_T/\partial x_l = 0$ and $\partial\tilde{V}_T/\partial z = 0$ and solving for x_l and z we obtain

$$x_l^{\diamond} = \frac{x_h\psi_h - \log\left(\eta_h^{\alpha_h}\eta_l^{-\alpha_l}\right)}{\psi_l} \tag{49}$$

$$z^{\diamond} = \frac{\beta e^{\beta T}\eta_l^{-\alpha_l}}{L\psi_l\left(\eta_h^{\alpha_h}\eta_l^{-\alpha_l}e^{\beta T-x_h\psi_h}-\eta_h^{\alpha_h}e^{-x_h\psi_h}\eta_l^{-\alpha_l}\right)} \tag{50}$$

Note that the both the optimal asset allocation $z^{\diamond}$ and the optimal investment $x_l^{\diamond}$ are now functions of x_h and are both subject to an upper bound of $\eta_i^* < e^{\alpha_i^{-1}x_i\psi_i}$.

The policy-makers Optimal Mandatory Investment

The policy-maker has received a information on $\hat{L}$ and $\tilde{\zeta}$, which in this derivation we treat as exogenous. However, the optimal initial bid of $\hat{L}$ from the targets to the policy-maker can be obtained by numerical analysis. The policy-maker sets a mandatory investment level of $\bar{x}_h$, from a restricted information set by minimizing

$$\tilde{V}_P = \frac{N_T}{\bar{\beta}} \hat{L} \left(e^{\bar{\beta} T} - 1 \right) \eta_h^{\diamond \alpha_h} e^{-\bar{\beta} T - x_h \psi_h} + N_T x_h \tag{51}$$

where

$$\eta_h^{\diamond} = \left(\frac{\tilde{\zeta} \left(e^{\delta T} - 1 \right) e^{-x_h \psi_h - \delta T}}{\gamma \delta} \right)^{\frac{1}{1-\alpha_h}} \tag{52}$$

solving the single equation and single unknown $\partial V_P / x_h = 0$, yields

$$\bar{x}_h = \frac{1}{\psi_h} \log \left(\mathcal{A} \right) + \frac{\alpha_h}{\psi_h} \left(T(\bar{\beta} - \delta) - \log \left(\mathcal{B} \right) \right) - \frac{\bar{\beta} T}{\psi_h} \tag{53}$$

Note that x_h is now a function of $\hat{L}$, $\tilde{\zeta}$ and the structural parameters δ, γ, $\psi_{i \in \{l,h\}}$, $\alpha_{i \in \{l,h\}}$ and T. Simplification of Equation 53 results in the policy-maker component of Proposition 3a. Substitution of $\bar{x}_h$ into Equation 52 provides the functional form of the attacker intensity $\bar{\eta}_h$ of Proposition 3a. The solution in terms of the model parameters is as follows:

$$\bar{\eta}_h = \mathcal{B}^{\frac{1}{1-\alpha_h}} e^{\alpha_h \left(\log(-\mathcal{A}) + T(\delta - \bar{\beta}) + T(\bar{\beta} - \delta) \right)^{\frac{1}{1-\alpha_h}}} \tag{54}$$

where

$$\mathcal{A} = \frac{\hat{L} \left(1 - e^{bT} \right) \psi_h \gamma^{\frac{1}{\alpha_h - 1} + 1} \delta^{\frac{1}{\alpha_h - 1} + 1} \tilde{\zeta}^{\frac{\alpha_h}{1-\alpha_h}} \left(e^{\delta T} - 1 \right)^{\frac{\alpha_h}{1-\alpha_h}}}{\bar{\beta} \left(\alpha_h - 1 \right)} \tag{55}$$

$$\mathcal{B} = \frac{\bar{\beta} \left(1 - \alpha_h \right) \gamma^{\frac{1}{1-\alpha_h} - 2} \delta^{\frac{1}{1-\alpha_h} - 2} \tilde{\zeta}^{\frac{1}{\alpha_h - 1} + 2} \left(e^{\delta T} - 1 \right)^{\frac{1}{\alpha_h - 1} + 2}}{\hat{L} \left(e^{bT} - 1 \right) \psi_h} \tag{56}$$

To derive the target allocation and attacker intensity $\eta_l^{\ddagger}$ we now simply need to substitute the functional forms of $\bar{x}_h$ and $\bar{\eta}_h$ into Equations 49 and 50 and simplify providing the functional forms in Proposition 3b for $x_l^{\ddagger}$ $z^{\ddagger}$ and $\eta_l^{\ddagger}$ are as follows.

$$\begin{aligned} x_l^{\ddagger} &= \frac{1}{\psi_l} \alpha_h (T(\bar{\beta} - \delta) - \log(\mathcal{A})) + \log(\mathcal{A}) - \bar{\beta} T \\ &\quad - \frac{1}{\psi_l} \log \left(\left(\frac{\beta \left(e^{\delta T} - 1 \right) e^{T(\beta - \delta)}}{\gamma \delta L \psi_l \left(e^{\beta T} - 1 \right)} \right)^{-\alpha_l} \left(e^{\alpha_h (\log(\mathcal{A}) - \bar{\beta} T + \delta T) + T(\bar{\beta} - \delta)} \right)^{\frac{\alpha_h}{1-\alpha_h}} \right) \end{aligned} \tag{57}$$

$$\begin{aligned} z^{\ddagger} &= \frac{\beta \mathcal{A}}{L \psi_l \left(e^{\beta T} - 1 \right)} e^{T(\beta - \bar{\beta}) - \alpha_h (\log(\mathcal{A}) + T(\delta - \bar{\beta}))} \times \\ &\quad \left(\mathcal{B} e^{\alpha_h (\log(\mathcal{A}) + T(\delta - \bar{\beta})) + T(\bar{\beta} - \delta)} \right)^{\frac{-\alpha_h}{1-\alpha_h}} \end{aligned} \tag{58}$$

$$\eta_l^{\ddagger} = \frac{\beta \left(e^{\delta T} - 1 \right) e^{T(\beta - \delta)}}{\gamma \delta L \psi_l \left(e^{\beta T} - 1 \right)} \tag{59}$$

which simplify to the equations in Proposition 3b ■

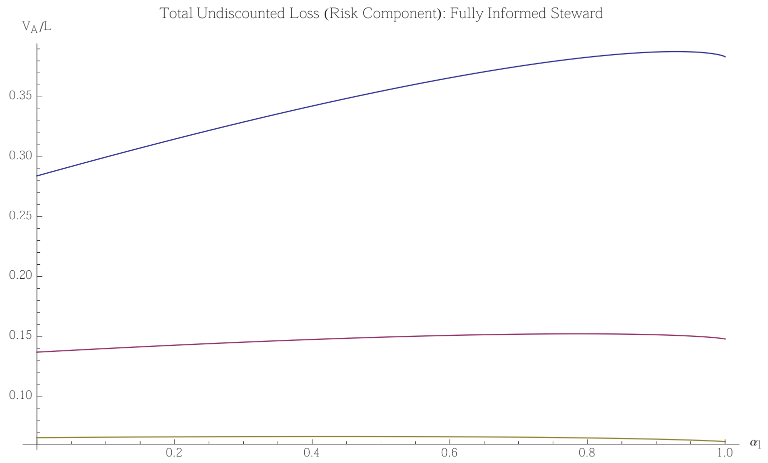


Figure 6: policy-maker total non-discounted loss function $\tilde{V}_A$ as a function of α_l. An important point to note is that this does not include the deterministic up front investment, so this curve can actually slope downwards, even with increasing α_l. The blue curve represents $\psi_l = \psi_h = \psi = 0.01$, the red curve $\psi = 0.1$ and the yellow curve is $\psi = 0.5$. Respectively, these values of ψ represent low, medium and high rates of risk reduction for additional investment.

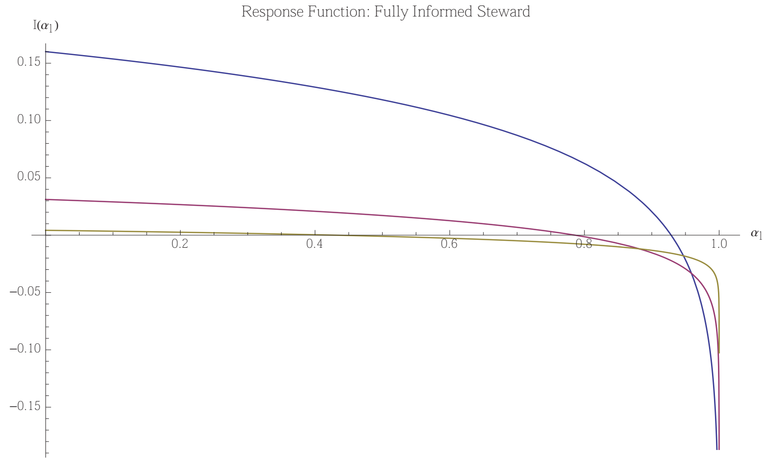


Figure 7: policy-maker response function $\tilde{I}(\alpha_l)$ as a function of an increasing shock in α_l, the abscissa values. Note that the policy-maker now takes a positive action and seeks to manage the direction of the shock, as α_l gets very big the policy-maker tolerates almost no attacking intensity and this effect is illustrated by the change in sign of the response.

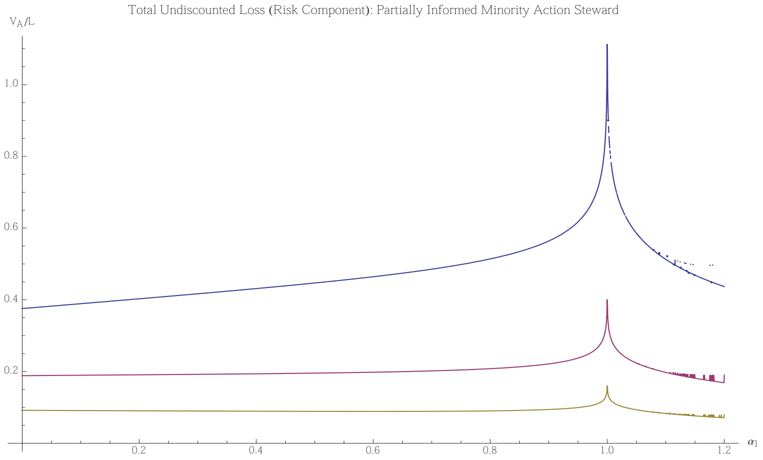


Figure 8: Partially informed policy-maker with minority action total non-discounted loss function $\tilde{V}_A$ as a function of α_I. In this case the targets maintain assets in the increasingly risky I class to avoid costly regulation in h, however a discontinuity exists at α_I causing the loss function to spike before the assets are shifted back to the regulated domain.

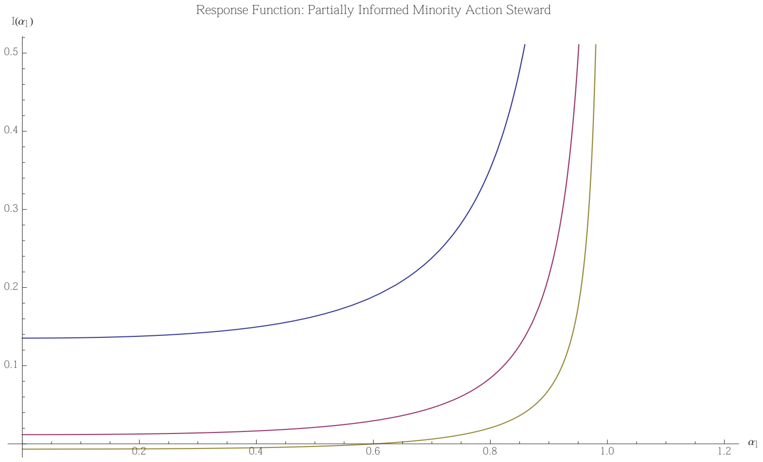


Figure 9: Partially informed policy-maker with minority action response function $\tilde{I}(\alpha_I)$ as a function of an increasing shock in α_I, the abscissa values. Note that after a shock of $\alpha_I \rightarrow 1$, the function $\tilde{I}(\alpha_I)$ is not defined.

ANNEX3. The Effect of Regulatory Structure upon Effective Cybersecurity Control for Critical Infrastructure: Models for the Electricity Transmission Sector

ANNEX3.1 Abstract

Choice of regulatory structure can have a profound impact upon the operational security behaviour of private firms running infrastructure that is deemed critical to society. In the electricity transmission sector, two types of structure are commonly discussed and contrasted, these being *rules-based* and *risk-based* regulation. This paper formulates mathematical and computational models to study the effects of (combinations of) these regulatory structures.

ANNEX3.2 Introduction

Many countries have chosen, or evolved, to have their bulk electricity transmission grids and systems operated by private firms rather than operating them as nationalised industries. Such grids are critical in the sense that their failure, or even partial failure, can have a severe impact upon the citizens that they ultimately serve. Policy-makers understand that resilience of the grid is essential and that there are large externalities in this sector [30].

There is a growing belief that grids are increasingly under attack — or at risk of attack — via their increasingly complex information systsms, by a range of actors, and that this trend will continue [31]. There is increasing awareness of this amongst policy-makers and the popular press [32]. The fact that the transmission system is a part of the critical national infrastructure means that it is necessary for policy-makers to find ways of ensuring that the transmission operators are incentivised appropriately to provide security of supply. In Europe, there has been considerable work done in providing an over-arching framework for security of supply [33, 34]. In particular, there must be appropriate incentives (interpreted broadly) for information security. The need for policy-makers to understand and get right the economics of critical infrastructure cybersecurity has been clearly explained by Anderson and Fuloria [35]

An important part of such incentive systems is regulation. There are often specific regulations that apply to the IT systems of transmission operators. Two primary types of regulatory regime for the IT of electricity transmission operators appear to be considered and contrasted. The first type is *rules-based*, in which a (possibly detailed) system of rules is communicated from (an agent representing) the policy-maker to the transmission operator; compliance with the rules is then monitored (often via a third-party external auditor) and the transmission operator is rewarded or punished accordingly (through a variety of mechanisms and institutions). The second type is *risk-based*, in which the transmission operator is charged with evaluating current and future risk (including security threats and vulnerabilities), and taking appropriate measures to mitigate that risk; communication of expectations from the policy-maker may be in explicit high-level principles, or implicit and through ongoing dialogue and negotiation; the operator is again rewarded or punished for (perceived) performance via a variety of mechanisms. In the UK, the regulation of security is somewhat indirect, but the expectations are that operators will take a reasonable posture with repect to an assessment of risk. In contrast, the regulatory system in the USA, operated for the Federal Energy Regulatory Commission (FERC) via the NERC CIP framework, is thought of as a more substantially rules-based system, particularly since the move to version 4 of CIP-002 [1].

There does not seem to be a very clear-cut distinction between the mechanisms for reward and punishment across the two types of regimes. Both potentially rely upon rate-setting agreements, risk to continuation or further contracts, punishments for negligence (either in process or in outcome), but the specifics may vary from country-to-country. Perhaps the only universal difference is that in the rules-based system direct punishments for non-compliance with the particular rules are at least theoretically possible, where this is not possible in a purely risk-based regime.

The economics are complicated by the fragmentation of the responsibilites for setting general policy, for setting particular regulations, for setting rules, for monitoring compliance with rules, for administering punishments and rewards, for rate-stting, not to mention the privatization of some of these functions and the differing legal and governmental systems underpinning them. Additional muddiness comes from the presence of multiple transmission operators in some grids, interconnectors, shared and externalised risk (for example, blackstart issues). Still further complexity comes from the fact that the transmission operators are subject to general IT security reqirements (e.g. compliance with standards like the ISO27000 series [36] or COBIT framework [37]) and also operate in other critical sectors (for example gas transmission) so that regulation from one sector may have an effect or impose costs upon another, or worse, regulations from two sectors may conflict. A significant source of complexity in comparing different regulatory regimes is that they operate under different legal frameworks. In some environments, there may be additional corporate liabilities for transmission operators that lead to transfers (such as damages) to parties other than the policy-maker; in others, the operator may be indemnified, in effect. This document will nevertheless not further engage with these very real issues.

There are various indirect mechanisms available to policy-makers in their attempts to influence the security behaviour of transmission operators. For example, the policy-maker may choose to do this indirectly through the employees of the operators. Individual employees may have civil or criminal liabilities associated with their conduct. They may belong to professional institutions that require standards of conduct. In some situations, individual reputations within a small community of senior security professionals may play a role. These possible mechanisms and effects will not be treated in this document.

The risk-based regime can be viewed as a decentralization of the function of the search for risk. A primary argument in favour of this is that it allows the firm to better and more quickly respond to a rapidly-changing threat environment, and to mitigate newly-understood or newly-introduced vulnerabilities. We refer to this as *agility*. A recent report [3] from the White House suggests that some policy-makers are increasingly receptive to such arguments.

Further support for risk-based approaches to critical infrastructure cybersecurity appears in a recent executive order by the US president [2]. Arguments in favour of a risk-based system point to agility, to appropriateness and effectiveness of controls in mitigating true risk rather than merely demonstrating compliance for the sake of it, for minimizing costs of inappropriate rules being applied unnecessarily. This view is by no means unopposed. Proponents of rules-based regimes point to the assurance that they provide that basic controls are in place, and that they provide specifications that help transmission operators to put in place security controls. Some critics of risk-based methodology further claim that it cannot apply effectively to cybersecurity [4]. Many of these criticisms are, essentially, known issues in risk managment and economic incentivization in other domains, and not specific to the rules-versus-risk question. However, it is noteworthy that the agility (or "maneuver speed") argument has been criticized directly [4], based on the difficulty of overcoming hard constraints from the environment (for example, operating constraints on the infrastructure that inhibit the frequency of security patching). It may be that quite specific properties of the critical infrastructure system and its threat environment constrain what forms of policy regime can be effective. For example, a certain type of power generating plant in a rapidly evolving threat environment may need to be treated differently to a transmission grid in a more slowly evolving environment.

The remainder of this document proposes a class of models for investigating agility versus (basic) assurance trade-offs arising from rules- and risk-based policies in regulated critical infrastructure. A key question is what the balance (if any) should be between the two approaches in various operating environments.

ANNEX3.3 The General Class of Models under Consideration

ANNEX3.3.1 Agility versus Basic Compliance Assurance in Single Transmission Operator Systems

IWe consider the situation of a single, simplified transmission operator — for the remainder of this section referred to as *the firm*. We consider it in the context of different regulatory regimes, and consider the trade-offs implicit in the the choice of regime by the policy-maker. The policy-maker will itself be treated as a single, coherent entity rather than a nexus of interacting institutions.

The regimes themselves will in general be mixtures of rules- and risk-based regimes, with the pure rules and pure risk variants as extreme choices. The principal decision for the firm will be on the effort spent in complying with definite rules (whether-or-not they mitigate real security risk), and with effort spent in (finding and) mitigating security risks. The firm trades off outcomes in terms of rewards (punishments) for compliance (non-compliance) with rules, and risk from transmission disruptions arising from unmitigated vulnerabilities. We refer to the assurance that the firm derives from complying with rules as *basic (compliance) assurance*. This form of assurance may be quite different from security assurance in a more holistic, risk-sensitive sense. We thus explore the trade-offs between basic assurance and agility.

The exploration is done in the context of a toy-model. This will make numerous simplifications and abstractions. In the first instance we seek a model of the general economic effects, and do not attempt to calibrate this against real world data.

ANNEX3.3.2 Loss Functions and Influences Upon Decision-making

In the various models that we will consider, decision-making will be idealized in terms of optimization problems for an objective function. In the present situation, we will consider the separate, yet interdependent, attempts of minimization of loss functions by the both the firm and the policy-maker. This suggets that game-theoretic methods will be required for the analysis. This will require additional detail as to how the interaction of choices takes place. Before delving into such detail, which will surely vary from scenario-to-scenario, we take as a preliminary step the consideration of the other factors that affect the calculation of loss. This requires idealization and simplification, as does the space of choices available to the parties.

Let us say that the policy-maker can choose just the following things: a level of investment over time, s_P; a (possibly structured, possibly empty) rule set, R; a policy for applying rewards based on compliance and transmission outcomes — for simplicity, we restrict this to a single reward weighting parameter, w. For simplicity, we assume that tme ranges over some fixed time period, and that the rule-set and weighting w are fixed at the beginning of that period.

The firm can choose: a level of investment at any time, s_F; a choice of security controls applied over time, cont.

In addition, there will be certain vulnerabilities that arise over time which may require mitigation. We thus assume that there are some Vuln of vulnerabilities at time t. Note that all of the above parameters may, in the general case, be variable paths over time.

Figure 10 is a kind of block diagram. The inputs are constellations of parameters and control choices by the firm and the policy-maker. The outputs are losses for the firm and the policy-maker. Each block displays some transformation that maps inputs to an output. The security budget and controls are set in a dependent fashion. Rather than fix the functional forms for the transforms and procede to specify how the interaction of decision-making takes place, we note that the problem is still rather complex, partly because of the number of parameters to be decided by each agent. We therefore move on to look at a simplification which holds many of these parameters constant, whilst still allowing us to examine the agility/basic-assurance trade-off implict in the policy-makers risk-versus-rules decision.

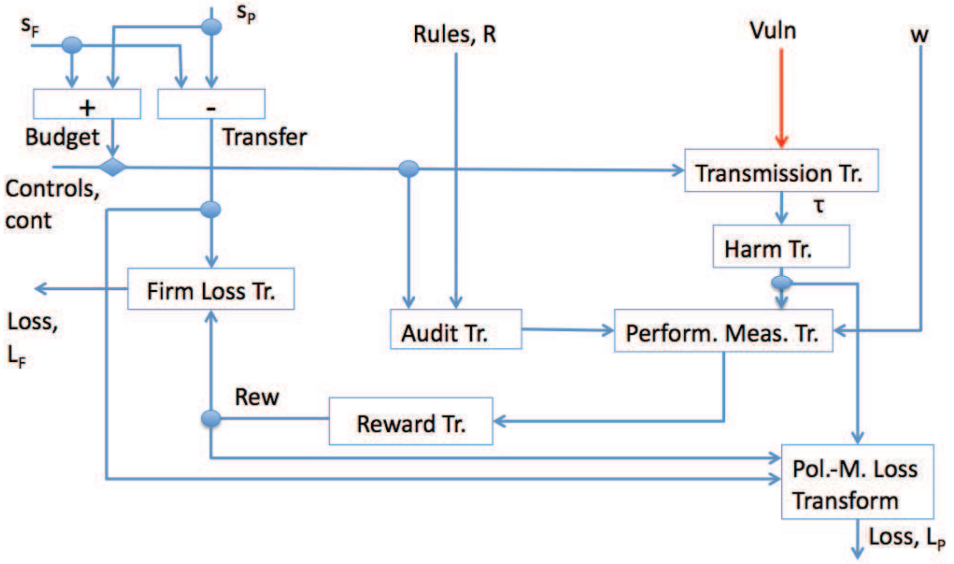


Figure 10: Policy-maker Loss Calculations: Before Stackelberg Equilibriation

ANNEX3.4 A Simplified Trade-Off Analysis in a Deterministic Model

ANNEX3.4.1 Basic Description of the Subsequent Models

In order to simplify matters, we abstract away the details of time. All of the paths taken by parameters thus collapse into single values. Our analysis says nothing separate about the rapidity aspect of agility; this is absorbed into its effectiveness. However, one aspect of time will remain, in that the interaction of the choices and the arrival of the vulnerabilities will happen in a certain order.

The interaction is structured in a single-shot game representing a single period of operation under a fixed regulatory regime (with a fixed, possibly empty, set of rules). More 'realistic' extensions of this to multiple periods and with internal temporal structure are easily imaginable, but the analysis may be less clear. Moreover, seeking further simplification, we hold the levels of spend s_P and s_F constant.

The game is now specified essentially as a Stackelberg extensive-form game (except with an intermediate move by nature). The policy maker chooses a value $w \in [0, 1]$, representing the emphasis on risk or on rules; the policy-maker also supplies a set of rules R, but for the reasons explained below this does not need to be treated as a decision-variable. A set of vulnerabilities $V_{\text{real.}}$ is chosen to be realized; the degree to which the vulnerabilities $V_{\text{real.}}$ is covered by the rules in R is determined (probabilistically) by the predictability of the process that generates it; this predictablity will be governed by an additional parameter, α, that can be used to eliminate R as a decision variable. The firm has a fixed, finite level of resource/effort available, and can choose the division of its efforts between compliance and risk mitigation; the firm chooses a set controls cont; this will be represented by a non-negative integer x chosen within certain bounds.

The use of an intermediate move by nature is a device to capture the supposed distinction between the use of a rule-set fixed at the beginning of the time period, and the potential to learn about new vulnerabilities in a risk-based regime. There is a kind of agility advantage (at the level of knowledge) for the risk-based approach thus baked-in to this model, but note that this may not translate into an overall advantage at the level of the final loss function for the firm which encodes its final preferences — the trade-off is more complex.

ANNEX3.4.2 Further Simplification to a Minimal, Purely Numerical Model

Rather than handle this as a stochastic model, we simplify below so that α simply fixes the number of realized vulnerabilities that are mitigated by controls that correpond to regulations.

Now let us make a number of further simplifying assumptions. Suppose that the set of possible vulnerabilities is V. Suppose that each regulation r mitigates precisely one vulnerability $\text{mitr}(r)$. This gives the set $V_{\text{reg.}} = \bigcup\{\text{mitr}(r) \mid r \in R\}$ of vulnerabilities that *could* be mitigated by complying with rules. For simplicity, we simply now identify $R = V_{\text{reg.}}$. Each control $c \in \text{cont}$ that the firm adopts mitigates precisely one vulnerability $\text{mitc}(c)$. This gives a set $V_{\text{cont.}} = \bigcup\{\text{mitc}(c) \mid c \in \text{cont}\}$ of vulnerabilities that *are* mitigated by the chosen controls. Again, we simply identify $\text{cont} = V_{\text{cont.}}$. The subsets $V_{\text{real.}}$, $V_{\text{cont.}}$, $V_{\text{reg.}}$ of V are depicted schematically in Venn diagram of Figure 11. More general models would replace these simple sets with more sophisticated probability distributions.

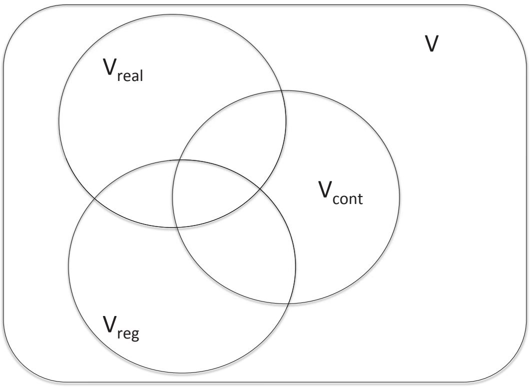


Figure 11: Vulnerability Mitigation under Simplifying Assumptions

The loss of the firm is (for simplicity assumed to be) of the form

$$\begin{aligned} L_F &= \mathrm{FirmLossTransform}(\mathrm{Transfer}, \mathrm{Reward}) \\ &= -\mathrm{Transfer} - \mathrm{Reward} \\ &= -(s_P - s_F) - \mathrm{Reward}. \end{aligned}$$

The reward will depend upon α, an ‘unpredictability’ parameter that simplifies the arrival of vulnerabilities. Since the spends are constant, we have eliminated stochastic effects, and we are only interested in the order of losses, we can re-write the reward more simply as $L_F = -\mathrm{Reward}$, where the reward will depend upon α, cont, w.

The Reward is assumed to take the form:

$$\begin{aligned} \mathrm{Reward} &= \mathrm{RewardTransform}(\mathrm{PerformanceScore}) \\ &= \mathrm{PerformanceScore} \\ &= \mathrm{PerformanceTransform}(\mathrm{AuditScore}, \mathrm{HarmScore}) \\ &= -(w \times \mathrm{AuditScore} + (1 - w) \times \mathrm{HarmScore}). \end{aligned}$$

For the firm, a higher AuditScore gives worse performance (as designated by the policy-maker), but so does a higher HarmScore. Worse performance results in a reduction of reward. This results in a higher loss. The parameter w determines a convex combination of preferences over these components.

We assume that AuditScore is a function only of the number of regulations with which the firm complies (through the choice of some control). We assume that the HarmScore is a function only of the number of realized risks that are not mitigated (through the choice of some control, but also subject to the environmental parameter α).

The firm will want to ensure that all of its controls only address vulnerabilities in $R \cup V_{\mathrm{real.}}$, since these are the only ones that have the capacity to incur additional loss. Now it seems realistic (for otherwise there is a combined over-resourcing by firm and policy-maker combined), and is required for an interesting allocation problem, to assume that it does not have sufficient resource for contols to cover all of $R \cup V_{\mathrm{real.}}$. That is, we have $V_{\mathrm{cont.}} \subsetneq R \cup V_{\mathrm{real.}}$.

Note that precisely those vulnerabilities that correspond to both a regulation and a realized vulnerability are those that can contibute both to increase both AuditScore and HarmScore. All unmitigated vulnerabilities are assumed to make the same contribution to HarmScore and all regulations not complied with make the same contribution to AuditScore. Thus the firm should choose to use its budget for controls to first cover as much as it can of $R \cap V_{\text{real.}}$. For simplicity, we assume that it can cover all of this set (not to do so would seem to be irrelevant to the current trade-off analysis and more to do with broader incentives for security, since it would somehow be about under-resourcing in total). The firm should also have some controls left over (again in order to give an interesting allocation problem). We thus have: $R \cap V_{\text{real.}} \subsetneq V_{\text{cont.}} \subsetneq R \cup V_{\text{real.}}$. The choice of the firm choice is then really to divide its remaining controls between $R \smallsetminus V_{\text{real.}}$ and $V_{\text{real.}} \smallsetminus R$.

The intersection of the set $R \cap V_{\text{real.}}$ depends upon the predictability of the environment. Let $\alpha = \#(R \cap V_{\text{real.}} \cap \text{cont})$ be the number of controls that both cover a rule and mitigate a realized vulnerability. The set-theoretic structure can now be seen to matter little. Let $n = n(\alpha) = \#(\text{cont} \smallsetminus (R \cap V_{\text{real.}}))$. That is, the number of controls left to allocate is n, when the predictability of the environment is given by α (and the budget is fixed). Let $N = \#(\text{cont})$, the total number of controls available. Then $N = \alpha + n$.

The firm chooses non-negative integer x of its controls from $R \setminus V_{\text{real.}}$, and so $n - x$ from $V_{\text{real.}} \setminus R$. The circle in Figure 12 depicts the division of cont. Note that we have constraints

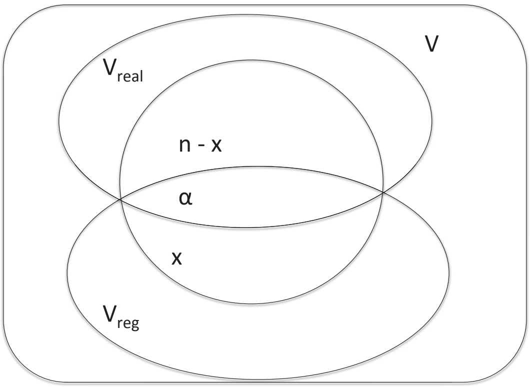


Figure 12: Allocation of the $N = n + \alpha$ Controls

$0 \leq x \leq N$, and $x \leq \#(R) - \alpha$ and $0 \leq n - x \leq \#(V_{\text{real.}}) - \alpha$, and that these can be rewritten as

$$x_{\text{min}} = \max(0, N - \#(V_{\text{real.}})) \leq x \leq \min(\#(R) - \alpha, n) = x_{\text{max}}. \tag{60}$$

We must now start to fix the functional forms of the audit, harm and transmission transforms more precisely. Suppose that AuditScore is just given by the fraction (between 0 and 1) of the rules for which there is a control allocated:

$$\begin{aligned} \text{AuditScore} &= \text{AuditTransform}(\text{cont}, R) \\ &= \#(R \cap \text{cont})/\#(R) \\ &= (\alpha + x)/\#(R). \end{aligned}$$

Note that this increases as x increases. Note that we are able to re-write the transform as a function of α (the 'predicability' of the environment, implicitly part of Vuln in our earlier description) because of the simplifying assumptions that we have made (replacing vulnerabilities with α).

In order to give the harm, we first have to postulate a form to capture the way that the transmission 'level' drops when vulnerabilities are left unmitigated. Let us again postulate a linear form:

$$\begin{aligned}\tau &= \text{TransmissionTransform}(\text{cont}, V_{\text{real.}}) \\ &= \#(V_{\text{real.}} \cap \text{cont})/\#(V_{\text{real.}}) \\ &= (N - x)/\#(V_{\text{real.}})\end{aligned}$$

The transmission level, τ, takes values between 0 and 1, and is (monotonically) decreasing in x. Note that this is a rather simplistic choice; it will not be appropriate if we wish to invsetigate models for variation in the number of arriving vulnerabilities $V_{\text{real.}}$. We defer building a better form into a model for later.

Suppose that the harm is given as follows:

$$\text{HarmScore} = \text{HarmTransform}(\tau) = \frac{1}{2}(1 - (2\tau - 1)^{1/3}).$$

A graph of the harm is sketched in Figure 13. Note that we have simply chosen to compress

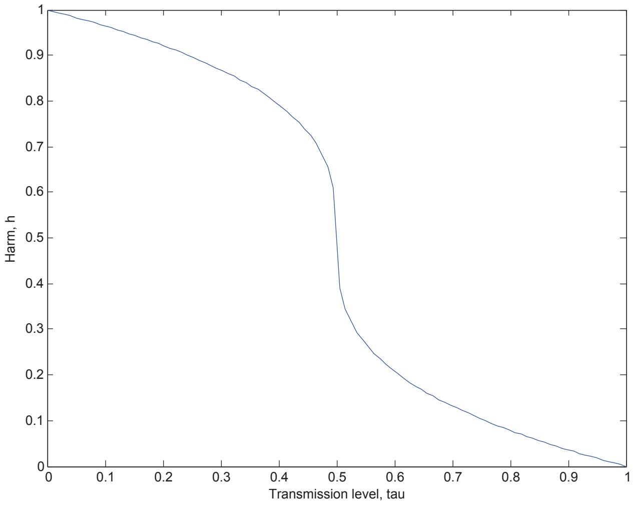


Figure 13: Decrease in Harm with Increase in Transmission Level

all the nonlinearity into HarmTransform (rather than spreading it also through the transmission transform.) This is a device for convenience in this toy model. The harm will be a value between 0 and 1, and decreases with τ, and so as x increases. The 'cliff' here represents the criticality of the infrastructure at an abstract level. The use of a cube root is purely for example. Doubtless, other functional forms — perhaps those with multiple cliffs, even discontinuous ones — would be of interest.

We have simplified the problem for the firm to one where losses depend only upon a set of numbers: the number of controls available to implement, N, as fixed at the fixed level of spend; the control choice of the firm, x; the control choice by the policy-maker, w;

the number of rules set by the policy-maker; this will simply be written R now (rather than $\#(R)$); the number of vulnerabilities that arrive; this will simply be written $V_{\text{real.}}$ (rather than $\#(V_{\text{real.}})$; the predictability, α, of the vulnerabilities that arrive. Note that $V_{\text{real.}}$ and α are the realizations in this model of Vuln as it appeared in Figure 10. In the treatment below, we shall treat the number of rules R as a parameter of the environment, rather than as a control choice. This is a feature of this highly-idealized model. If we were to investigate R as a control choice, then we would have to take into account the fact that the number of controls #(cont) would be expected to increase at the same time (in some way).

A further significant weakness of the present model is the fact that the firm has perfect knowledge of the number of vulnerabilities $V_{\text{real.}}$ and the overlap α at the time it makes its decision. A more realistic model would at least only give the firm partial knowledge of these, perhaps according to some distribution. However, it is then only a short step to asking for the set-theoretic structure of vulnerabilities to be re-introduced and for probability distributions over those to describe the firm's knowledge. Again, there are many possible extensions of the present work.

The firm will seek to choose x to maximize the resulting loss, subject to the parameters α, N, R, $V_{\text{real.}}$, and w. To be precise, the resulting loss function is:

$$\begin{aligned} L_F(\alpha, N, R, V_{\text{real.}}, w, x) &= w(\tfrac{\alpha+x}{R}) + (1-w)[1-\tfrac{1}{2}(1-(2\tau-1)^{1/3})] \\ &= w(\tfrac{\alpha+x}{R}) + (1-w)[1-\tfrac{1}{2}(1-(2\tfrac{N-x}{V_{\text{real.}}}-1)^{1/3})]. \end{aligned}$$

Let us fix a simple loss transform for the policy-maker. Suppose that it is simply given by the harm:

$$L_P = \text{PolLossTransform}(\text{HarmScore}, \text{Reward}, \text{Transfer}) = \text{HarmScore}.$$

The policy-maker's loss can also be re-written a function with respect to the parameters α, N, R, $V_{\text{real.}}$, and w:

$$L_P(\alpha, N, R, V_{\text{real.}}, w, x) = 1 - \frac{1}{2}(1-(2\frac{N-x}{V_{\text{real.}}}-1)^{1/3}).$$

The policy-maker will choose w to minimize L_P. However, this will depend upon the firm's reaction (choice of x).

ANNEX3.4.3 Investigation of the Purely Numerical Model

We can investigate the effects on the firm's behaviour as the policy-maker's trade-off parameter is chosen differently.

Matlab [38] code for plotting the loss functions against values of the firm's instrument x, and finding the optimal reaction, can be found in appendix ANNEX3.7. A screenshot of a calculator implemented in Simulink [39] for computing the loss functions is given in Figure 14.

It is instructive to start the discussion of this by looking at Figure 15, which depicts resulting losses for the firm (in a particular case $\alpha = 200$, $N = 400$ (numControls), $R = 600$, $V_{\text{real.}} = 600$, $w = 0.5$). In this figure the x-axis shows the possible values of choice of control x, bounded by the minimum and maximum possible values; the dark blue line is the audit

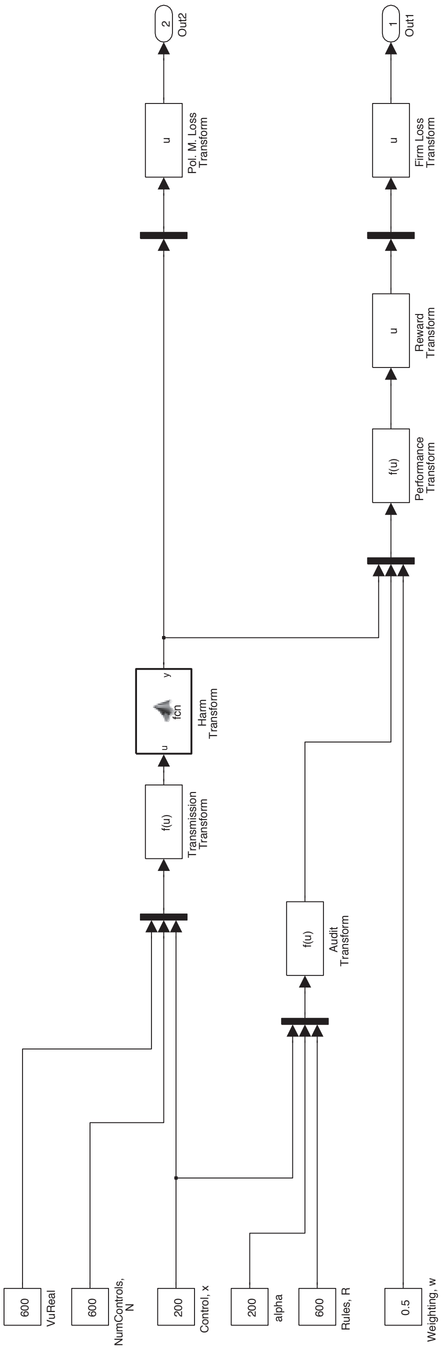


Figure 14: Loss Calculator (without Spend)

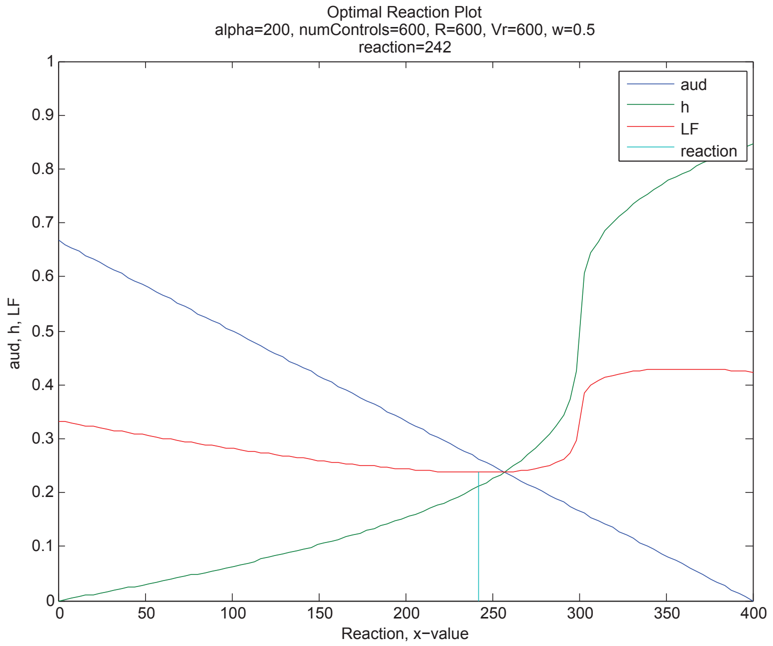


Figure 15: A Plot of AuditScore, Harm, and Loss Against the Firm's Control Instrument, x

score, the green line is the harm score; the red line is the loss for the firm; the vertical line is cyan intersects the x-axis at the firm's optimal reaction.

In this case, the firm's reaction to the choice of w would appear to be acceptable, in the sense that it produces a control that is significantly to the left of 'cliff' in the harm. Note that the loss of the firm is the convex combination of the harm and audit scores, so the policy-maker can optimize its choice of w by taking $w = 0$ (pure risk). This is not a deep point — it is obvious by construction. A pure rules regime ($w = 1$) leads to a situation in which the firm's reaction leads to the worst possible outcome for the policy-maker. There is a bias in this first model towards the risk-based approach: whatever the environmental parameters, the policy-maker can always attain the best possible result by taking $w = 0$. This will be remedied in the model of Section ANNEX3.5 and similarly in subsequent models.

A more subtle point is that there are poor choices of w in combination with the parameters, and that there are some very rapid changes in outcome for small changes in w. For example, only varying the parameter w from 0.73 to 0.74 in the foregoing example, produces a change in the firm's optimal reaction from $x = 87$ to $x = 200$ as shown in Figure 16.

The particular forms shown give us a loss function L_F with at most two critical points (in the sense of calculus) at

$$x = N - \frac{V_{\text{real.}}}{2}\left(1 \pm \left(\frac{R(1-w)}{3wV_{\text{real.}}}\right)^{3/2}\right)$$

but, these may not necessarily occur within the range of meaningful x-values. These values are defined if and only if $w \neq 0, 1$. The smaller of the two will be a minimum and the larger a maximum. If it exists, the mimimum always occurs for the positive value of $\left(R(1-w)/(3wV_{\text{real.}})\right)^{1/2}$. Let us call the location of this minimum (if it exists) x_{lmin}, and the

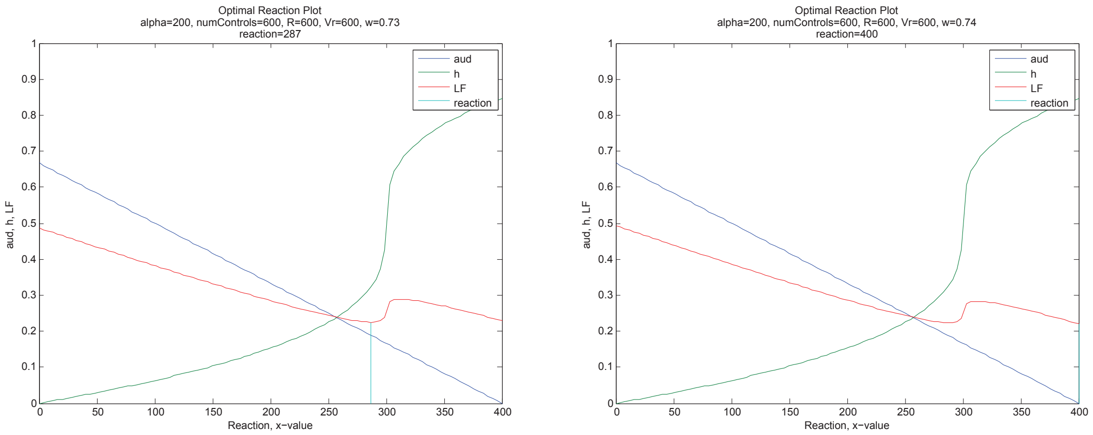


Figure 16: Jump in Firm's Reaction, x, with Small Variation in Policy-Maker's Choice, w

	Circumstance	x_*	L_P Optimal
1	$w = 0$	$x_{\min}$	yes
2	$w = 1$	$x_{\max}$	no
3	$x_{\text{lmax}} \leq x_{\min}$	$x_{\min}$	yes
4	$x_{\max} \leq x_{\text{lmin}}$	$x_{\max}$	no
5	$x_{\min} = x_{\text{lmin}} < x_{\text{lmax}} < x_{\max}$ & $L_F(x_{\text{lmin}}) < L_F(x_{\max})$	x_{lmin}	yes
6	$x_{\min} < x_{\text{lmin}} < x_{\text{lmax}} < x_{\max}$ & $L_F(x_{\text{lmin}}) < L_F(x_{\max})$	x_{lmin}	no
7	$x_{\min} \leq x_{\text{lmin}} < x_{\text{lmax}} < x_{\max}$ & $L_F(x_{\text{lmin}}) = L_F(x_{\max})$	$x_{\text{lmin}}, x_{\max}$	yes, no
8	$x_{\min} \leq x_{\text{lmin}} < x_{\text{lmax}} < x_{\max}$ & $L_F(x_{\text{lmin}}) > L_F(x_{\max})$	$x_{\max}$	no
9	$x_{\text{lmin}} \leq x_{\min} \leq x_{\text{lmax}} \leq x_{\max}$ & $L_F(x_{\min}) < L_F(x_{\max})$	$x_{\min}$	yes
10	$x_{\text{lmin}} < x_{\min} \leq x_{\text{lmax}} \leq x_{\max}$ & $L_F(x_{\min}) = L_F(x_{\max})$	$x_{\text{lmin}}, x_{\max}$	yes, no
11	$x_{\text{lmin}} < x_{\min} \leq x_{\text{lmax}} \leq x_{\max}$ & $L_F(x_{\min}) > L_F(x_{\max})$	$x_{\max}$	no
12	$x_{\min} < x_{\text{lmin}} \leq x_{\max} < x_{\text{lmax}}$	x_{lmin}	no
13	$x_{\min} = x_{\text{lmin}} \leq x_{\max} < x_{\text{lmax}}$	x_{lmin}	yes

Table 3: Reactions of the Firm in Various Circumstances

location of the maximum x_{lmax}. The minimum of L_F that should be selected by the firm will always be either at the extremal x-values $x_{\min}$ and $x_{\max}$ described by the constraints in (60), or possibly at x_{lmin} where it exists and satisfies those constraints. In fact, because we have chosen L_P to be given just by the harm, the minimum cannot occur at $x_{\max}$.

Let the reaction by the firm be x_*. We see that the possible circumstances and outcomes as outlined in Table 3; in all but the first twos line $w \neq 0, 1$, and we let $L_F(x)$ be shorthand for $L_F(\alpha, N, R, V_{\text{real.}}, w, x)$. We can find choices of w that are optimal for the policy-maker in various circumstances. By way of example, we do this in a couple of simple cases. Firstly, we can see that in this case that $w = 1$ will not be optimal (in fact, it will lead to the worst reaction). Now consider row 3 of the table in a situation where $N < V/2$. In the case $x_* = x_{\min} = 0$ and this is achieved by taking w with

$$0 \leq w \leq \frac{R}{R + 3V(1 - \frac{2N}{V})^{2/3}}.$$

Thus policy-maker optimality can be achieved in this case, by placing sufficient emphasis on risk-based performance by the firm.

ANNEX3.5 A Second Model: Extending to Account for Spend by the Firm

In this section, we refine and extend the purely numerical model of the previous section to give an account of a situation in which the firm's defensive capabilities are potentially enhanced as it spends more on security. It is also a situation where the loss function of the firm is more complex.

The firm now chooses a level of expenditure (spend) s_F up to some maximum s_F^{max}, whilst each control has a uniform cost c. Since the reward used so far has been arbitrarily scaled to the unit interval, an additional parameters w_{Pun} is now used to scale it back to units that make it comparable to the spend, s_F. Similarly, a parameter w_{Pol} is used to scale the harm to units comparable to those accruing to the transfer. The spend by the policy-maker is again assumed to be a fixed parameter s_P. The loss functions thus take the forms

$$L_F(\alpha, c, R, s_F, s_P, V_{\text{real.}}, w, w_{\text{Pun}}, w_{\text{Pol}})$$
$$L_P(\alpha, c, R, s_F, s_P, V_{\text{real.}}, w, w_{\text{Pun}}, w_{\text{Pol}}).$$

The forms of the two functions are constructed by modification of the transforms considered previously. Specifically, we take

$$\begin{aligned}
\text{Budget} &= s_P + s_F \\
\text{Transfer} &= s_P - s_F \\
N &= \lfloor \text{Budget}/c \rfloor \\
\text{AuditTransform}(\alpha, N, R, x) &= 1 - \min(1, (\alpha + x)/R) \text{ if } \alpha \leq N \\
\text{AuditTransform}(\alpha, N, R, x) &= 1 - \min(1, N/R) \text{ if } \alpha > N \\
\text{RewardTransform}(\text{PerformanceScore}, w_{\text{Pun}}) &= -w_{\text{Pun}} \times \text{PerformanceScore} \\
\text{FirmLossTransform}(\text{Transfer}, \text{Reward}) &= -\text{Transfer} - \text{Reward} \\
\text{PolLossTransform}(\text{Transfer}, \text{Harm}) &= w_{\text{Pol}} \times \text{Harm} + \text{Transfer},
\end{aligned}$$

and leave all other transforms as in Subsection ANNEX3.4.2. Note that N is just the number of controls available to the firm, as before, but is now defined using the mathematical floor operation and the available budget.

A screenshot of a Simulink [39] calculator for these quantities is given in Figure 17. Matlab [38] code, for plotting the loss functions against x and s_F is contained in Appendix ANNEX3.8.

ANNEX3.5.1 Initial Exploration

Figure 18 shows plots (left) and contour plots (right) of harm, firm loss and policy-maker loss against the parameter x, and the investment by the firm s_F. In the code that generates this, and subsequent, figures in this section: alpha = α, controlCost = c, spendP = s_P Vr = $V_{\text{real.}}$, wPerf = w, and spendFmax = s_F^{max}. Each of the contour plots contains a hard black line: points below and to the right of these lines are infeasible because they are not affordable at

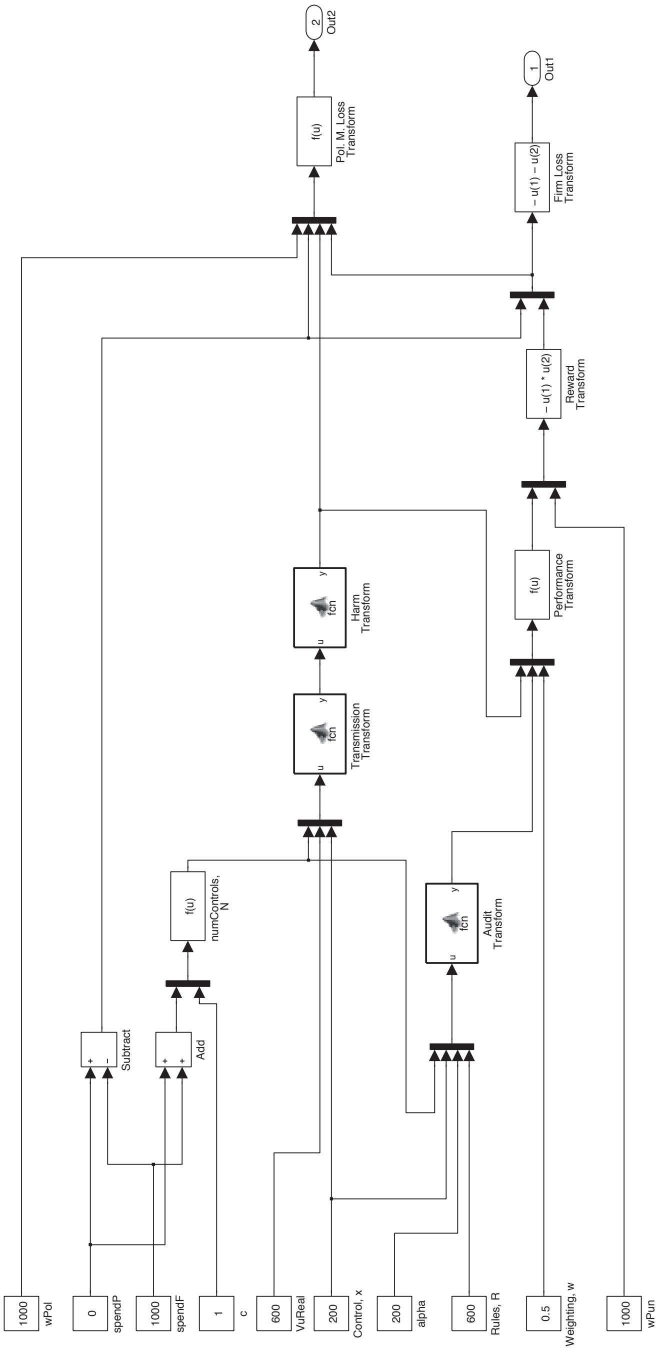
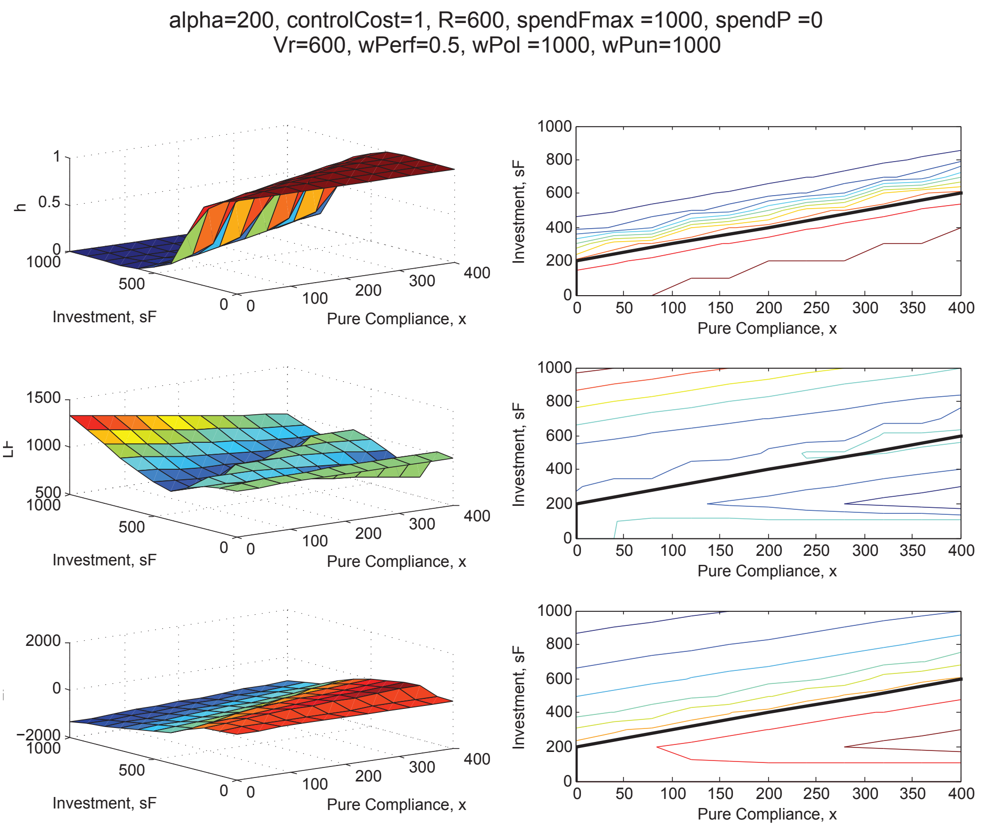


Figure 17: Loss Calculator (with Spend)



alpha=200, controlCost=1, R=600, spendFmax =1000, spendP =0
Vr=600, wPerf=0.5, wPol =1000, wPun=1000

Figure 18: Plots of Harm and Loss against Firm Investment and Control

the chosen budget. The top two plots show that for this configuration of parameters, on the feasible region the lowest level of harm occurs where there is most spend, s_F but least pure compliance, x. In the bottom pair of plots, the loss function for the policy-maker, L_P, show that the policy-maker's loss, in this case, are closely aligned with the harm. Let $x_*(w)$ be the reaction of the firm to the choice of w. In the middle-pair of plots, we see the firm's loss, and that the form of this is not completely trivial. In particular, the plot suggests (and it can be calculated to be the case that) the minimum of L_F (at $x_*(w)$) is at a low level of investment and a low level of pur compliance. However, $x_*(w)$ is not at a minimal level of investment on the feasible region. Note that such a reaction by the firm may appear for the policy-maker to be sub-optimal. However, final judgement on this depends upon consideration of the firm's reactions $x_*(w')$ to all other control choices w' by the policy-maker.

The calibration of the parameters will have a significant impact upon the forms of the losses to be minimized. For example, simply increasing the w_{Pol} and w_{Pun} factors (and thus increasing the impact of both performance (for the firm) and harm (for the policy-maker)) gives the results shown in Figure 19. Whilst the minima of harm and L_P remain at the top-left

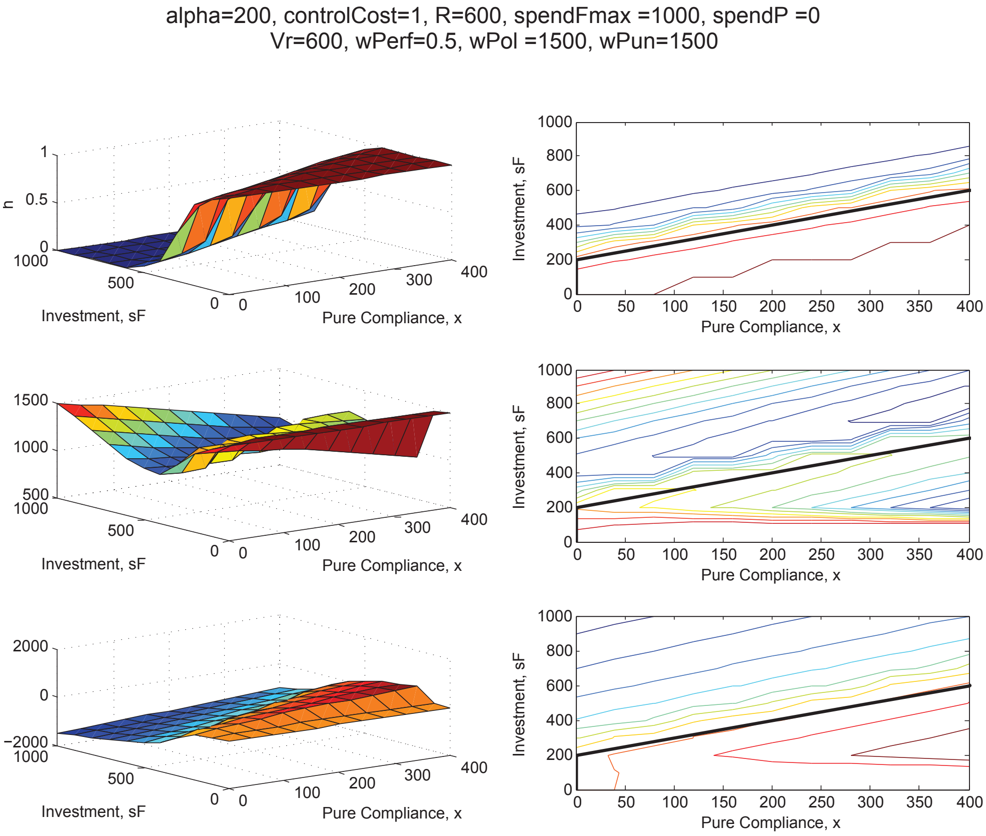


Figure 19: Recalibrating the Impact of Harm and Audit

(low x, high s_F), the minimum of L_F now occurs for high (although not maximum) s_F and large x. Thus the firm's reaction may once again appear to be undesirable from the point-of-view of the policy-maker, but in a quite different way than before.

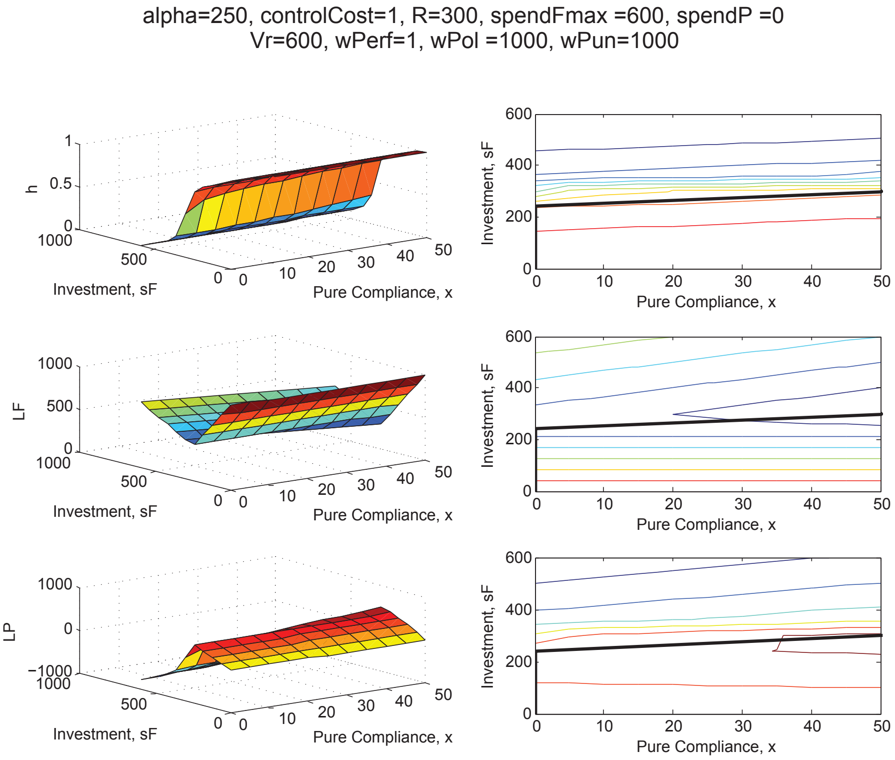


Figure 20: High predictability, low number of rules, all rules-based

Figure 20 shows a situation of high predictability but few rules. Note that the firm's reaction may once again occur well away from the policy-maker's minimum — indeed it is close to the worst possible reaction to the given w. However, if the policy-maker uses a larger number of rules and takes a purely risk-based approach ($w = 1$), then the firm makes a choice that leads to a low-level of loss for the policy-maker. Such a situation is depicted in Figure 21. Thus there are parameter constellations in which a rules-based approach appears viable —

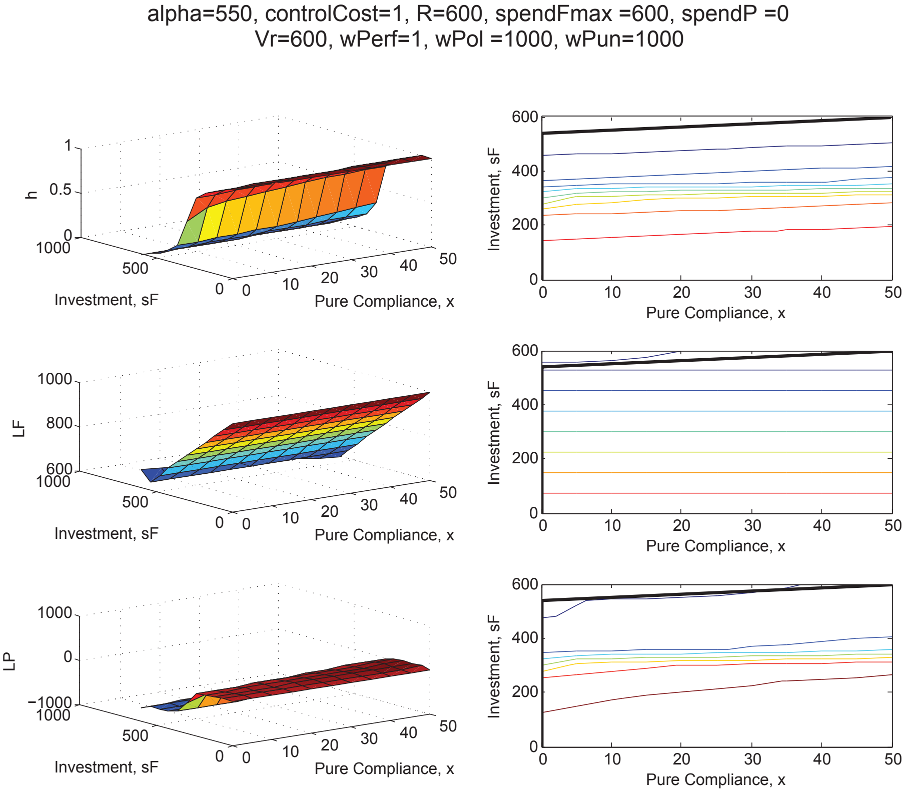


Figure 21: High predictability, high number of rules, all rules-based

although we do not claim at this stage that it is optimal. In Figure 22 we see a situation in which simply imposing a high number of rules rules-based policy is unsuccessful (because of low predictability): the firm's reaction results in a high loss for the policy-maker.

If the firm is not incentivized to treat harm with the same magnitude of seriousness as the policy-maker, then this can lead to poorly aligned loss functions. Figure 23 depicts such a situation. The firm will not pick a

For any fixed choice of parameters, the optimizations can be done by entirely standard exact (or numerical) methods. In the absence of specific knowledge of these parameters, we do not from pursue any of these optimizations at this point.

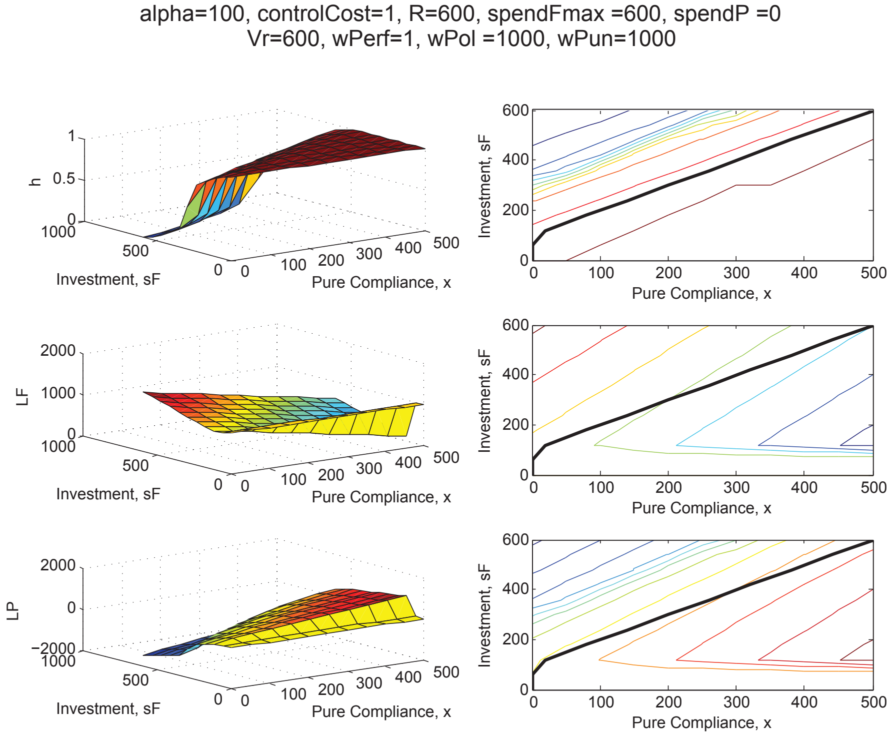


Figure 22: Low predictability, high number of rules, all rules-based

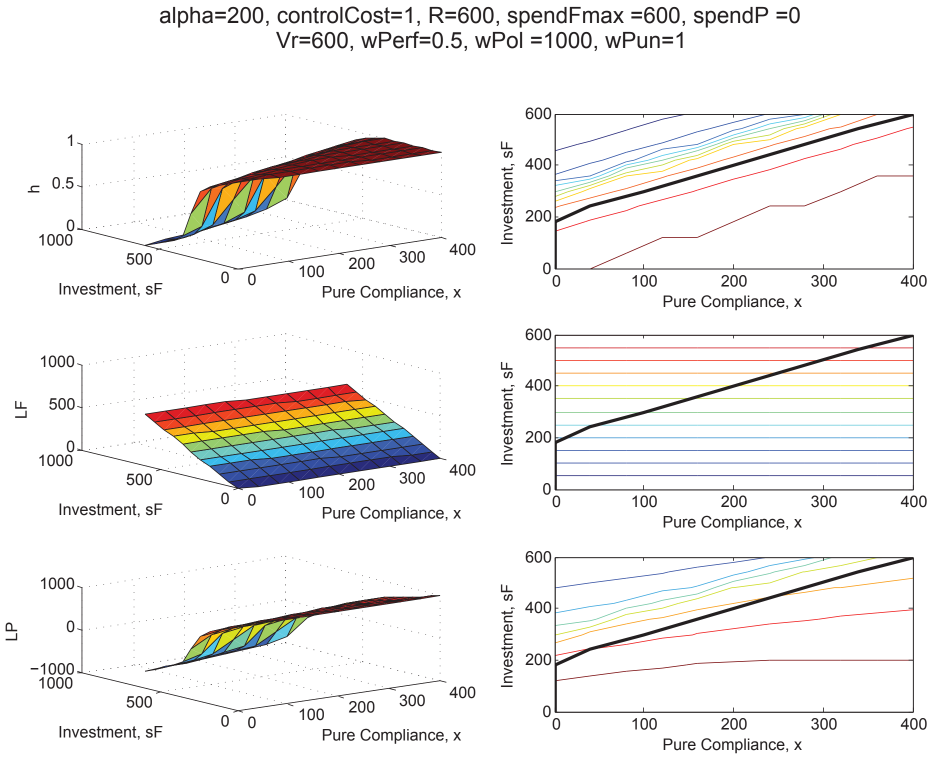


Figure 23: Insufficient Incentive to Firm for Security Relative to Policy-Maker

ANNEX3.5.2 Alternative Transmission and Harm Transforms

The Transmission Transform and Harm Transform presented above are likely far too simplistic. In this section, we present an alternative combination, by way of indicating how complex the decision problem can become when we start to include more complex, realistic transforms.

One natural form of transmission transform would seem to simply consist of a sequence of steps downward as the number of uncontrolled vulnerabilities increases. The resulting optimization for the firm can be non-trivial and potentially contain many local minima, each of which is a potential candidate for the firm's reaction in the circumstances it is given. An example of this can be seen in row 2, column 2 of Figure 24. In order to find its optimal reaction(s), the firm must explore each of the areas surrounded by a light-blue contour for a local minimum, and then compare each of these. In this example, the set-up is as in Section ANNEX3.5 except that $\tau = 1$ if $u \leq 20$, $\tau = 0.5$ if $20 < u \leq 300$, $\tau = 0$ if $u > 300$, where τ is the transmission level and u is the number of vulnerabilities that are not controlled (mitigated) at the given choice of x, and the harm $h = 1 - \tau$. Again, we do not carry the optimization any further since the results are contingent upon accurate calibration of the functional forms and relevant parameters.

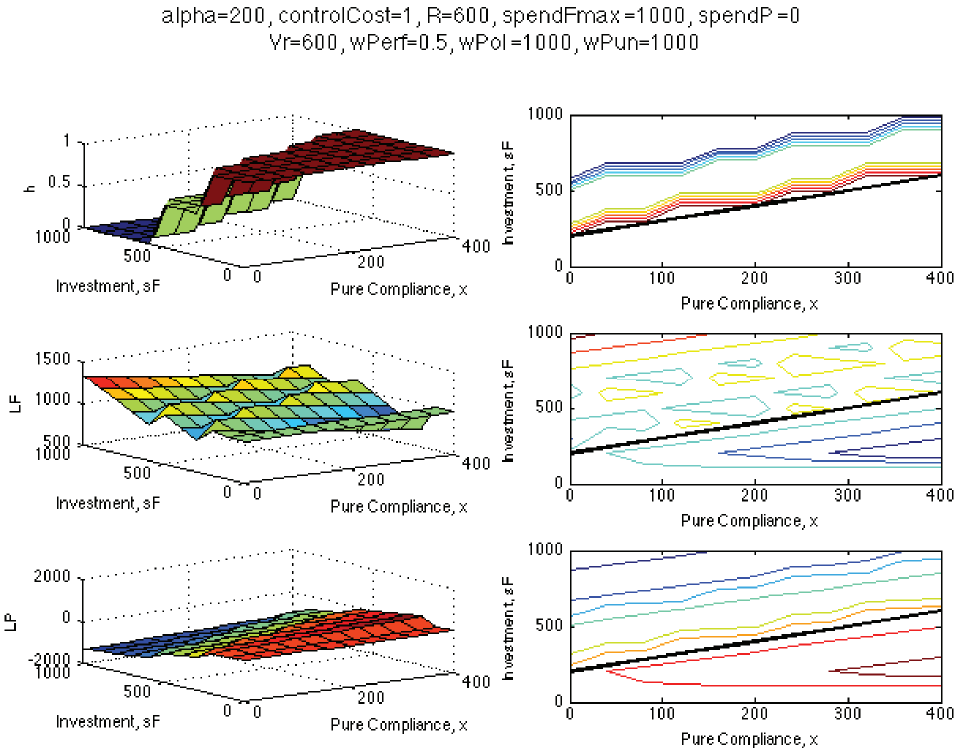


Figure 24: Complicated Firm Reaction Resulting from Harm with Two Steps

ANNEX3.6 Conclusions and Future Work

The present work has demonstrated the use of mathematical and computational models in analyzing the effects of different effects of combinations of incentives for risk-based and rules-based performance set by policy-makers for critical infrastructure. These models illustrate how the firm's reaction can be far from optimal (in more than one way) in response to choices made by the policy-maker. Whilst complete, exact analyses are certainly possible for the kinds of toy models given, this is subject to knowledge of the relevant parameters. Even with relatively simple choices of function (for example, for the Harm Transform) the reaction by the firm can be surprisingly complex, and the resulting optimization for the policy-maker dependent upon precise data.

Policy models in other domains (for example, macroeconomics) are often conerned with the behaviour of systems over time and use stochastic processes. Such models have also been applied to informations security policy problems [40, 41, 42, 43, 44, 45]. The toy models in this document are first steps toward such models that are both extended in time and have random parameters. Of particular interest will be models that examine the agility of the firm's response over time to different allocations of its effors over investments that vary in response to incentives set by the policy-maker, specifically to conform with risk-based responsibility or rules-based compliance.

ANNEX3.7 Appendix: Code for The First Model Without Spend

```
function agility1(alpha, numControls, R, Vr, w)
    plotSequence(alpha, numControls, R, Vr, w);
end

function aud = auditTransform(alpha, R,  x)
    aud = 1 - complianceScore(alpha, R, x);
end

function g = complianceScore(alpha, R, x)
    g = (alpha + x)/R;
end

function n = controlsLeft(alpha, numControls)
    n = numControls - alpha;
end

function [reaction, reactionResult] = firmReaction(alphaP,
   numControlsP, RP, VrP, wP, x_min, x_max)
     [reaction, reactionResult] = firmReactionExact(alphaP,
        numControlsP, RP, VrP, wP, x_min, x_max);
end

function [reaction, reactionResult] = firmReactionExact(alphaP,
   numControlsP, RP, VrP, wP, x_min, x_max)
```

```
    if not(wP==0)
        middlemin = numControlsP - VrP * (
           (RP*(1-wP)/(3*wP*VrP))^(3/2) +1 ) / 2;
        [reaction, reactionResult] = optimCases(alphaP, middlemin,
           numControlsP, RP, VrP, wP, x_min, x_max);
    else
        reaction = x_min;
        reactionResult = lossFunction(alphaP, numControlsP, RP,
           VrP, wP, x_min);
    end
end

function maxx = getmaxx(alpha, numControls, R, Vr, w)
    maxx = min([controlsLeft(alpha,numControls), R - alpha]);
end

function minx = getminx(alpha, numControls, R, Vr, w)
    minx = max([0, numControls - Vr]);
end

function harm = harmFunction(alpha, numControls, Vr, x)
    tau = transmissionTransform(alpha, numControls, Vr, x);
    harm = harmTransform(tau);
end

function harmScore = harmTransform(tau)
    harmScore = (1 - nthroot(2 * tau - 1, 3))/2;
end

function LF = lossFunction(alpha, numControls, R, Vr, w, x)
    auditScore = auditTransform(alpha,R,x);
    tau = transmissionTransform(alpha, numControls, Vr, x);
    harmScore = harmTransform(tau);
    performanceScore = performanceTransform(auditScore, harmScore,
      w);
    reward = rewardTransform(performanceScore);
    LF = lossTransform(reward);
end

function lossScore = lossTransform(reward)
    lossScore = - reward;
end

function [reaction, reactionResult] = optimCases(alphaP,
   middlemin, numControlsP, RP, VrP, wP, x_min, x_max)
    if (x_min < middlemin && middlemin < x_max)
       candMat = [x_min, x_max, floor(middlemin), ceil(middlemin)];
    else
        candMat = [x_min, x_max];
    end
    outMat = lossFunction(alphaP, numControlsP, RP, VrP, wP,
       candMat);
    [reactionResult, I] = min(outMat);
    reaction = candMat(I(1));
end

function performanceScore = performanceTransform(auditScore,
   harmScore, w)
    performanceScore = w * auditScore + (1 - w) * harmScore;
end

function plotSequence(alpha, numControls, R, Vr, w)
    figure;
    x_min = getminx(alpha, numControls, R, Vr, w);
    x_max = getmaxx(alpha, numControls, R, Vr, w);
    x = linspace(x_min, x_max);
    [reaction, reactionResult] = firmReaction(alpha, numControls,
       R, Vr, w, x_min, x_max);
    y0 = auditTransform(alpha, R, x);
    y1 = harmFunction(alpha, numControls, Vr, x);
    y2 = lossFunction(alpha, numControls, R, Vr, w, x);
    plot(x,y0,x,y1,x,y2,[reaction reaction],[0 reactionResult]);
    axis([x_min x_max 0 1]);
    title({'Optimal␣Reaction␣
       Plot';strcat('alpha=',num2str(alpha),',␣
       numControls=',num2str(numControls),',␣R=',num2str(R),',␣
       Vr=',num2str(Vr),',␣
       w=',num2str(w));strcat('reaction=',num2str(reaction))}); %
       Title for The Plot
    xlabel('Reaction,␣x-value');
    ylabel('aud,␣h,␣LF');
    legend('aud','h','LF','reaction');
end

function reward = rewardTransform(performanceScore)
    reward = - performanceScore;
end

function tau = transmissionTransform(alpha, numControls, Vr, x)
    tau = 1 - Uncontrolled(alpha, numControls, Vr, x) / Vr;
end

function uncont = Uncontrolled(alpha, numControls, Vr, x)
    uncont = Vr - (numControls - x);
```

```
end
```

ANNEX3.8 Appendix: Code for The Second Model With Spend

```
function agility2(alpha, controlCost, R, spendF_max, spendP, Vr,
    wPerf, wPol, wPun)
    spendF_min = 0;
    spendF_intervals = 10;
    spendF_step = (spendF_max - spendF_min) / spendF_intervals;
    y_max = spendF_max;
    y_min = spendF_min;
    y_step = spendF_step;
    plotSequence(alpha, controlCost, R, spendP, Vr, wPerf, wPol,
        wPun, y_min, y_step, y_max);
end

function basicCover = alphaCovered(alpha, numCont)
    basicCover = (numCont >= alpha);
end

function auditScore = auditTransform(alpha, numControls, R, x)
    auditScore = 1 - complianceTransform(alpha, numControls, R, x);
end

function budget = budgetTransform(spendF, spendP)
    budget = spendP + spendF;
end

function complianceScore = complianceTransform(alpha, numControls,
    R, x)
    if alphaCovered(alpha, numControls)
        complianceScore = (alpha + x)/R;
    else
        complianceScore = numControls/R;
    end;
    complianceScore = min([1, complianceScore]);
end

function cont = controlled(alpha, numControls, Vr, x)
    cont = max([0, numControls - x]);
    cont = min([cont, Vr]);
end

function numControls = controlsAtSpend(budget, controlCost)
    numControls = floor(budget / controlCost);
end
```

```
function n = controlsLeft(alpha, numCont)
    n = max([0, numCont - alpha]);
end

function LF = firmLossFunction(alpha, controlCost, R, spendF,
   spendP, Vr, wPerf, wPol, wPun, x)
    transfer = transferTransform(spendF, spendP);
    budget = budgetTransform(spendF, spendP);
    numControls = controlsAtSpend(budget, controlCost);
    auditScore = auditTransform(alpha, numControls,  R, x);
    tau = transmissionTransform(alpha, numControls, Vr, x);
    harmScore = harmTransform(tau);
    performanceScore = performanceTransform(auditScore, harmScore,
       wPerf);
    reward = rewardTransform(performanceScore, wPun);
    LF = firmLossTransform(reward, transfer);
end

function lossScore = firmLossTransform(reward, transfer)
    lossScore = - transfer - reward;
end

function harm = harmFunction(alpha, controlCost, spendF, spendP,
   Vr, x)
    budget = budgetTransform(spendF, spendP);
    numControls = controlsAtSpend(budget, controlCost);
    tau = transmissionTransform(alpha, numControls, Vr, x);
    harm = harmTransform(tau);
end

function harmScore = harmTransform(tau)
    harmScore = (1 - nthroot(2 * tau - 1, 3))/2;
end

function performanceScore = performanceTransform(auditScore,
   harmScore, wPerf)
    performanceScore = wPerf * auditScore + (1 - wPerf) *
       harmScore;
end

function plotSequence(alpha, controlCost, R, spendP, Vr, wPerf,
   wPol, wPun, y_min, y_step, y_max)
    x_min = 0;
    x_max = R - alpha;
    x_step = (x_max - x_min)/10;
    xgv = x_min:x_step:x_max;
    [rows,len] = size(xgv);
```

```
ygv = y_min:y_step:y_max;
[yrows,ylen] = size(ygv);
meshgrid(xgv,ygv);
Z2Out = zeros(ylen,len);
Z3Out = zeros(ylen,len);
Z4Out = zeros(ylen,len);
for i=1:ylen
  for j=1:len
    Z2Out(i,j) = firmLossFunction(alpha, controlCost, R,
       ygv(i), spendP, Vr, wPerf, wPol, wPun, xgv(j));
    Z3Out(i,j) = harmFunction(alpha, controlCost, ygv(i),
       spendP, Vr, xgv(j));
    Z4Out(i,j) = polLossFunction(alpha, controlCost, R,
       ygv(i), spendP, Vr, wPerf, wPol, wPun, xgv(j));
  end
end;
figure;
xlabelstring = 'Pure␣Compliance,␣x';
ylabelstring = 'Investment,␣sF';
v = ones(1,ylen);
maxheight = max(max(Z2Out));
maxheighteps = maxheight + eps;
h = v .* maxheighteps;
s = 1:ylen;
ct = zeros(ylen);
cl = zeros(ylen);
for ks = 1:ylen
    ct(ks) = controlsAtSpend(budgetTransform(ygv(ks),spendP),
       controlCost);
    cl(ks) = controlsLeft(alpha, ct(ks));
end
boundarywidth = 2;
sp1 = subplot(3,2,1);
surf(xgv,ygv,Z3Out);
xlabel(xlabelstring);
ylabel(ylabelstring);
zlabel('h');
sp2 = subplot(3,2,2);
contour(xgv,ygv,Z3Out);
hold all;
plot3(cl(s),ygv(s),h(s),'Color','black','LineWidth',boundarywidth);
hold off;
xlabel(xlabelstring);
ylabel(ylabelstring);
sp3 = subplot(3,2,3);
surf(xgv,ygv,Z2Out);
```

```
xlabel(xlabelstring);
ylabel(ylabelstring);
zlabel('LF');
sp4 = subplot(3,2,4);
contour(xgv,ygv,Z2Out);
hold all;
plot3(cl(s),ygv(s),h(s),'Color','black','Linewidth',boundarywidth);
hold off;
xlabel(xlabelstring);
ylabel(ylabelstring);
sp1 = subplot(3,2,5);
surf(xgv,ygv,Z4Out);
xlabel(xlabelstring);
ylabel(ylabelstring);
zlabel('LP');
sp2 = subplot(3,2,6);
contour(xgv,ygv,Z4Out);
hold all;
plot3(cl(s),ygv(s),h(s),'Color','black','LineWidth',boundarywidth);
hold off;
xlabel(xlabelstring);
ylabel(ylabelstring);
str = 'alpha=';
function strOut = appstr(strNew)
  strOut = strcat(str,strNew);
end
str = appstr(num2str(alpha));
str = appstr(',␣controlCost=');
str = appstr(num2str(controlCost));
str = appstr(',␣R=');
str = appstr(num2str(R));
str = appstr(',␣spendFmax␣=␣');
str = appstr(num2str(y_max));
str = appstr(',␣spendP␣=␣');
str = appstr(num2str(spendP));
subtitle1 = str;
str = 'Vr=';
str = appstr(num2str(Vr));
str = appstr(',␣wPerf=');
str = appstr(num2str(wPerf));
str = appstr(',␣wPol␣=');
str = appstr(num2str(wPol));
str = appstr(',␣wPun=');
str = appstr(num2str(wPun));
subtitle2 = str;
spacetitle = '';
```

```
    suptitle({subtitle1;subtitle2;spacetitle});
end

function LP = polLossFunction(alpha, controlCost, R, spendF,
  spendP, Vr, wPerf, wPol, wPun, x)
    transfer = transferTransform(spendF, spendP);
    budget = budgetTransform(spendF, spendP);
    numControls = controlsAtSpend(budget, controlCost);
    auditScore = auditTransform(alpha, numControls,  R, x);
    tau = transmissionTransform(alpha, numControls, Vr, x);
    harmScore = harmTransform(tau);
    performanceScore = performanceTransform(auditScore, harmScore,
      wPerf);
    reward = rewardTransform(performanceScore, wPun);
    LP = polLossTransform(harmScore, reward, transfer, wPol);
end

function LP = polLossTransform(harm, reward, transfer, wPol)
    LP = transfer + reward + wPol * harm;
end

function punish = punishmentTransform(performanceScore, wPun)
    punish = wPun * performanceScore;
end

function reward = rewardTransform(performanceScore, wPun)
    reward = - punishmentTransform(performanceScore, wPun);
end

function transfer = transferTransform(spendF, spendP)
    transfer = spendP - spendF;
end

function tau = transmissionTransform(alpha, numControls, Vr, x)
    tau = 1 - (Uncontrolled(alpha, numControls, Vr, x)/Vr);
end

function uncont = Uncontrolled(alpha, numControls, Vr, x)
    uncont = Vr - controlled(alpha, numControls, Vr, x);
end
```