Chapter 1.3 Modelling the Extended Enterprise
Neil Allan, Elliot Varnell, Louise Gravina, Jake Storey, Christos Ellinas

Introduction

As we will read later in this report, the Extended Enterprise (EE) has often been developed in order to make more efficient use of resources (i.e. cut costs) or to extend the capabilities of the core enterprise beyond just direct suppliers and customers. However, as we will also read, the EE will often result in increased risk exposure for the core enterprise.

This can be partially explained by the nature of the increasingly interdependent world we occupy, along with the heightened number and diversity of stakeholders involved in the vast majority of modern enterprises. As a result, emergent issues and cascading failures, defined by far-reaching impact within the EE are increasingly becoming the rule rather than the exception, challenging our capacity to effectively and efficiently manage the 21\textsuperscript{st} century organisation (Cantle et. al. 2013).

Functional interactions and relationships (or, connections) between stakeholders can be physical or social. In this report you will read a great deal about the social relationships – and read about some of the physical relationships too. Sometimes these relationships are overt (e.g. through the supply of manufacturing components), but sometimes they are opaque (e.g. through networks of social relationships).

Either way, they are essential to the operation of the EE which is enabled and driven by them. Technically, the EE can be described as a set of separate systems that have been coupled at various interfaces to produce intra (i.e. within a system) and inter (i.e. between self-contained systems) dependencies which can provide increased functionality – indeed create a whole greater than the sum of its parts. This, usually large, number of dependencies, along with their asymmetric distribution is a universal characteristic of complexity (see Test 1, Chapter 2) of both natural and man-made systems – the EE being an example of the latter.

When a system is complex, it can achieve increased efficiency and performance, along with increased capacity to adapt to its external environment. Alas, such systems are also increasingly sensitive to instabilities (sometimes catastrophic) and are rather fragile when central elements are affected, leading to cascades of failure. Some examples of complex systems and recent failures that have resonated within them are:

- The fragile economy that can be tipped into a recession by relatively small perturbations;
- The power grid that collapses due to a single sub-station failure;
- Relatively minor technical failures that result in huge consequent disasters in a variety of levels, ranging from economic to environmental;

Such systems are not defined by the number of components that they are composed of (i.e. complicatedness) – their degree of technical intricacy effectively becomes irrelevant. Methods for dealing with large numbers of variables are well established (ex. any form of statistical inference) and risk mitigation against failure is fairly established (ex. introducing redundancies). Rather we are
facing a problem of interfaces and coupling – this is the domain of complexity where predictability and the path of causality only becomes evident *post-mortem*. Indeed, in a complex world, everything is obvious once it has happened (and assuming that your organisation has survived it).

Our argument in this chapter is that the EE can be effectively viewed through the lens of complex systems and as such, if we wish to be able to shield the EE, we will need to reach for modelling tools found within this domain. Complex network\(^1\) analysis will form the backbone of our approach, mainly due to its increased flexibility, and suitability in its inherent ethos – namely, focusing on the importance of interconnectivity rather than the discrete elements themselves. Other tools that are found within the domain of Complex Systems do exist - examples include: System Dynamics, Bayesian networks and Agent Based Modelling. The interested reader is referred to the extended technical reviews of Albert and Barabási (2002) and Newman (2009).

**A Network Toolset for Extended Enterprise Risk**

As a part of a network systems approach, it is necessary to decide where the boundary of the EE lies and what is worth including. The key here is to be explicit about which stakeholders are considered to be inside the EE, which are outside but need to be included in the analysis, and those which are outside the EE and are not going to be included in the analysis. Reasons for non-inclusion might be stakeholders that cannot be *controlled*, difficulty in obtaining meaningful data, importance or simply expediency. Remember that a model needs to be as simple as possible but not simpler.

Once all the relevant stakeholders are identified, we have the set of *nodes* that will form the basis of our model. The next step is to think about how they are connected – such will result in a network which is an effective abstraction (and thus, a *model*) which can allow further analysis and insight on the potential risks of that the EE may be exposed to. The following example is intended to illustrate the basic steps and parameters involved in mapping such network (a systematic process is also included in the form of a flow chart – see Figure 7), followed by typical insights that one may infer from such an approach. In a way, it paves a methodology on how suitable paradigms can be used to map a real problem into an abstract model, along with typical insight that can be gained by applying a set of analytical tools on such model.

We should note that the proposed methodology is purposefully described at a high-level in order to ensure generalizability and applicability to a range of practitioners, irrespective of the specifics of their own challenge. Nevertheless, it is strongly recommended that a more detailed analysis on a case-by-case scenario is further produced, building on the suggested approach, in order to maximise the relevance and utility of the insights.

---

\(^1\) Complex network analysis is a scientific field which is currently attracting a lot of attention as it can provide an analytical toolkit for the analysis of real-world systems. It has emerged by empirical observations across systems of different domains but of which similar patterns appear to unite them – systems ranging from the human brain, the economy, shipping routes and inter-organisational communications.
Example
Yam Yam Ltd. is a fictional enterprise which competes in the consumer retail market and its main income revolves around 3 core products – A, B and C. Typical of such an enterprise, it has a number of internal departments the Buying, Product Managers, Finance and Quality Assurance. A major competitor in the market also exists, producing product 1. Figure 1 illustrates a typical internal communication network – an information exchange process which enables the organisation to perform its function.

Outside this organisational core, one expects to find an underlying supply chain. Its fundamental purpose is to increase the value of raw material by converting it to a final product. Thus, its efficiency and robustness is critical for the profitability of the EE.

One might expect to encounter increased complexity within such systems as the EE attempts to increase the value obtained by this process along with conforming to changes in its operational environment (ex. new legislation introduced etc.) – usually in terms of increasing flexibility, adaptability, efficiency, robustness in order to attain a competitive advantage. Typically, such supply chains will be composed of a number of stakeholders at a variety of tiers and the nature of connections between them can be money flow, contractual obligations or material flow. In this example, we will focus only the *material flow aspects*, simply for the sake of clarity and generalizability.

The output of the process provided by the supply chain will then follow the distribution channels in order to reach the final customer. The intermediate stops between the outputs of the supply chain and the customer will vary depending on the context of the EE – typical composition of the distribution channels in retail will include depots, distribution centres and retail units. The rather simple supply chain and its underlying distribution system which mobilises Yam Yam Ltd. can be seen in Figure 2.
Figure 2: Typical distribution/supply chain system for Yam Yam Ltd. Within this context, the size of each node represents the output of each stakeholder in terms of value, the dotted lines represent a transient material (i.e. cannot be directly marketed to a customer, though can be exchanged at a suppliers level) while a solid line represents the flow of a marketed (i.e. final) product.

We can now inflict a more realistic notion on the operational aspect of the supply chain – effectively ask the question of what enables the supply chain to operate. One vital element is its interaction with the transportation system, as it is coupled to the interactions of the stakeholders within the supply chain i.e. the system that enables the suppliers to interact with each other – see Figure 3. Risk materialisation that can affect the transport system will inevitably resonate through the supply chain, as suppliers will not be able to interact as planned, hindering the function of the EE as a whole.

Using Figure 2, consider Supplier T (with a relatively small output) who is only able to transport its raw material to Supplier R by shipping. The port of which exportation takes place is highly dependent on the ability of the material to be transported there i.e. from the farm to the port, through the rail system. Thus, the ability of the supply chain to function (i.e. for stakeholder R to interact with T) is entirely dependent on the ability of the transportation system to function as expected. Notice how the inevitable dependence of the supply chain to the transportation system of a (potentially) foreign county has substantially altered the risk exposure of the EE. Political volatility in terms of future expansion of the transportation system, new legislation controlling its capacity, weather conditions of which the transportation system is exposed to, the degree and diligence that
maintenance works is applied etc. have now been added to the list of risks which can significantly impact the ability of the EE to function.

The materialisation of any such risks can, for example, hinder the ability of a supply chain stakeholder to utilise the usual route to export, upon which characteristic delivery times are calculated – for example consider the inability to use the Rail Stop A(a) due to signal failure – see Figure 3. Consequently, another route must now be chosen, which will inevitable cause delays and increased costs for both the stakeholders involved and, as a whole, the EE. As such, the capacity of the enterprise to undertake its function, as expressed through both business promises (i.e. contracts) and implied security (ex. insurance) has effectively been compromised simply because of interdependencies found between two coupled systems that have entirely different operational regimes (and inevitably, exert different risk management practices). The resilience of the EE is evidently as strong as its weakest (or more suitably, exposed) component.

![Diagram of Supply chain coupled to a transportation system](image)

**Figure 3**: Connection of the supply chain and the transportation system. The former can only be operated if the latter is functioning, however the risk exposure of the former is entirely different than from the latter. Such coupling can induce cascading failures which resonate within the EE on a much grander scale as one may initially anticipate.

It is now becoming evident that even the trivial example of Yam Yam Ltd. is evolving into a rather complex EE. Again, it is worth noting that this evident complexity has not been a product of increased number of components (i.e. scale) but rather an issue of interfaces. Arguably, being able to understand the shifts in terms of risk exposure as various interfaces are uncovered is of great importance for the understanding the real EE. Uncovering the key constituents of a complex situation is the first step in order to construct a much simpler model which we can fully understand and thus, model and predict certain aspects of the EE. In summary, let us first identify some key elements that have shaped its complexity profile by piecing the picture together – see Figure 4.
Figure 4: The Extended Enterprise Network of Yam Yam Ltd, within the context of four relevant aspects.

From right to left:

- **Yellow Boundary**: represents the core enterprise and some of its composing elements (for this specific example, viewed from an organisational point of view) and how the functionality of the core emerges by the interactions (in this case, mainly revolving around information exchange) between self-contained entities in the form of departments.

- **Purple Boundary**: The number of relevant stakeholders (and their respective interactions) is expanded by adopting a material flow view. Specifically, we now focus on suppliers and physical structures. From this perspective, the functionality of the core enterprise expands from mere management to the provision of tangible products, enabled by the interactions (in this case, material flow) of the aforementioned physical components.

- **Grey Boundary**: A further aspect which serves as a vital infrastructure of the interconnections within this layer to take place is also introduced – in this case we have used the example of a transportation system that enables the material flow to take place (in the case of the Yellow boundary, such enabling infrastructure could include computer networks that enable individual between and within the departments to communicate and exchange relevant information etc.). The transportation system, and its subsequent coupling to the material flow, is again another aspect which can influence the functionality of the entire
enterprise – failure in the function of the former will inevitably affect the capacity of the latter to perform one of its key business aspects; namely deliver physical goods per agreed conditions.

- Cyan Boundary: Lastly, the cyan layer introduces the peculiarities found within the operation environment of the EE – in this case two such systems include media and regulatory agents. To further elaborate, consider a wave of customers expressing their dissatisfaction on the condition of a product though social media. Such action is expected to be noticed by relevant regulatory boards and potentially initiate reforms that can substantially impact the capacity of the EE to operate profitably. Notice that at no point the EE has any direct influence (or control) on the aforementioned causal path.

The Extended Enterprise

The entirety of the systems included in Figure 4 share a fundamental aspect; they all have the power to meaningfully influence the capacity of the EE to function – thus, they play a significant role in the control structure that drives such enterprise. This observation will form the cornerstone of our approach towards defining, describing and understanding the EE network and its subsequent risk exposure. The following section will attempt to abstract the specifics of the introduced example in order to construct a generalizable methodology.

A generalised model for mapping the Extended Enterprise

Our aim in composing this chapter is to provide something that can help practitioners with their decision making under their unique situation, in terms of the aforementioned EE network. In order to do so, it is necessary to first describe the EE in terms of its behaviour, form, viability and purpose. Additionally, it is important to identify the environment within which the EE is operating, as the latter can be shaped by domain-specific forces and exposures – the operational environment. Furthermore, in order to consider what enables the EE to perform its function, one needs to closely examine its resource environment. Figure 5 illustrates the relationships between these concepts on an abstract level in order to help their identification.

In relation to Yam Yam Ltd. the resource environment is effectively the supply chain (Figure 4, Purple Boundary); enabled by the transportation system while the operational environment is where the regulatory agents and media influence (Figure 4, Cyan Boundary) come in play. Finally, Yam Yam Ltd. can be defined by understanding its form (i.e. e. internal organisation structure – Figure 4, Yellow Boundary), its viability (e.g. capacity to reduce its exposure by leveraging other agents such as suppliers, insurance etc.), and its purpose (e.g. long-term growth) and its behaviour (e.g. ethics and culture).

Figure 5: Generic Enterprise Model – adapted from (Hitchins, 2008)
Identifying stakeholders
As soon as the boundary of the EE is determined, key entities (i.e. stakeholders) that can influence its function need to be mapped. In order to do so, an appropriate property needs to be selected in order to filter out irrelevant stakeholders or agents. In this case we are interested in the ability to exert control on the EE – see Figure 6. Note that this aspect further enables to answer Test 3, as introduced in Chapter 2.

Stakeholders found within the inflow directly exert (meaningful) influence on the enterprise but cannot be influenced by the latter (in terms of the Yam Yam Ltd example, Figure 4, Grey Boundary contains agents of this sort). Similarly, agents found in the outflow are those who are being directly influenced by the enterprise but cannot directly reciprocate. Importantly, some stakeholders do not interact with the enterprise itself but can have a substantial, indirect, influence upon it, as they can influence the reciprocity capacity of the agents found in the outflow without the ability of the enterprise to effectively act against it – such stakeholders are found within the tendrils of the system. With reference to the Yam Yam Ltd. example, such agents can be found in Figure 4, Cyan Boundary. Finally, notice that this approach can further accommodate for the influence of external factors such as externally coupled systems.

Defining the interactions
The next step is to shift the focus from the single, discrete stakeholders to the nature of their interactions. This might include factors such as information exchange, material flow, regulatory agreements, money flows, social interactions and even organisational hierarchy. Alternatively it might be just domain expertise that determines the connections – see Figure 7 below for a complete process that can aid in transcribing a real situation to an analytical network model.

Figure 7: Process flow for creating an Extended Enterprise network.
Once information about the nature of the interactions is collected a network is created upon which we can perform analysis and simulations. This network can then enable detailed scenario testing, for example, to stress-test the enterprise on both internal but also external shocks that may materialise due to its exposure in fast-evolving, dynamic environments and complex connections. Such models can further provide useful insights on how local failures (e.g. a number of elements under-perform or become non-functioning) can influence the performance of the entire EE. Consequently, key stakeholder (or in more general terms, nodes) in the network can be identified to ensure that these have extra levels of security or risk mitigation measures in order to ensure the likelihood of local tipping points controlling the operation of the EE is minimised.

Before being able to explore these questions, the required level of aggregation for doing the analysis needs to be decided. This aspect can be ideally driven by the question, but in reality, other elements such as the nature of the data itself and the need for expedience can influence this decision.

Complex Networks Analysis

Complex networks is a scientific field which is currently attracting a lot of attention as it can provide an analytical toolkit for the exploration and modelling of real-world, complex systems – see Barabási (2007) for a brief overview. Generally speaking, it is possible to analyse any such network at two distinct levels of detail – at a local or global level.

Local Level
A significant part of complex networks analysis revolves around the identification of central nodes (and thus, can be considered to be of a local level) in an attempt to identify drivers that can dictate the dynamics of the entire network. A variety of different approaches exists within the field, though they can be roughly categorised thematically in terms of the individual node; the distance between the nodes (closeness); the ability of a node to control some sort of flow within the network (betweenness) and the importance of a nodes’ neighbours. They can be briefly described as follows:

- **General centrality** – how well connected a node is i.e. number of in/out coming connections;
  - Such nodes will most likely be the most visible node in the network as it will be connected (and thus visible) to a greater number of nodes. Such examples may include highly connected individuals in a social network, well-connected manufacturers within a sparse industry, major financial institutions within the economy etc.
- **Closeness centrality** – how easily a node can reach any other node i.e. how close it is to its neighbours in terms of hops;
  - A node is central in terms of its distance to other nodes; a node with great distance can be interpreted to have greater autonomy. A typical example is the emergence of important cargo airports acting as distribution points with minimum distance between export and import points (such as Hong Kong International Airport, sitting between China, a major export source, and Europe, a major import point) – this is partly due to their high closeness centrality within the considered network (i.e. available airports)
- **Betweenness centrality** – how important a node is in terms of connecting other nodes;
  - This measure can be interpreted as a measure of control upon something that flows through a network. High node betweenness can often result in bottle-necks which can be of great importance in keeping a network flowing. Reflecting back on Figure 2, the Depot can be intuitively identified as a bottleneck (and thus, possesses high
betweenness) as if one were to remove it, the network would immediately become disconnected and material flow from tier 1 suppliers to distribution centres would have been restricted.

- Neighbour’s characteristics – how important, central or influential a node’s neighbours are; effectively representing the idea that “you are as important as the people you know”.  
  - This idea is typically used by internet search engines and builds on the idea that a node is as important as its neighbours’ are. In terms of supply chains, one may consider a stakeholder who provides a single (i.e. very low connectivity) but much bigger stakeholder with a relatively low-value material. Nevertheless, if this material does not flow from the former to the latter, the impact will be great as the big stakeholder will not be able to perform its function. Under this perspective, the relatively low output, low degree node can be considered to be of great importance.

**Global Level**

One may also wish to characterise networks in order to allow global comparison between other networks to compare the inherent robustness of the EE. Such global measures include:

- Network Distribution – the mapping of how connections are distributed amongst nodes.
  - Such measure can indicate whether the network is homogeneous (i.e. every node has more or less the same number of connections) or heterogeneous (i.e. every node has very few connections with occasional super-connected nodes). The implications can be of great importance as the effect of local failures on the overall system are qualitatively different – see Figure 8.
- Network Density – the ratio between the connections found within the system and the theoretical maximum that the network can accommodate for.
  - A network in which all nodes are connected with all other nodes will have a density of one. Highly connected networks may imply that individual connections are not so important, but may also imply, that such EE is highly sensitive to any kind of perturbation.

**Network complexity** is related to **network density and network distribution** in two ways, based on the assumption that increasingly convoluted network structures demand higher operational resources.

1. Network density is conceptually linked with network complexity because a denser network requires more effort to build and maintain.
2. Network distribution implies higher coordination costs as highly connected nodes will require much more effort to coordinate.

**Modelling**

Understanding and adequately mapping such network characteristics can contribute to understanding a number of peculiar features of complex systems. For example, the “Robust-Yet-Fragile” nature observed in a number of systems such as the Internet,  

![Figure 8: Typical behaviour of a complex system under node failure. Evidently, complex systems are relatively robust to random failures but extremely vulnerable to targeted (i.e. central node) failures. This behaviour is fundamental for such systems and is encapsulated via the term “Robust-yet-Fragile”.

Page | 10
the power grid etc. can be attributed to their underlying degree distribution (Doyle et al., 2005).
Under specific configurations, random failures have little impact while failure of “central” nodes can have disproportionate effects on the overall performance of the system, assuming of course that the latter is dependent on its inherent connectivity ex. a transport network is enabled by its mere ability to connect nodes with links. Supply chains are typically described by similarly heterogeneous distributions, and thus, can be expected to behave in a similar fashion.

However, a note of caution should be made here as the majority of suitable methods that can be used (including System Dynamics, Bayesian Networks and Agent Based Modelling) are sensitive to the initial parameters and thus, carefully tailored models should be constructed. A number of exogenous factors should also be considered and introduced within any such model – such factors may include inflation and interest rates, product demand, labour, resource and energy costs etc.

Using the process entailed in Figure 7, we have illustrated how this general methodology can be applied to the simple (in terms of scale) but surpassingly complex (in terms of interfaces) example of Yam Yam Ltd. As such, we have identified both key nodes (i.e. suppliers, organisational departments etc.) that need to be acknowledged within the model, along with their assigned interactions. Notice that only one kind of interaction will be considered (i.e. material flow) as the aim of this example is to illustrate a methodology and a set of tools rather than present an elaborate analysis with limited transferability, and thus, usability to a practitioner. The analysis will exemplify some of the key metrics mentioned in the previous sections, along with typical interpretations that may be applied. Nevertheless, the importance of a detailed analysis on a case-by-case approach in order to deliver truly applicable and relevant understanding cannot be overstated.

Network analysis using Yam Yam Ltd.

Node Betweenness

Figure 9: Node Betweenness Analysis results. Note that results are normalised – the darker the hue, the higher the value.
Node betweenness allocates centrality on nodes depending on their ability to control a flow of material throughout the network. This sort of information, used in conjunction with knowledge of the system, can provide meaningful insights into the possible risks to the EE based on the network interactions. Within the context of Yam Yam Ltd., and using the quantitative results captured in Figure 9, the following observations and deductions can be made:

- The Finance department within the organisation, along with the Depot found within the distribution network, are clearly highly central to the EE as they control the majority of flow in terms of information within the organisation, and material within the distribution network respectively.

- Consider the control of a supplier upon the final output of a product (i.e. the Depot’s output). Supplier R has a higher centrality score when compared to other second tier suppliers. Specifically, in order for Supplier Q to provide the final product, Supplier R must enable the flow of material originating from supplier T; this is not the case in term of Supplier S for example. Thus, Supplier R may not be the most connected (and thus most visible) entity within the supply chain but can potentially create a cascade of failures as it sits within a critical position of the network.

- In the case of a potential contamination within the network, the betweenness metric allows us to identify which parts of the extended enterprise are more exposed by highlighting the weak links. For example, one can identify Supplier U having an increased capacity for spreading a contaminant within the network as it is able to control a higher number of flows when compared to any other supplier – notice that this is not as obvious as one would expect since it contains exactly the same number of incoming connections. Similarly, one can signify the Depot as being the single most prominent entity as it essentially connects the two clusters by enabling all processed material to reach customers – thus highlighting their capacity to enable cascades within such a system.

**Node Degree**
Figure 10: In-Degree Analysis (number of incoming connections to a node). Note that results are normalised – the darker the hue, the higher the value.

Degree analysis, as previously mentioned, refers to the number of connections a node has. Clearly this can be approached from two perspective; mapping either the in-degree (i.e. incoming connections, see Figure 10) and/or the out-degree (i.e. outgoing connections, see Figure 11). Such measures can have a number of useful interpretations, though one needs to be explicit on the nature of the connections to make operational sense and draw risk related conclusions. A number of simple but interesting interpretations about Yam Yam Ltd. can then be made from degree analysis when we use information flow as the context of the connections.

Firstly, the finance department within Yam Yam Ltd. has is defined by a high in-degree centrality. This makes sense as it probably deals with a heavy flow of information from buyer exchanges and such analysis might highlight the potential to generate risks that can incur from mishandling information. Also, it will be most sensitive to perturbations in other parts of the organisation downstream. Thus, it would imply that an increased attention should be given to managing and mitigating such lapses in information flow, particularly as it is also highly ranked in terms of between-ness (see Figure 9).

However, once the out-degree perspective is introduced, (Figure 11) both the Finance and Quality Assurance control become equally important. One might ask why finance and Quality Assurance are not more closely connected and maybe this is an area of possible risk mitigation. Remember this is only a simple simulation and in practice of course both departments may communicate with each other and also have a much broader set of inward and outward communication.

Figure 11: Out-Degree Analysis (number of outgoing connections from a node). Note that results are normalised – the darker the hue, the higher the value.

It is also worth noting that in Figure 10; Supplier Q has a higher number of incoming connections than the other suppliers but a lower number of outward connections as shown in Figure 11. This is interesting as it places Supplier Q in a very important position to influence the supply to the Depot and it is also a central pin in its own mini network. This is also confirmed by its between-ness ranking in Figure 8. Any failure by Supplier Q would disproportionately impact distribution and supply to the stores. Common sense of course in the simple Yam Yam Ltd. example but the point being that this is...
backed up by analysis which can be applied to large networks. By overlying different networks and different metrics, a clear picture of key nodes and key relationships becomes apparent, this provides for an invaluable risk management tool.

The observations in this simple case study are quite trivial and somewhat obvious, but the power of this technique is to highlight risky areas in the network when they are much larger and opaque to any one person in the EE. By making explicit the connections and their interactions it is possible to reduce the complexity of the EE, and help risk managers spot higher risk elements across disciplines and stakeholder groups. It can also be used as a useful scenario testing model by taking out certain nodes or connections.

Summary

The purpose of this chapter was to introduce a methodology to abstract the Extended Enterprise (EE) into a tangible model which can then be analysed and used to aid decision making, from a risk perspective.

A simple example was first introduced in the form of a fictional origination, Yam Yam Ltd., which was slowly built-up from simple obvious set of connections to a more complex EE with multiple interdependent connections. It illustrates the importance of interactions and how they can alter the risk exposure profile of an EE and subsequently how the function can be influenced. A generalised model was introduced (Figure 5 & 6), along with a mapping process (Figure 7); in order to illustrate how the process can be applied to any situation or EE. The analysis can provide meaningful and usable insight into potential risks, as presented in the final section of the chapter.

Take away points

- Modern organisation are striving to achieve more with less by coupling a number of their activities to external systems; for the purpose of this Chapter, this is the essence of the EE.

- Complex networks are a powerful modelling framework that has been successfully applied in a range of complex systems, from the human brain to the economy. As EEs are becoming increasingly similar to such systems (due to the inter/intra connections), this framework can serve as a great step in improving our capacity to manage, control and protect the EE.

This Chapter has laid down a process flow in which a set of tools has been introduced in order to aid a practitioner in mapping the EE as a complex network. A fictional example was used in order to enable reflection between theory and application, a sense on the data that may be needed and finally, an interpretation on the analysis results.

References


