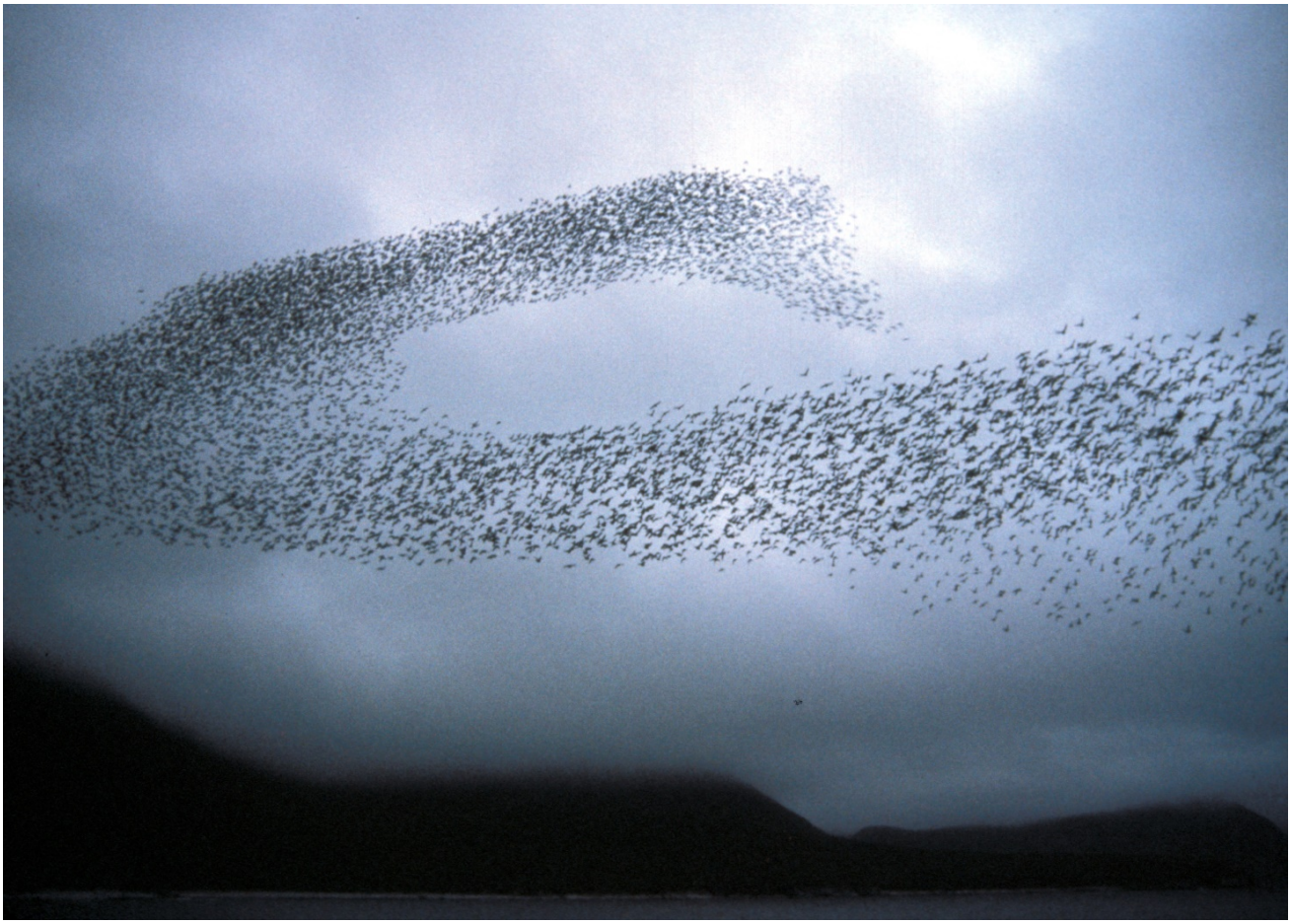
A New Perspective on Risk within Cyber Eco-Systems

Introducing the BHI – a new approach to modelling risk assessment of cyber eco-systems and their socio economic impacts.



Charles Fox – Security Lead Digital Catapult

Brian MacAulay – Lead Economist Digital Catapult

November 12th 2018

The project HERMENEUT has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740322

AN EXECUTIVE OVERVIEW

Digital Catapult has produced this short white paper to provide a high level overview of a new risk modelling approach, known as the Benefit Harm Index (BHI). This approach has been developed as a part of the Hermeneut Project. The Hermeneut project is a part of the European Community's Horizon 2020 Program.

The BHI modelling methodology is designed to provide new insights into the potential risks associated with the cyber eco-systems that underpin the complex and dynamic markets driven by the exploitation of emerging technologies. These rapidly evolving markets typically contribute significantly to national and international level economies and often form an integral part of Critical National Infrastructures.

Unlike a controlled (deterministic) system with a known set of risks and a well-defined future state, a complex system features many unknown risks and is evolving into something new that is not fully predetermined. In the complex biological world in which we live a single virus can mutate, evolve and spread through our Bio eco-systems and could result in a global pandemic infecting significant numbers of the human population. The ability for such microscopic changes in the Bio eco-system to propagate rapidly and create macroscopic effects (which can be positive or negative) highlights the uncertainty associated with such complex systems.

So it is with our Cyber eco-systems since these too are complex dynamic environments which evolve rapidly and feature high levels of uncertainty. These eco-systems can generate emergent behaviours that can often not be predicted by studying the way in which the constituent parts interact. We can see emergent behaviour manifesting itself in many forms including the murmurations of birds in the Biosphere and in the emergence of new socio political collective behaviours through the use of social media in cyberspace.

Attempting to apply traditional risk assessment methodologies to Cyber Eco-systems will typically involve pretence of knowledge of all the risks. Traditional risk assessment methodologies assume a complete knowledge of all possible states of the system being assessed and that a mathematical likelihood can be applied to each event. Such an approach to risk does not address the complex dynamics and the associated uncertainties of Cyber eco-systems.

The Hermeneut BHI introduces a new approach to risk assessment that models the growth of benefits and risk in the context of complex Cyber Eco-systems. It also features event driven scenario analysis methods, recognising the change of such systems over time.

Modelling the dynamic complexity provides a perspective for exploring the rate of growth of the socio economic benefits generated by an evolving cyber eco-system over time. It also provides a perspective for exploring the rate of growth of threats to that eco-system and the associated socio economic harm they could generate over time. The difference between the level of benefit and the level of harm at any given time period is a key output of the BHI model.

The event driven scenario approach enables us to explore the implications of cyber chain reactions to help identify hidden risks (and benefits) using tools such as the Implication Wheel. This helps us mitigate the fact that in complex dynamic systems we do not know all the risks some of which are emergent and may be very significant.

The BHI methodology exploits many of the principles of the latest research in economics (Ref 1), which also recognises that the real economy is a complex living system within other systems. When we apply our BHI methodology to a target Cyber eco-system we can explore the balance between benefit and harm and how that balance changes over time at a macro-economic level. We use BHI to identify and mitigate emergent threats then we explore eco-system level mitigation strategies for those scenarios where the socio-economic harm outweighs the benefits. The residual risks can then be managed using traditional risk assessment methodologies.

CONTENTS

1 USING BHI TO MITIGATE TO EMERGENT THREATS

Cyber eco-systems are complex systems and such systems exhibit emergent behaviour. There are different levels of complexity and as the complexity increases different types of Emergent behaviour come into play, these being:

1. Simple Dynamic behaviour (e.g. clock, measuring time)
2. Weak Emergent behaviour (e.g. Flocking of Birds/ drones)
3. Strong Emergent behaviour (e.g. Bubbles in the Financial Markets)
4. Spooky Emergent behaviour (e.g. Conscious thought in humans / AI)

The first two are associated with deterministic systems. These types of emergent behaviour can be easily reproduced using simulations of the system. The third and fourth are associated with stochastic (random interactions defined by probability distributions) systems. Stochastic systems can exhibit strong emergent behaviour that cannot be fully reproduced by simulations. Spooky emergent behaviour cannot be reproduced even by detailed simulations of the systems.

If you are governing / operating a Cyber eco-system the extent to which you (as its defender) can control it is intrinsically linked to the level of complexity of that eco-system. The stability of the system is related to its level of complexity, changes at the micro level can result in dramatic change at the macro level. An attack on the system can trigger a significant cyber chain reaction which will appear as an Emergent behaviour.

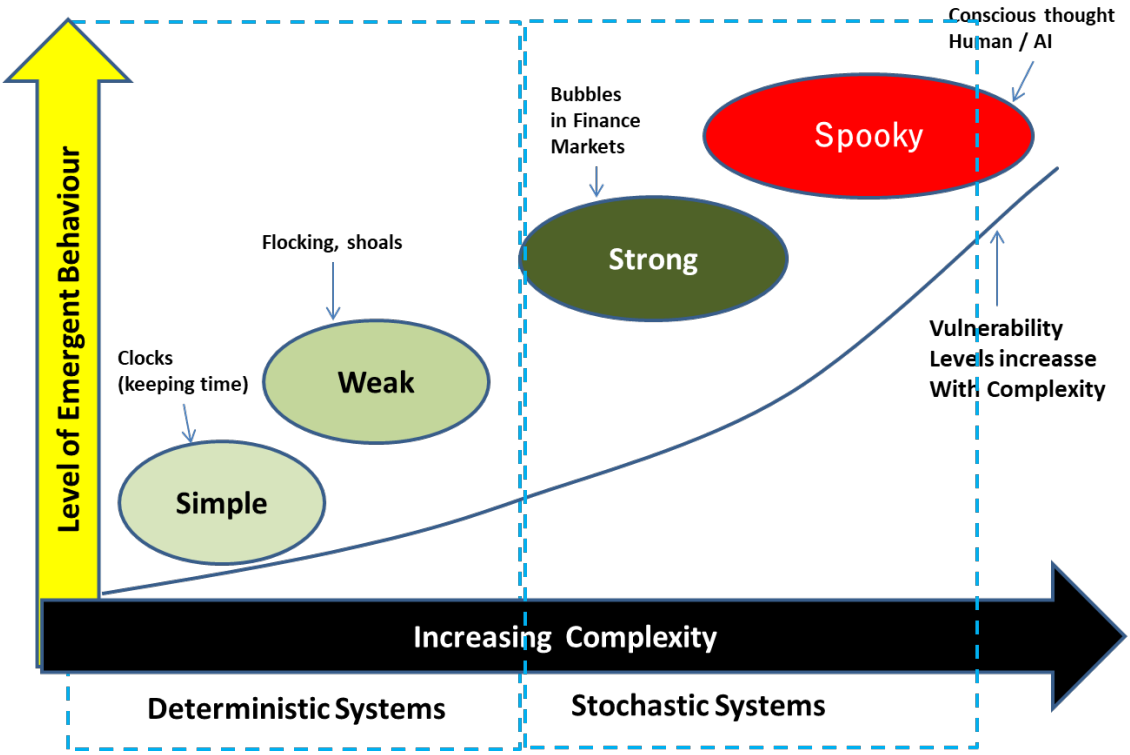


Figure 1 – Complexity and Emergent Behaviour

In the case of Strong and Spooky emergence (stochastic systems) then the system is fundamentally uncontrollable! In simple terms, the higher the complexity of the eco-system the more vulnerable it is to emergent threats.

One of the key components of the BHI approach to dynamic risk involves mitigating Emergent threats in complex eco-systems.

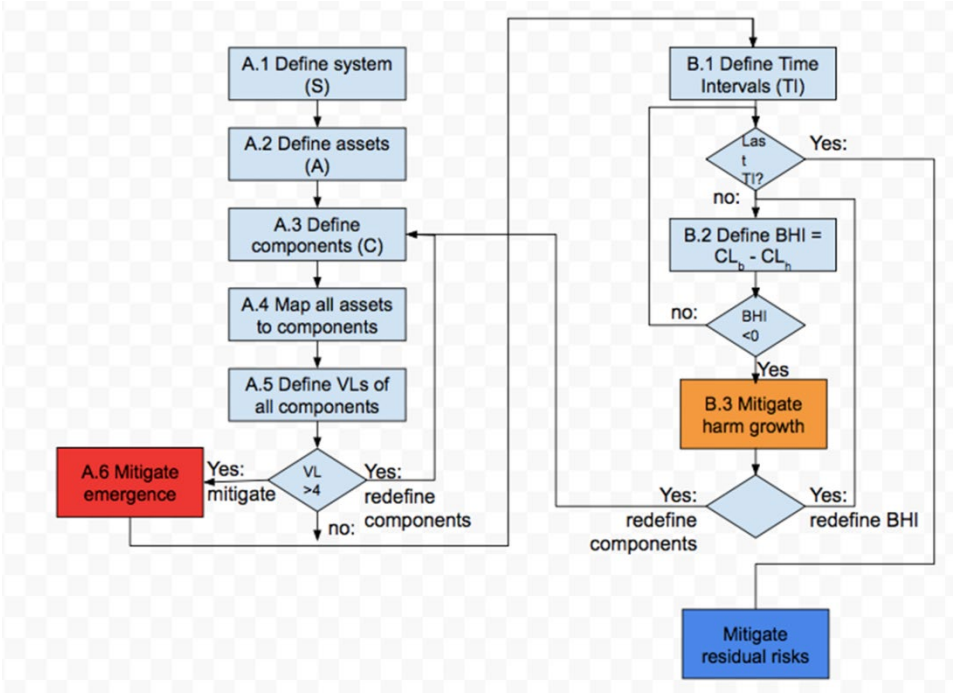


Figure 2- BHI Process for mitigating Emergent Threats

The first three steps for addressing Emergent Threats (A.1-A.3) as shown in Figure 2 define:

- A.1: The Eco-System being considered,
- A.2: The set of Assets, whose sensitivity is such that their loss or compromise would cause significant harm, and which - as a whole or in part - may be of interest to a threat agent for malicious, fraudulent and criminal behaviours or activities.
- A.3: The set of Components, into which the system is decomposed. A component must contain hardware and may contain software and data. It is assumed that components can communicate with each other using sufficiently secure protocols.

The fourth step (A.4) defines the association between each asset and the component(s) that directly influence the security of the asset.

The fifth step (A.5) defines the vulnerability level (VL) for each component. In the BHI approach there are distinct levels of Vulnerability that increase with the complexity of the eco-system. This activity is performed considering the nature of a component and its vulnerabilities, as well as the threats from the environment and other components.

If any component has VL>4, which corresponds to emergent threat, the process takes one of two paths:-

- Redefine the components, for example to localise an associated asset in a component that has a lower VL value. This results in re-iterating over steps A.3-A.5.

- Mitigate emergence (A.6), by designing a set of security controls that seek specifically to mitigate risks from emergence. These controls will necessarily need to detect, and potentially isolate and neutralise the impact of an attack.

Using BHI, it is expected to distinguish those characteristics that can be localized, from those that cannot. One cannot expect companies rationally to mitigate the latter, so we must apply other classes of intervention to safeguard the ecosystem. For the latter class, mitigations must be a set of governance, standard, and other interventions across the ecosystems, and key

criteria for adoption must seek to minimize impact on the individual organisations adopting such recommendations.

Once this process has iterated to completion, the process of considering emergent threat is complete, and analysis passes to using BHI to mitigate threats from growth.

2 USING BHI TO MITIGATE TO THE GROWTH OF HARM

Modelling the dynamic complexity provides a perspective for exploring the rate of growth of the socio economic benefits generated by an evolving cyber eco-system over time. It also provides a perspective for exploring the rate of growth of threats to that eco-system and the associated socio economic harm they could generate over time. The difference between the level of benefit and the level of harm at any given time period is a key output of the BHI model.

Benefit and Harm can grow at different rates within a Cyber eco-system. There are two key features of complex eco-systems that help to refine our understanding of these growth rates. **First each eco-system** will evolve through a number of distinct phase transitions as it evolves.

For example the introduction of a new product or class of products - penetrates a market Initially there is near exponential growth, which is often modelled as compound growth in business plans, with a constant or slowly varying Compound Annual Growth (CAGR) parameter. As penetration of the market occurs and saturation approaches, and the Bass Diffusion distribution starts to manifest its asymptotic growth complexity level of 0 – a constant.

It is therefore appropriate to consider the BHI in three distinct time intervals:

- TI0 – from product introduction when the complexity level is 4 (exponential)
- TI1 – from when the complexity level transitions from 4 to 0
- TI3 - from market saturation onwards, when the complexity level is 0 (constant).

Second each eco-system will typically have multiple domains each of which can feature different levels of complexity and associated growth rates.

The right-hand side of Figure 2 shows the process for using BHI to mitigate threats from growth.

The first step (B.1) defines the set of Time Intervals, that are relevant to the various developments of both the benefit and harm over time. In particular, these time intervals will consider for example:

- The time of events that mark the start and end of relevant changes, such as investment rounds, introduction of new products, etc.

- The time at which the distribution of growth is likely to be discontinuous, for example as a result of some material event, such as change in a product or the channel it uses to access the market.

The second step (B.2) iterates over the intervals to compute the Benefit to Harm Index (BHI) for each sub interval, by determining the Complexity Index (CI) for each growth distribution. If the BHI is negative, indicating that the CI for growth of harm exceeds that of benefit, the process proceeds to mitigate harm growth (B.3), which specifies security controls that seek to mitigate the growth of harm. In the case that a plausible mitigation is found, the process re-computes the BHI value and iterate to the next time interval.

In some cases, for example where an effective mitigation cannot be found, it may be considered appropriate to redefine the components. In this case, the process returns to the right-hand side of the diagram at step (A.3).

Level of Benefit	Level of Harm 0	1	2	3	4
0	0	-1	-2	-3	-4
1	1	0	-1	-2	-3
2	2	1	0	-1	-2
3	3	2	1	0	-1
4	4	3	2	1	0

Figure 3 – The BHI for distinct time intervals

For BHI < 0 systemic (eco-system) level mitigations are required.

Once all members of CI have been processed, the mitigation of risks from growth are complete, and the process can continue by using traditional risk management techniques to address any residual risks

3 APPLYING BHI TO CYBER ECO-SYSTEMS

To apply the BHI methodology to a target Cyber Eco-System we use the following high level eco-system domain model.

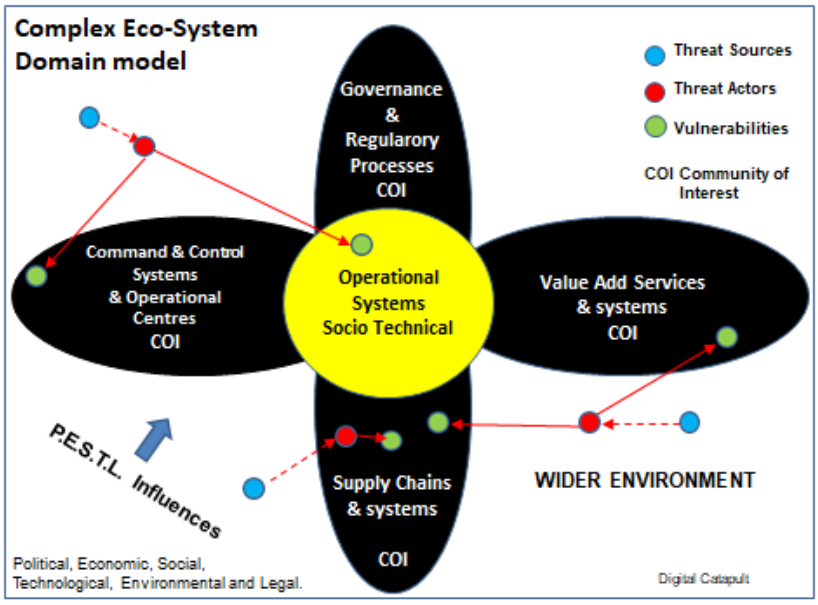


Figure 4 - Cyber Eco-System High Level Domain Model

A Cyber Eco-System is a complex system of systems, where each system can be modelled in terms of a set of interacting components. Each Eco-system will have a scope / system boundary and will typically be embedded in a wider environment. This wider Environment will generate Political, Economic, Social, Technological, Environmental and Legal (PESTL) influences on the operation and growth of that Eco-system.

In our approach each Cyber Eco-system is structured into a number of domains that support different dynamic communities of Interest (COI). As shown in Figure 4 these domains reflect the distinction between e.g. the operational systems within the ecosystem and the supply chain systems that support the manufacture and production of the components that eventually populate that operational systems domain.

The other domains shown include the Command & control systems domain and the underlying system components, processes and interactions that comprise them. The Governance and regulatory processes domain that contains the governance systems and regulatory frameworks that are used to set and police the policies rules and standards associated with governing the cyber eco-system. The final domain is the Value added services domain that includes the systems and processes associated with services that add value to the operational services, for example Insurance services.

The Cyber-system domains will all have vulnerabilities. Threats to the Eco-system will exploit these vulnerabilities through attack vectors originating from threats sources (e.g. hostile state) attacking via threat actors (external & internal), as illustrated schematically in Figure 4. Our BHI approach exploits methodologies such as the Implementation wheel to investigate the vulnerability levels of components in such complex systems and the potential for cyber chain reactions being generated through multiple iterations. We use targeted scenario analysis in this context to help identify such events through systematically exploring the implications of interaction / contagion through multiple first, second, and nth order interaction flows.

Our BHI dynamic approach to risks also enables us to construct multiple phase states of each Cyber Eco-System model to reflect the different evolutionary states. This is then used to help crate the BHI growth model across those different time intervals, resulting in an output of the form shown earlier in Figure 3.

4 FIND OUT MORE ABOUT BHI AND THE WIDER HERMENEUT PROJECT

The BHI approach is described in full technical detail in EU Hermeneut project deliverable document, D4.2 BHI Index report. This is available on the Hermeneut site at the following link: https://www.hermeneut.eu/resources/

Hermeneut's cybersecurity cost-benefit approach to risk assessment combines integrated assessment of vulnerabilities and their likelihoods with an innovative macro- and micro-economic model for intangible costs, delivering a quantitative estimation of the risks for individual organisations or a business sector and investment guidelines for mitigation measures.

Learn more about the wider Hermeneut project here: https://www.hermeneut.eu/about/

Enterprises intangible Risk Management via Economic models based on simulatioN of modErn cyber-aTtacks

HERMENEUT

CATAPULT Digital

REFERENCES

(Eds) (1997) The Economy as an Evolving Complex System II. Proceedings Volume XXVII Santa Fe Institute Studies in the Science of Complexity, Reading, MA: Addison-Wesley