Achieving cybersecurity improvements through Enterprise Systems Engineering

Tania Wallis, University of Glasgow, tania.wallis@glasgow.ac.uk

Categorisation

- Accessibility: BEGINNER
- Application: GOOD PRACTICE
- Topics: Enterprise Systems Engineering, Cyber Security, Risk Management, Critical Infrastructure, Supply Chains

Abstract

The Critical Infrastructures (CI) that provide essential services such as energy, water and transport have been undergoing a digital transformation to achieve more effective and efficient operations. These changes are increasing the potential attack surface and exposure to cybersecurity incidents. The EU Directive on Security of Network and Information Systems (NIS Directive) (National Cyber Security Centre, 2018) has brought a new emphasis on improving the cybersecurity of essential services. It has introduced mandatory incident reporting and a framework to raise the cybersecurity and resilience levels of CI.

Rather than a dislocated approach to managing the system in parts, taking on responsibility for cybersecurity requires an integrated, whole-system governance approach, to discover the full end-to-end picture and risk assess the potential gaps in security. The NIS Directive expects cybersecurity to be managed through the wider system of contractors and sub-contractors and vendors to the sector, all participating in a complex adaptive system. From whole organisations down to products, components and data flows, deciding the scope of critical systems that support essential services has integrated activity across different work areas such as operational technologies, enterprise IT and telecoms networks. Understanding the end-to-end system and whole enterprise interactions is necessary to achieve the outcome-based nature of the NIS Directive.

This paper investigates the activities that have evolved to secure the broader and deeper supply chains as well as internal networks and systems of CI organisations. Enterprise Systems Engineering (ESE) is introduced as a tool to facilitate the shared cybersecurity requirements across organisations for securing essential services, streamlining whole system security behaviours of people, processes and technology towards a more resilient CI.

Introduction

The NIS Directive was transposed into UK law in May 2018. It requires operators of essential services to manage their cybersecurity risks and protect against cyber-attack, while increasing their ability to detect cybersecurity events and minimise the impact of incidents. The NIS Directive also expects an understanding and management of the cybersecurity risks presented by tiers of supply chains.

"An enterprise is a complex, socio-technical system that comprises interdependent resources of people, information and technology that must interact with each other and their environment in support of a common mission" (Giachetti, 2010). Systems Engineering addresses complex technical systems with many stakeholders. ESE adapts the Systems Engineering concept to socio-technical systems including a significant human aspect. Rather than being for single projects, ESE is a continuous process due to enterprises constantly evolving (White and Rebovich, 2011). The systems approach allows a process to unfold and encourages adaptability to an evolving situation. Decisions are informed by the set of relationships between interdependent actors (Jackson, 2003). ESE involves aligning all the small developments across the enterprise to contribute to the purpose of a whole enterprise (Giachetti, 2010).

There is a vast array of issues affecting the cybersecurity of our CI that involve technology, people, processes and organisations. This paper presents ESE as an approach to align the achievements so far to improve the cybersecurity of CI. Guiding whole system influences, towards a common purpose of a more resilient, cybersecure system, requires agreed actions and shared accountability within a performance framework to chart progress. The application of ESE methods demonstrates how the interactions and combined efforts of multiple organisations can direct participation in a complex adaptive system and achieve the outcome of improved cybersecurity levels. In this paper, the term 'Enterprise' will refer to the combined endeavour involving both public and private actors to improve cybersecurity. In particular it refers to the collaborations and partnerships that have evolved with a vision to improve cybersecurity across interdependent activities. This analysis is based on the author's interviews and discussions with industry and government, on participation in cybersecurity Public-Private Partnerships (PPP) as well as on academic literature.

The NIS Directive

The NIS Directive has established a communication structure among private and public organisations to support improving the cybersecurity capability of essential services. Implementing the NIS Directive has introduced the following roles:

- **Operators of Essential Services (OES)** are implementing the NIS Principles and are required to report incidents affecting essential services to the Competent Authority.
- **Competent Authorities (CA)** produce sector specific guidance and are required to audit and assess the cybersecurity levels achieved by OES in their sector.
- **Computer Security Incident Response Team (CSIRT)** provides technical expertise and assistance with cybersecurity incidents.
- **Single Point of Contact (SPOC)** engages with EU partners and participates in the NIS Cooperation Group to further international cooperation.

In the UK, the National Cyber Security Centre (NCSC) performs the role of CSIRT and SPOC as well as offering advice and guidance to OES and CA in tailoring NIS requirements to each sector (NCSC, 2019a). NIS assumes responsibility on individual OES to take appropriate measures to secure their supply chain where their essential service is dependent on a third-party product or service. This has proved problematic as individual OES often have little negotiating power to ensure their security requirements are met, especially where the choice of suppliers is limited. In addition, OES have limited visibility of their supply chain beyond tier 1 suppliers to really know and manage their supply chain risks (Wallis and Johnson, 2020).

A response is required beyond organisational boundaries, with contributions from multiple owners and accountability to cybersecurity. Figure 1 shows an individual OES having control over some aspects of the system to be secured and needing to use their influence, as far as they can, to negotiate the required security for other aspects of the system. Cyber maturity assessments that focus on this area of control rest on a relatively narrow evidence base without considering dependencies across extended supply chains. Cybersecurity often entails a sharing of risk that requires a collective effort to mitigate (Christensen and Petersen, 2017). The area of influence in Figure 1 includes OES engagement with other organisations tasked with NIS responsibilities and includes their relations with suppliers to negotiate security requirements. The area outside OES control includes the changing threat landscape, the many unknowns in cybersecurity and areas where an OES has limited visibility, such as sub-contracting processes or components used in devices and systems. The potential sphere of influence can be expanded through the collaborative effort of stakeholders to contribute to understanding the latest threat landscape, reducing vulnerabilities and minimising the impact of incidents (Wallis and Johnson, 2020). ESE offers a synthesis by looking at the problem of securing an OES within the context of its containing whole, hence making the solution space larger (Rebovich, 2005).

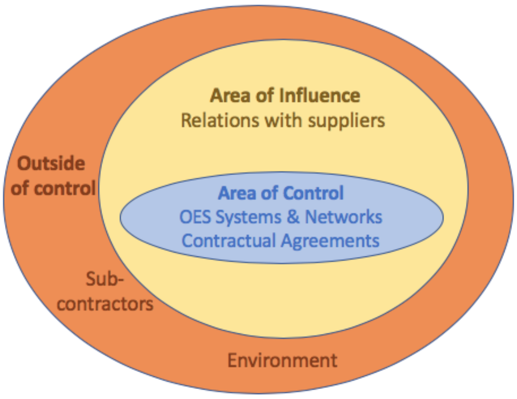

Figure 1 OES areas of influence and control

There have been a multitude of adaptations to implement the NIS related initiatives. This paper considers the overall enterprise of activity as a collaboration of several organisations to develop cybersecurity capability and support the delivery of essential services. “Proper management of the enterprise and extended enterprise increases resilience” (Madni and Boehm, 2017). The whole ‘enterprise’ of influence being considered includes:

- OES.
- Suppliers directly contracted by an OES.
- ‘Extended’ enterprise of supply chain activity.
- Government departments guiding the cybersecurity improvements of each sector.
- Collaborations and partnerships sharing best practice information for each industry sector.

Managing Complexity

The complexity of the whole system reduces an individual OES' ability to control and direct the required outcomes of the NIS Directive. Improving their ability to influence the outcomes would help to manage the complexity and achieve more holistic improvements in cybersecurity. Exploring what it means to comply with the NIS Directive has resulted in a proliferation of approaches to the problem, displayed by the horizontal axis in Figure 2. While each OES acknowledges a similar need for cybersecurity, their response to that need can be quite different, depending on existing capability and the risk appetite of each organisation. Negotiating cybersecurity requirements of suppliers has been challenging for individual OES, they have looked to a more uniform approach to collectively negotiate alongside other OES their expectations on suppliers, represented by the vertical axis in Figure 2. When a circle of control is relatively small, balancing differentiation and integration in a complementary way can achieve the best outcomes. The NIS implementation has enabled OES to seek a balance of actions for efficiency and order with effective adaptation to the environment (Swarz and DeRosa, 2006).

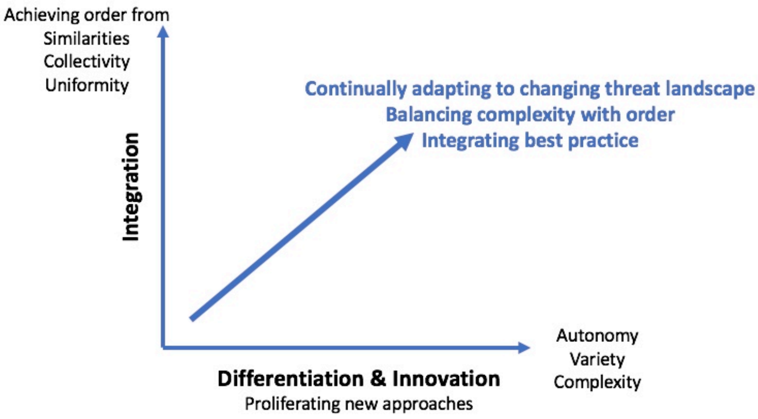
Achieving order from
Similarities
Collectivity
Uniformity
Integration
Continually adapting to changing threat landscape
Balancing complexity with order
Integrating best practice
Autonomy
Variety
Complexity
Differentiation & Innovation
Proliferating new approaches

Figure 2 Balancing Complexity with Order

Emergence of Trusted Partnerships

There are key and potentially complementary differences in focus between government and private sector cybersecurity requirements. From a government perspective there is a need to assure the cybersecurity of essential services that are provided over privately owned CI. Government interest tends towards defence of the nation and the attribution of perpetrating actors. Their view is more outwardly focussed towards threats from other states or state-sponsored actors. Conversely the private sector is more inward looking and focussed on vulnerabilities. Their attention is on the inevitability of cybersecurity risks and balancing those alongside other business risks. A private actor's inward view is to detect, mitigate and foster their ability to recover from attack. Awareness of a company's reputational risk has also brought more emphasis to cybersecurity preparedness. Embracing the diverse perspectives of public and private sector participants, could bring "many different threat realities and approaches" to the table (Christensen and Petersen, 2017).

The concept of cybersecurity as a shared mission and the reality that "no single management entity has control over the whole" (Swarz and DeRosa, 2006) has encouraged Public-Private Partnerships (PPP) or Information Sharing and Analysis Centres (ISAC) to form, enabling government and industry to work together. An enabling 'enterprise' is already emerging from combined efforts across industry and through such trusted partnerships. There would be a massive overhead of cost and time for each OES to attend to the cybersecurity of their entire supply chain, with thousands of suppliers and testing of all components being unachievable (Madni and Boehm, 2017). Instead, for example, a group of OES are collaborating to discuss their common security requirements and meeting with suppliers to discuss requirements that can be built into suppliers' offerings, rather than cybersecurity add-ons being sold separately to each OES (Wallis, 2020).

A wider participation of both public and private actors in this task would aid a more balanced intervention by government (McCarthy, 2018). Reducing risks to acceptable levels depends on the risk appetite of each individual entity. The capability to achieve NIS outcomes is upheld by an entity's business interests and goals. Governments need to achieve an acceptable security level for their nation from a mix of different private sector responses to the risks. An ESE approach can be used as a tool to find common ground, as well as understand the differing requirements, to design how to work together, understand and integrate the different requirements of business and government. This would allow a broad and flexible understanding of the shared risks enabling a continuous adaptation "to the benefit of both the individual partners and the common good" (Christensen and Petersen, 2017).

PPPs in cybersecurity have been shown to be based on more than a strategic self-interest and management of reputational risk. There is a social glue that binds these partnerships with professional loyalty, founded by higher moral principles. This gives a subtle power of commitment and loyalty to these partnerships that goes beyond simple strategic interests. Embracing the different perspectives from diverse participation also gives value to the PPP. Such partnerships bring "a commitment to future commitments" (Christensen and Petersen, 2017) often through voluntary contribution and going beyond immediate results without specifying outcomes. This commitment requires:

- Openness and trust.
- Shared understanding of risks/threats requiring mitigation through collective effort.
- Collaboration for new solutions to a common purpose.
- Long term relations (Christensen and Petersen, 2017).

Tasking CA, NCSC and OES with NIS responsibilities has established a "trust anchor" (Distelrath, 2019) for incident reporting and a collaborative operational responsibility to support the protection of systems operated by OES. The use of a trusted intermediary has proven to be particularly effective in anonymising and normalising information, to establish a risk picture for the energy sector and identify areas where a combined approach offers more scope for progressing issues (Wallis, 2020). The Energy Networks Association (ENA) provided cybersecurity procurement guidance through a collaboration of government, vendors and operators (ENA, 2016). Also, the idea of a common assurance framework is evolving to achieve a more cost-effective balance between variety and commonality in the system. Such partnerships and collaborations provide an important foundation to assemble and discuss the requirements of government and the private sector. Facilitation through ESE prioritises the interconnectedness and dependencies because the design extends across organisations to achieve the required capability, while acknowledging the limits to cooperation where interests of government and private actors are more disparate.

Shaping Interactions

To progress the ESE concept from Figure 2 of balancing complexity with order, Figure 3 illustrates interactions patterns shaping the selection of strategy or best practice from the varied approaches arising from different NIS implementations (Swarz and DeRosa, 2006). Trusted partnerships such as PPPs or ISACs can provide a context to shape interactions and direction, with awareness of the whole set of public private interests. This provides a context for the required behaviour, creating the space to modify behaviours through awareness (Koop and Lodge, 2017). The selection of best practices/solutions need to be based on local considerations as well as the CI system as a whole.

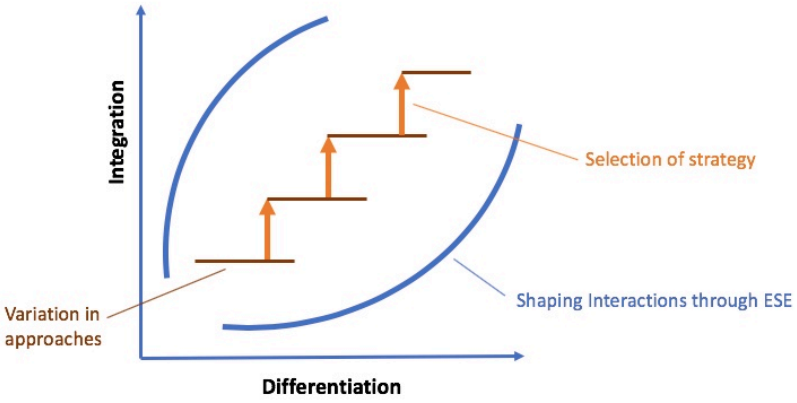

Figure 3 Shaping interactions to discover and implement best practices (Rebovich, 2005)

The NCSC have provided a Cyber Assessment Framework (CAF) from the NIS outcomes (NCSC, 2019b). The CAF acts as a “shared image” and “common perception” for all components in the Enterprise to adhere to (Swarz and DeRosa, 2006). The CAF was originally provided to support the implementation of the NIS Directive by OES. It has since been expanded for a wider user base to be applied to other parts of CI and to cyber related safety risks. From this CAF the CA for each sector has decided on baseline targets and an outline approach per sector. This has enabled a range of methods to be trialled at the CA level. The CAF profile is providing a target state per sector for the system to work towards.

Rather than a prescriptive approach, the NIS outcomes give the OES a choice in how they manage their own risks. The OES complete a self-assessment and produce their own cyber security improvement plans. This has also triggered a variety of approaches by OES in how they achieve the NIS outcomes (Wallis, 2019).

There is a verification activity by CA as they audit OES against their self-assessments and improvement plans. CA are also offering improved guidance to OES to support weaker areas. There have been investigations into dependencies on common suppliers and components to discover where there is a requirement for greater diversity of technology for a more resilient infrastructure. However, a diversity of vendors may not improve resilience if their products share common components and vulnerabilities (Wallis, 2020).

The progression of the Enterprise pictured in Figure 3 is exemplified through the activity of assessing the current state of the system against a target state to expand the existing set of capabilities:

- Current state, decided through OES self-assessment.
- Target state, NIS principles and CAF profile setting baseline expectations for each sector.
- Gap in capability, identified in OES Improvement Plans, audited by CA.

The practice of ESE can facilitate an integrated set of organisations, understand their roles and responsibilities, to foster an environment in which cybersecurity capability can emerge. A synthesis of knowledge and experience from different stakeholders, and integration of the multi-dimensional aspects is crucial to improve the cybersecurity performance of industry (Hoogervorst, 2009).

Enterprise Engineering a complex adaptive system

The inability of OES as individual entities to make progress with securing global supply chains requires a collaborative intervention from public-private partnerships. The task is too vast for individual organisations to resolve using varied approaches. It requires a balance between a more uniform approach to meet common needs and requirements while retaining the ability to form bespoke solutions for specific deployments by different OES (Wallis, 2019).

To improve the cybersecurity capability of the whole system requires a shared understanding of the threats to give a context of scenarios to prepare for. A combined effort in this regard can be more effective and efficient. The gathering of knowledge through incident reporting to CAs will provide "a more comprehensive view of the current threat landscape" (Christensen and Petersen, 2017). Private companies are interested in the knowledge compiled by government where it can be shared to assist preparations. OES can be caught in the crossfire of attacks that were targeted elsewhere when they carry the same product vulnerabilities in their infrastructure (Wallis, 2020).

Beyond post incident analysis, potential earlier alerting to the latest threats has been proposed by the Network Code on Cybersecurity (Distelrath, 2019). Cyber threats against CI require information sharing and collaborative partnership "to improve the volume, timeliness, and quality of shared cyber threat information" (Madni and Boehm, 2017). Multiple perspectives are required to maintain awareness of the environment, to gather the latest threat picture and anticipate preparations. Adaptability to this dynamic situation requires (Madni and Boehm, 2017):

- Self-awareness, enabled by the NIS self-assessment and improvement plans.
- Context awareness, knowing the latest threat scenarios to prepare for.
- Shared awareness, shared risks requiring a collective effort to mitigate.
- Maintain awareness, through combined governance and oversight.

While risks are somewhat shared through collaborations or transferred through outsourcing, the private sector entity owning the assets and providing the essential service retains the liability. Where NIS outcomes cannot be achieved by an individual OES working alone, ESE offers a tool to coordinate and facilitate the ecosystem of private sector capability across multiple organisations, to understand fully what the requirements of government and private sector are in cybersecurity of CI and how to achieve them, by individual OES or sector collaborations.

Conclusion

The process of NIS implementation has mobilised some collaborations to more effectively work towards the outcomes required by the NIS Directive. This has highlighted the importance of partnership to achieve cybersecurity across dynamic and extended boundaries. An ESE approach adds to this by enabling continuous changes to be managed to adapt the enterprise towards meeting new threats, facilitating a continual redesign of the enterprise to respond to the latest cybersecurity challenges (Giachetti, 2010).

NIS implementation and cybersecurity improvements need to be embodied within a form of enterprise governance to acknowledge the socio-technical dynamics and to organise adaptations to the evolving threats and risks. (Hoogervorst, 2009) (Koop and Lodge, 2017). The application of ESE concepts can provide a more joined-up approach to resolving and implementing an improved cybersecurity level for CI. Rather than traditional systems engineering thoroughly specifying system elements, ESE can hold an integrated, constantly evolving entity to enable the required capability to emerge (White and Rebovich, 2011). This cybersecurity case study provides a basis for further development and could also be usefully applied to other socio-technical enterprises undergoing change.

References

Christensen, K. K. and Petersen, K. L. (2017) 'Public-private partnerships on cyber security: A practice of loyalty', *International Affairs*, 93(6). doi: 10.1093/ia/iix189.

Distelrath, V. (2019) *Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management*.

ENA (2016) *Energy Delivery Systems - Cyber Security Procurement Guidance*.

Giachetti, R. (2010) *Design of Enterprise Systems. Theory, Architecture & Methods*. CRC Press.

Hoogervorst, J. A. P. (2009) *Enterprise Governance and Enterprise Engineering*, *Enterprise Governance and Enterprise Engineering*. doi: 10.1007/978-3-540-92671-9.

Jackson, M. C. (2003) *Systems Thinking. Creative Holism for Managers*. Wiley.

Koop, C. and Lodge, M. (2017) 'What is regulation? An interdisciplinary concept analysis', *Regulation and Governance*, 11(1). doi: 10.1111/rego.12094.

Madni, A. M. and Boehm, B. (2017) *Disciplinary Convergence in Systems Engineering Research*, *Disciplinary Convergence in Systems Engineering Research*. doi: 10.1007/978-3-319-62217-0.

McCarthy, D. R. (2018) 'Privatizing political authority: Cybersecurity, public-private partnerships, and the reproduction of liberal political order', *Politics and Governance*, 6(2). doi: 10.17645/pag.v6i2.1335.

National Cyber Security Centre (2018) *NIS Guidance Collection*.

NCSC (2019a) *NCSC CAF Guidance NIS introduction*. Available at: https://www.ncsc.gov.uk/collection/caf/nis-introduction (Accessed: 1 May 2020).

NCSC (2019b) 'The Cyber Assessment Framework (CAF)'.

Rebovich, G. (2005) ‘Enterprise Systems Engineering Theory and Practice’, *Enterprise Systems Engineering Theory and Practice*, pp. 2–1. doi: 10.1002/9780470403501.ch7.

Swarz, R. S. and DeRosa, J. K. (2006) ‘A Framework for Enterprise Systems Engineering Processes’, pp. 1–10.

Wallis, T. (2019) *Interviews with industry*.

Wallis, T. (2020) *Interviews with industry*.

Wallis, T. and Johnson, C. (2020) ‘Implementing the NIS Directive, driving cybersecurity improvements for Essential Services’, in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*.

White, B. and Rebovich, G. (2011) *Enterprise Systems Engineering: Advances in the Theory and Practice*. Taylor & Francis Group.