Resilience in Information Stewardship

Christos Ioannidis, David Pym, Julian Williams, and Iffat Gheyas

-WEIS 2014 -

PENNSYLVANIA STATE UNIVERSITY

23 June 2014

Resilience in Information Stewardship

1. Definitions

In the information ecosystem, threats to

the confidentiality, integrity, and availability

of individual components the ecosystem can be transmitted to others, impacting negatively on their security status .
In such an environment, the role of the :

information steward

is to maintain

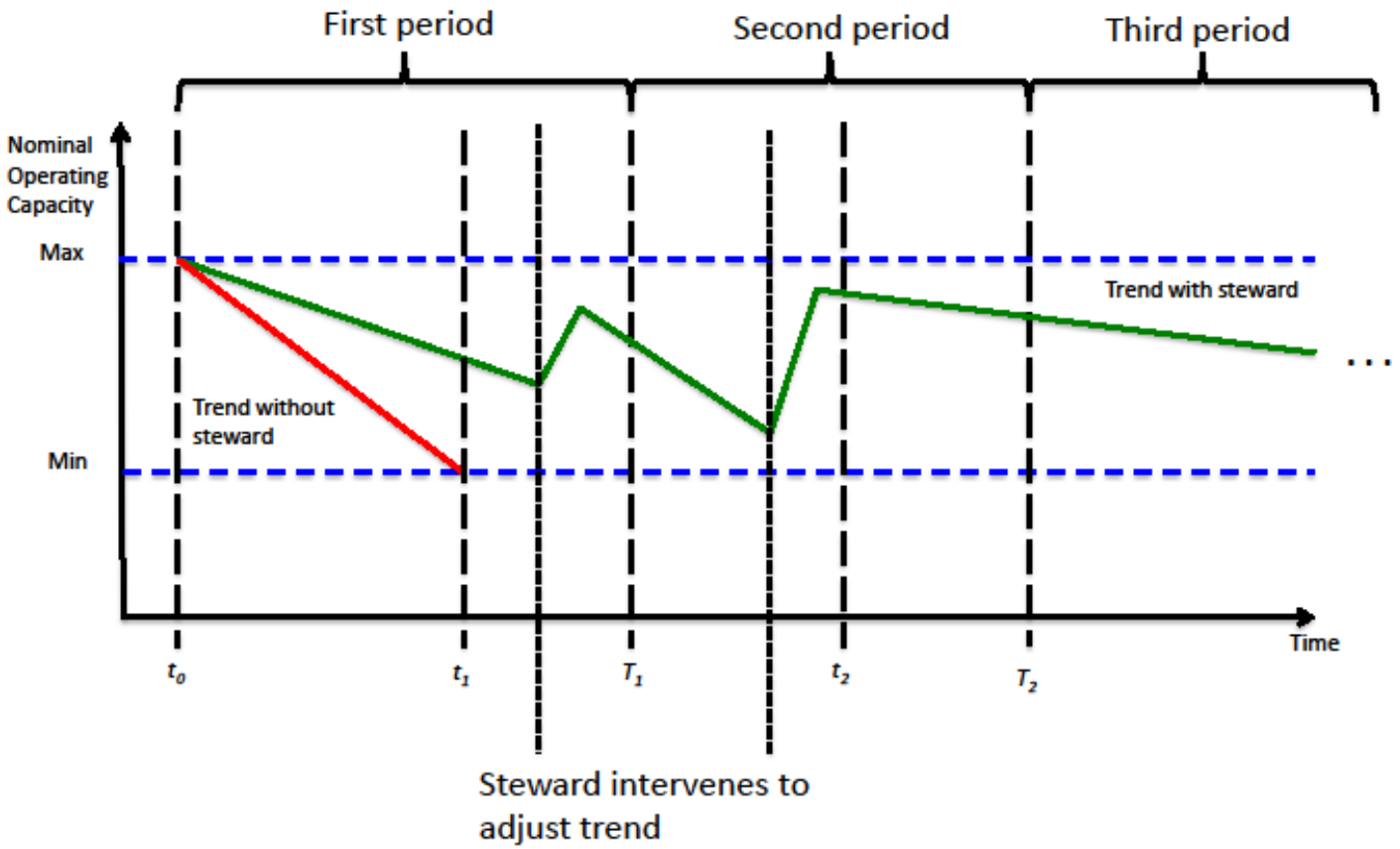
the sustainability and resilience

of the ecosystem's nominal operating capacity.

By the sustainability of a system, subject to finite degradation caused by a persistent stream of attacks, we mean its tendency to remain within specified levels of nominal operating capacity

Resilience in Information Stewardship

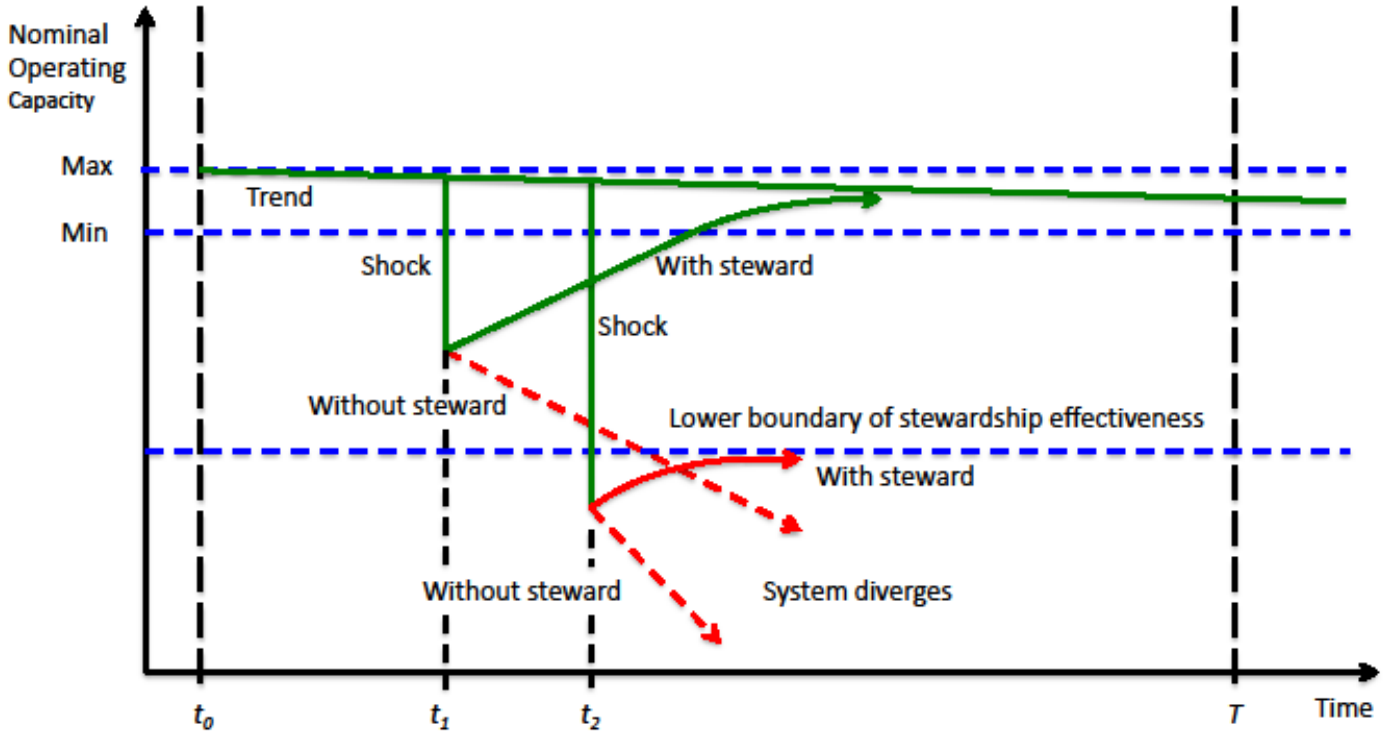
1. Definitions : Sustainability



By **resilience,** we mean the ability of the system to return back to its operating capacity to within the specified bounds following a shock

Resilience in Information Stewardship

1. Definitions : Resilience



We postulate that implicitly the "value" of information assets is signalled by their classification.

What's the mix ?

"ICS/SCADA" or "Corporate Information Assets"
Our main question centres on whether a firm would seek to adjust its declared mix of ICS/SCADA and Corporate Information Assets

Table: Decisions on: x_h, x_l, z. Parameters: $\psi_h, \psi_l, \alpha_h, \alpha_l$

	investments	allocation	risk-reduction rate	attacker elasticity
ICS/SCADA	x_h	$1-z$	ψ_h	α_h
Corporate	x_l	z	ψ_l	α_l

In the US, 1,900 bulk power system operators are regulated by
The North American Electric Reliability Corporation (NERC).
The corporate network has many of the same features as the
ICS/SCADA system and there are elements of substitutability between the two.
Consider an operator who could phase out using expensive fibre optic cables
to communicate between ICS/SCADA systems and substations
and replace them 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.

What's the response to this technological development, in terms of the system's ability to withstand a shock ?

We consider a set of N_T ex-ante identical targets choosing to allocate defensive expenditure x.
We consider two types of outlays h and l that correspond to the areas of high and low security
where information assets are held: The quantities

$$x_h \geq 0 \text{ and } x_l \geq 0$$

denote the one-off investments made at time t_0 in securing assets located in the corresponding areas.
And

$$z$$

is a switching variable such that a fraction $0 \leq z \leq 1$,of assets is allocated between h and l
Attackers per target is given by (η)

1. Modelling the Attackers I

Instantenous probability of a successful attack.

$$\tilde{\sigma_i} = e^{-\psi_i \mathbf{x}_i} \eta_i^{\alpha_i}, \qquad i \in \{l, h\}.$$

$$\alpha$$

parameter that captures the marginal effectiveness of an additional attacker per target

$$\psi$$

parameter that captures the relative rate of risk reduction for additional security investments by targets in each asset

1. Modelling the Attackers II

Let the reward $R > 0$ for a successful attack be proportional to the assets allocated in each area, h and l, and for notational simplicity 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 the attacker's time preference is described by δ.
The profit function for a single attacker is

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

2. Modelling the Targets I

For the targets of such attacks, 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

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

The optimal allocation bundle ?

$$(z^{\diamond}, x_l^{\diamond}, x_h^{\diamond}),$$

Setting up the Solution

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 rate, $\tilde{\theta} = \min(\delta, \beta)$, by construction

$$Limit_{T \to \infty} \int_{t_0}^{T} \tilde{\theta}^{-1} e^{-\theta t} dt = 1.$$

Therefore, the approximation of the time horizon $\tilde{T}$ covering the $1 - 1/\lambda$ proportion of the future losses is derived from $\tilde{T} = \log(\lambda)/\tilde{\theta}$. Assume that $\beta > \delta$ and $\tilde{T} = \log(\lambda)/\delta$, such that the interval t_0 to $\tilde{T}$ covers 90% of the expected present value; that is, $\lambda = 10$.

Solving the Model I:

$$Non - Cooperative \quad - \quad Nash \;\; Equilibrium$$

$$x_i^* = \frac{\alpha_i}{\psi_i} \log\left(\frac{L\psi_i\psi_j^2\left(e^{\delta T}-1\right)^2}{\gamma\delta\beta\left(\psi_j+\psi_i\right)^2}\right) - \frac{\alpha_i\delta T}{\psi_i}, \quad i \in \{I,h\}, j \in \{I,h\}, j \neq i$$

$$z^* = \frac{\psi_I}{\psi_h+\psi_I}.$$

Solving the Model I:

$$Non - Cooperative \quad - \quad Nash \;\; Equilibrium$$

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

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

3. Introducing the Steward

The first stewardship action we evaluate replicates our previous work by postulating a Stackelberg policy framework in which the policy-maker stewarding the system sets rules relative to a target level of sustainability.

When the steward is fully informed, our model reverts to the mechanism design problem in which the steward is able to set a mandatory investment bundle on the individual targets $(\bar{x}_l, \bar{x}_h)$ as well as imposing a specific asset allocation $\bar{z}$.

Solving the Model II: Introducing the Steward: The fully informed steward

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

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

Introducing the Steward: Does it work ?

Compare the attacking intensities as $\bar{x_l}, \bar{x_h} > x_l^*, x_h^*$ **(proposition 3)**

$$\bar{\eta_i} = \left(\frac{\psi_i \left(e^{\delta T} - 1\right) e^{-\bar{x_i}\psi_i - \delta T}}{\gamma\delta\left(\psi_j + \psi_i\right)} \right)^{\frac{1}{1-\alpha_i}} < \eta_i^* = \left(\frac{\psi_j (e^{\delta T} - 1) e^{-x_i^*\psi_i - \delta T}}{\gamma\delta(\psi_i + \psi_j)} \right)^{\frac{1}{1-\alpha_l}}$$

Does the institutional arrangement matter ?

3.1 Full Information with Limited Action: Majority and Minority Cases

3.1.a: The majority-action-case

- Consider the case in which the steward can **observe** $x_{i \in \{l,h\}}$ and z but can **only impose** constraints on x_h and z.
- Whilst the steward **can attain its desired risk expenditure trade-off** it can do so only at a **lower level of efficiency** (in terms of total initial cost $x_l + x_h$)

3.1 bThe Partially Informed Steward with Limited Action

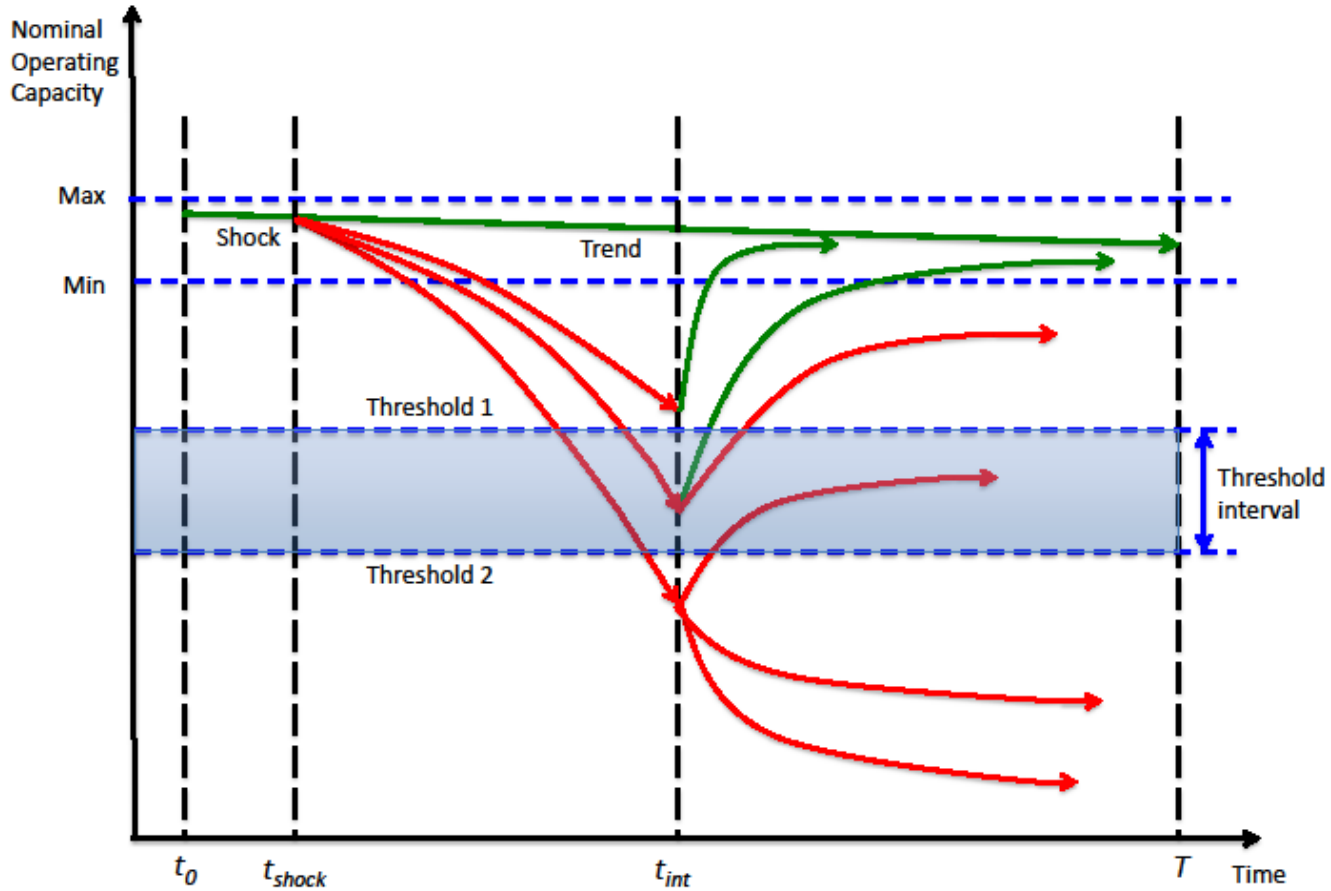
3.1.b *The Partially Informed Steward with Limited Action: Minority Case*

- The steward can **observe and internalize** the externality in η_h, **but cannot observe or enforce** z or x_I
- The targets then choose the investment and allocation bundle (x_I, z).
- The steward is simply given $\hat{L}$ by the targets and z is unrelated to the overall asset allocation of the targets from the point of view of the steward.
- The steward is not a Stackelberg policy maker, but in a Nash equilibrium with the targets and attackers.

- We show that there can be "natural limits" in the reaction of targets setting x_l and attackers choosing η_l
  The ecosystem's performance may be deteriorate, compared to the Nash Equilibrium case, when the stewards capacity is limited
- The Institutional Setup Matters !!!

3.1 bThe Partially Informed Steward with Limited Action

3.1.b *The Partially Informed Steward with Limited Action: Minority Case*



The combined outcome of the choices made by the agents, attackers and the steward about $x_{i\in\{l,h\}}$, z, and $\eta_{i\in\{l,h\}}$ are combined in the proposed : Total Non-Discounted Loss Function (below)

$$\begin{aligned}
\tilde{V}_A(\tilde{v},\tilde{u}) &= \int_{t_0}^{\tilde{T}} \tilde{z}\tilde{\sigma}_l\left(\tilde{x}_l,\tilde{\eta}_l\right)L + \left(1-\tilde{z}\right)\tilde{\sigma}_h\left(\tilde{x}_h,\eta_h\right)Ldt \\
\tilde{v} &= \left(\tilde{z},\tilde{x}_{i\in\{l,h\}},\tilde{\eta}_{i\in\{l,h\}}\right) \\
\tilde{u} &= \left(\alpha_{i,i\in\{l,h\}},\psi_{i,i\in\{l,h\}}\right), \qquad (2)
\end{aligned}$$

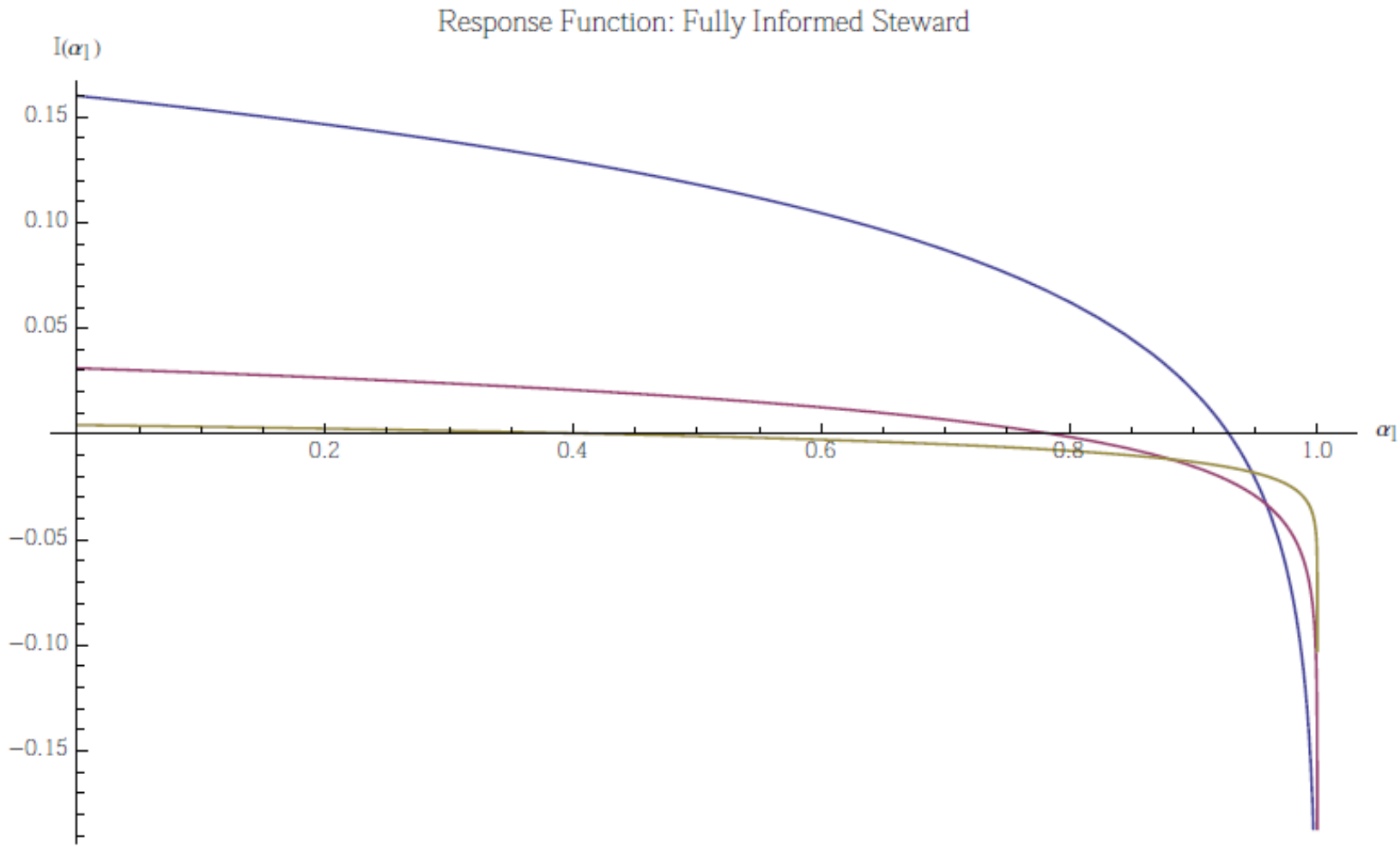
The value of $\tilde{T}$, represents the step-size of the periods considered in the model

For a single period, **resilience** will be measured by a response function to shocks to the parameters $\tilde{u}$.
Our choice of response function to technology shocks allows for shocks across the set of parameters $\tilde{u}$ either simultaneously of individually. It is given by the numerical evaluation of the following ordinary differential equation:

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

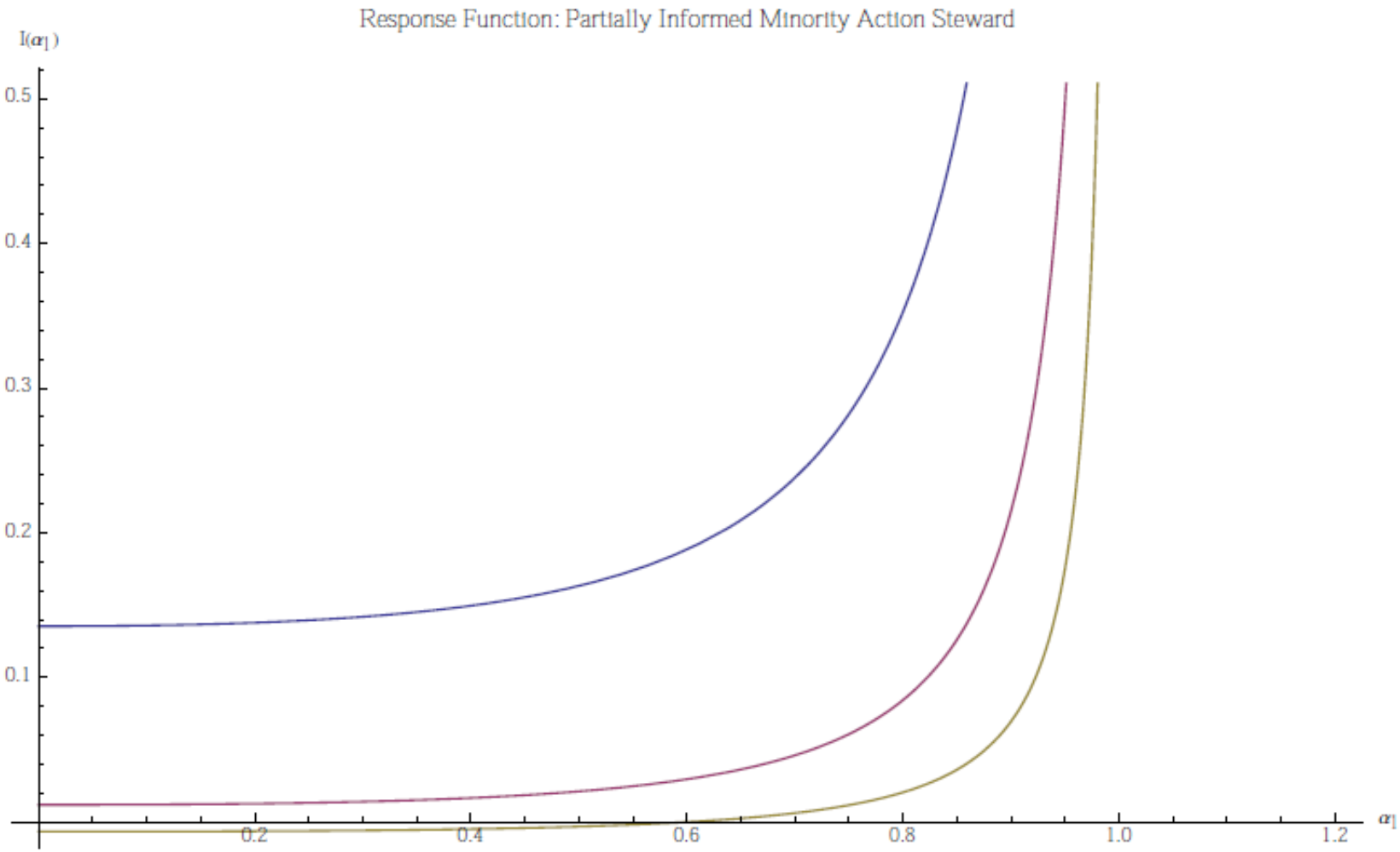
We are interested in establishing the existence of possible thresholds, , which describe levels of system operating capacity, as measured by loss, for differing degrees of stewart's effectiveness. We attempt to establish whether the system restores, through co-ordinated investment, to the target zone or not.

- 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 steward.
- To compare the resilience of the system when the stewards information set is restricted by comparing $\tilde{I}(u^*)$ and $I(\bar{u})$ to $I(\bar{u}^{\ddagger})$, for varying sizes of shocks in $\tilde{u}$.


Response Function: Fully Informed Steward
I(α1)
0.15
0.10
0.05
−0.05
−0.10
−0.15
0.2
0.4
0.6
0.8
1.0
α1

Resilience in Information Stewardship

TOWARDS A MODEL ; Measuring Resilience



The "creation/emergence" of an institution assigned the role of Infromation Stewardship can be truly beneficial for the resilience of the ecosystem.
The orderly co-ordination of the defensive postures assumed by the agents is fully incorporated in the responses of rational attackers
To achieve such co-ordination the structure of institutional arrangements is crucial, as the successful STEWARD requires:

- information disclosure on expenditure/investment in "information security"
- information disclosure about incidents of attack
- auditing and classification of assets
- authority to enforce expenditure in investment security

Failure to empower correctly the steward may actually be detrimental to the unregulated system's resilience