Soft Systems Methodology in Net-Centric Cyber Defence System Development

Richard Craig
Faculty of Engineering
University of Bristol
Bristol, United Kingdom
richard.craig@bristol.ac.uk

Theodoros Spyridopoulos
Faculty of Engineering
University of Bristol
Bristol, United Kingdom
th.spyridopoulos@bristol.ac.uk

Theo Tryfonas
Faculty of Engineering
University of Bristol
Bristol, United Kingdom
t.tryfonas@bristol.ac.uk

John May
Faculty of Engineering
University of Bristol
Bristol, United Kingdom
j.may@bristol.ac.uk

***Abstract*—Complexity is ever increasing within our information environment and organisations, as interdependent dynamic relationships within sociotechnical systems result in high variety and uncertainty from a lack of information or control. A net-centric approach is a strategy to improve information value, to enable stakeholders to extend their reach to additional data sources, share Situational Awareness (SA), synchronise effort and optimise resource use to deliver maximum (or proportionate) effect in support of goals.**

This paper takes a systems perspective to understand the dynamics within a net-centric information system. This paper presents the first stages of the Soft Systems Methodology (SSM), to develop a conceptual model of the human activity system and develop a system dynamics model to represent system behaviour, that will inform future research into a net-centric approach with information security.

Our model supports the net-centric hypothesis that participation within an information sharing community extends information reach, improves organisation SA allowing proactive action to mitigate vulnerabilities and reduce overall risk within the community. The system dynamics model provides organisations with tools to better understand the value of a net-centric approach, a framework to determine their own maturity and evaluate strategic relationships with collaborative communities.

***Index Terms*—Command and Control, Net-Centric, Situational Awareness, System Dynamics, Distributed Information Systems**

I. Introduction

One of the implications of our Information Age, has been to transfer significant economic value away from natural resources and physical labour, to where substantial sources of economic wealth are now generated by information, and effective communication; predicted by some to "become the dominant force in defining and shaping human actions, interactions, activities, and institutions" [1]. Information is a key organisations asset which supports decisions, achieves strategic goals and benefits through its effective and innovative use. This concept has driven a global market that has removed many barriers to technical interoperability, providing opportunities for collaborative effort and information sharing. With greater openness, interconnection and dependency comes greater vulnerability as the consequences of information system failure becomes severe. The scale and sophistication of security threats have grown and frequently outpace traditional security tools. Organisations have to guard against a more focused adversary with the resources and capabilities to target highly sensitive information, often through persistent campaigns. Nations understand the extent to which their critical infrastructures are dependent upon cyberspace and cyber attacks remain one of the top four threats to UK national security alongside international terrorism [2]. The existing *reactive* approach to cyberspace means it is impossible to take evasive action or even predict the next threat. Having identified and prioritised cyber dependencies, appropriate resilience measures and contingencies can be put in place, and enabled through the provision of sufficient cyber situational awareness to ensure timely response.

To better secure the cyber domain and the emerging cyber dependencies, governments are encouraging multi-organisation collaborations to create information infrastructures between public and private sectors [2]. A net-centric approach refers to a dynamic ecosystem where interconnecting people and systems (independent of time or location), improves situational awareness and shortens decision cycles; that along with inter-organisational collaboration and information sharing, will generate shared situational awareness and enable self-synchronisation that will result in increased whole system performance, effectiveness of action and use of resources [3]. While a theoretical definition of a 'net-centric approach' is lacking and its interpretation mainly depends upon context or perspective, the expected benefits can be intuitively accepted [4], but will remain out of reach until human-centric aspects are addressed [5]. This has placed a burden on Command and Control (C2) systems, that broadly include the activities of acquiring, managing, sharing and exploiting information, to support decision making [3]. The intent is to improve agility through collaborative forms of organised behaviour to translate an information advantage into a competitive advantage through well informed synchronised actors, understanding at the same time their existence within a responsive ecosystem and the systemic effect of actions. Without a holistic, efficient information infrastructure supporting a net-centric capability, the ability for a whole system response to take a proactive posture to threats or put in place effective mitigation and resilience measures is severely reduced, leading to even greater vulnerability.

The remainder of this paper will introduce the SSM methodology and problem expression (section II), a system dynamic model is then realised with results (section III), before conclusions are presented in section IV.

II. Soft Systems Methodology (SSM)

Information systems address sociotechnical problems that cross the boundary between human activity systems and engineering artefacts that often involve many interested parties with different perspectives (world views), where ill defined issues cause difficulty in agreeing objectives (success requires stakeholder consensus). Soft Systems Methodology (SSM) is an action-oriented process of inquiry in which stakeholders formulate a solution strategy from a systemic understanding of the problem situation, and take action to improve it [9]. SSM has had considerable success as a problem structuring methodology and has been applied to learning systems [10], and information system design [11]. SSM addresses unstructured ('soft') problematic situations where there may be little consensus among stakeholders (even about the actual problem). SSM aims at accommodating different perspectives through conceptual models of human activity systems. These models are then used to decide on interventions for the resolution, or improvement, of the situation.

SSM focuses on the development of a conceptual model (a view of what could exist) with the aim to express stakeholder mental models of the problem and gain consensus on objectives and issues. A problem may even disappear as the result of stakeholder consensus on a number of key issues. A concept model does not describe what exists but is modeling a *view* of what exists within a human activity system. When models are used in the design of information systems intended to support physical processes, a comparison between the models and the physical world is required. During SSM analysis, a 'soft' problem will be expressed to provide a perspective that can be considered a 'hard' problem to be solved by a variety of traditional methods. Checkland argues that SSM could be used to address systems engineering problems, as the ability of SSM to address 'soft' problems is akin to Operation Research which solves structured 'hard' problems [10]. SSM can be an iterative process to drive continuous improvement [7] .

Traditional SSM is broken down into seven stages: 1) Entering the unstructured problem domain, 2) Expressing a structured problem situation, 3) Formulating root definitions of relevant systems, 4) Building conceptual models of human activity systems, 5) Comparing the models with the real world, 6) Defining changes that are desirable and feasible, and 7) Taking action to improve the real world situation. This paper considers the first four stages to express the problem situation, develop a conceptual model and understand the behaviour of a net-centric information system.

A. Unstructured Problem Domain

Framing the problem situation, understanding the organisational context (and culture), and identifying actors is the first stage in SSM. A rich picture is an unstructured way of capturing information, and communication within a human activity system. Figure 1 provides a visual representation of the following description of the problem domain.

There is currently a gap in the ability to gain sufficient Situational Awareness (SA) of the cyber domain that will

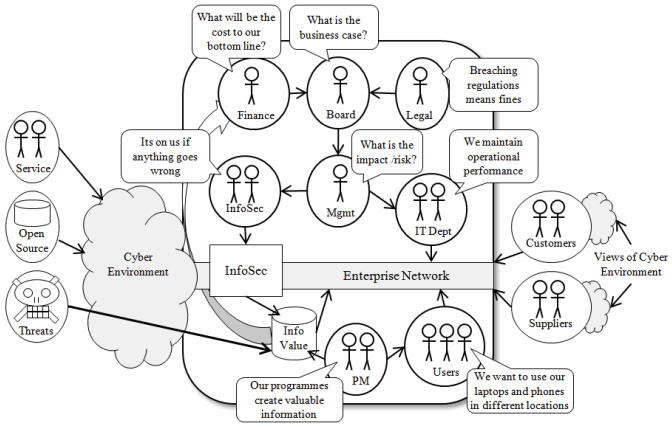

Figure 1. A rich picture of the information security human activity system within an organisation

enable a proactive response to the mitigate vulnerabilities within enterprise information systems and better defend against malicious activity. Many decisions have a dependency on cyberspace and an established SA picture provides the underpinning confidence to carry out activities. Organisations need an approach for sustaining SA of their own, and interdependent systems, platforms and infrastructures to support decision-making and improve . A range of information security products and services are available, along with open source intelligence, but these options are limited in scope and do not have the variety to address threats within the wider cyber environment.The information security boundary could move outwards to included other organisations, within a wider perspective of the near, mid and far boundaries of cyberspace. The majority of defensive activity is still focused on the 'near space' (within organisation boundaries), as information silos exist within organisations at all levels. An organisation may have customers and suppliers that interact with their enterprise network, providing an opportunity to extend the reach for security information to the 'mid space' and engage with existing stakeholders to improve SA and provide an early warning of events, enabling proactive action and improving whole system resilience.

B. Problem Expression

The second stage in SSM examines the relationships within and between structure and processes. People, process and technology form the activity system of an organisation, that are dynamically entangled, rather than self-contained entities with discrete interactions. Deming states that "If you can't describe what you are doing as a process, you don't know what you are doing!", therefore the process of a net-centric approach should be captured within a model [7]. The stated benefits of a net-centric approach would be more robust and secure networks, through improved information sharing and situational awareness, to better inform decision makers, for improved or proactive action, that can deliver synchronised and proportionate effect towards objectives.

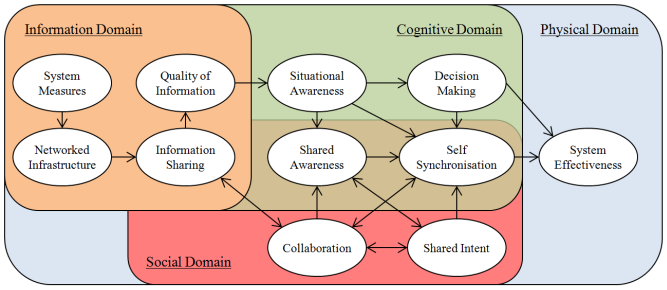

Figure 2. A Net-Centric Value Chain Model. Adapted from "NATO NEC C2 Maturity Model," by Dr. David S. Alberts, 2010, DoD Command and Control Research Program, Washington, D.C. Adapted with permission.

To realise the competitive advantage of a net-centric approach, Alberts (2010) describes a value chain model that identifies required processes [3], that we have adapted to capture the flow from measures to system effectiveness (Figure 2). These processes are located across four domains: physical, information, cognitive, and social domains. The physical domain is where activity is conducted across land, sea, air, and space environments, and where effective action is realised. The information domain is where information is created, processed and communicated. The cognitive domain resides within the mind of human actors and holds their perceptions, awareness, understanding, decisions, and beliefs. The social domain represents cooperative relationships where entities interact, share information, awareness, understandings and making collaborative decisions. In the value model, the social domain overlaps the information and cognitive domains through shared processes, but remains distinct; Comprehending situational awareness (SA) within the context of shared situational awareness (SSA), to enable self-synchronisation from enhanced awareness or collaboration, can be considered a socio-cognitive process (detailed in section III).

C. Root Definitions

A root definition of a system (relevant to the problem) is a clear statement of purpose, that identifies the stakeholders, processes and value of the system-in-focus. Two systems are identified from the problem descriptions: 1) a system to develop Situational Awareness (SA) within an organisation boundary to support information security activity, and 2) a system to extend the information reach of the organisation through participation within a community of interest and access to Shared Situational Awareness (SSA). A CATWOES analysis of the root system(s) identifies the Customer (who are system beneficiaries), Actors (who transform inputs to outputs), Suppliers (who provide input resources) and Owner (who has the power of veto), the Transformation process (purpose of the system), World view and Environmental constraints are expressed (Table I). A definition of each system is given;

1) System A: Organisational Awareness (Node) : A system owned by the Chief Information Officer (Owner) of an organisation, where analysts (Actors) process information from local and external sources, to develop SA of the enterprise network

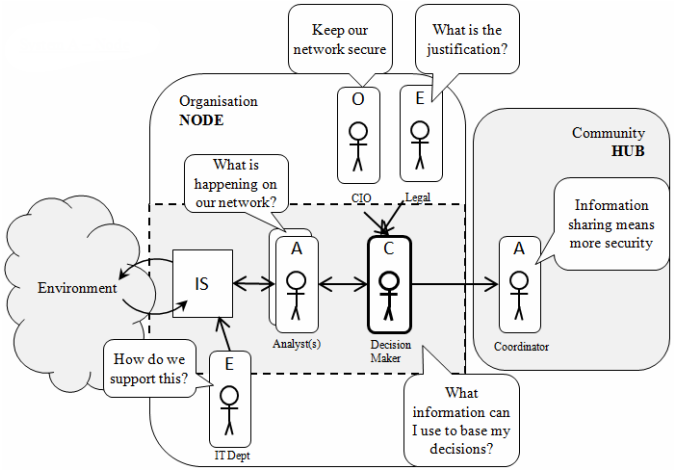

Figure 3. System A: Activity within an organisation to gain SA

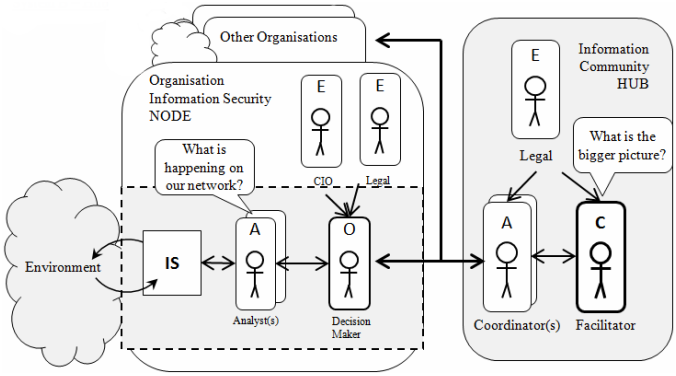

Figure 4. System B: Collaboration for shared awareness

and wider cyber domain dependencies, for the decision maker (Customer) to take action to prevent malicious activity, reduce risk and secure information assets (Figure 3). The IT and Legal departments are environmental actors who can influence the activity system, but do not participate (regularly).

2) System B: Collaborative Community (Hub): A system owned by the Decision Maker (System A) within each organisation, who decides to share information to the Hub Coordinators (Actors) who combine information from group members to provide the Hub Facilitator (Customer) with an understanding of the 'bigger picture' through enhaced SA of cyber domain activity. The added value from this shared awareness is returned to stakeholders to improve their SA and enable proactive action (Figure 4).

III. System Dynamics Model

Through a system dynamics model, we examine the concept of a net-centric approach to the problem of generating Situational Awareness (SA), and the value of participation within an information sharing community to access new information from Shared Situational Awareness (SSA) and minimise cyber security risks. The problem expression and root definitions from section II identified two systems that: leverage the information system within an organisation to generate SA

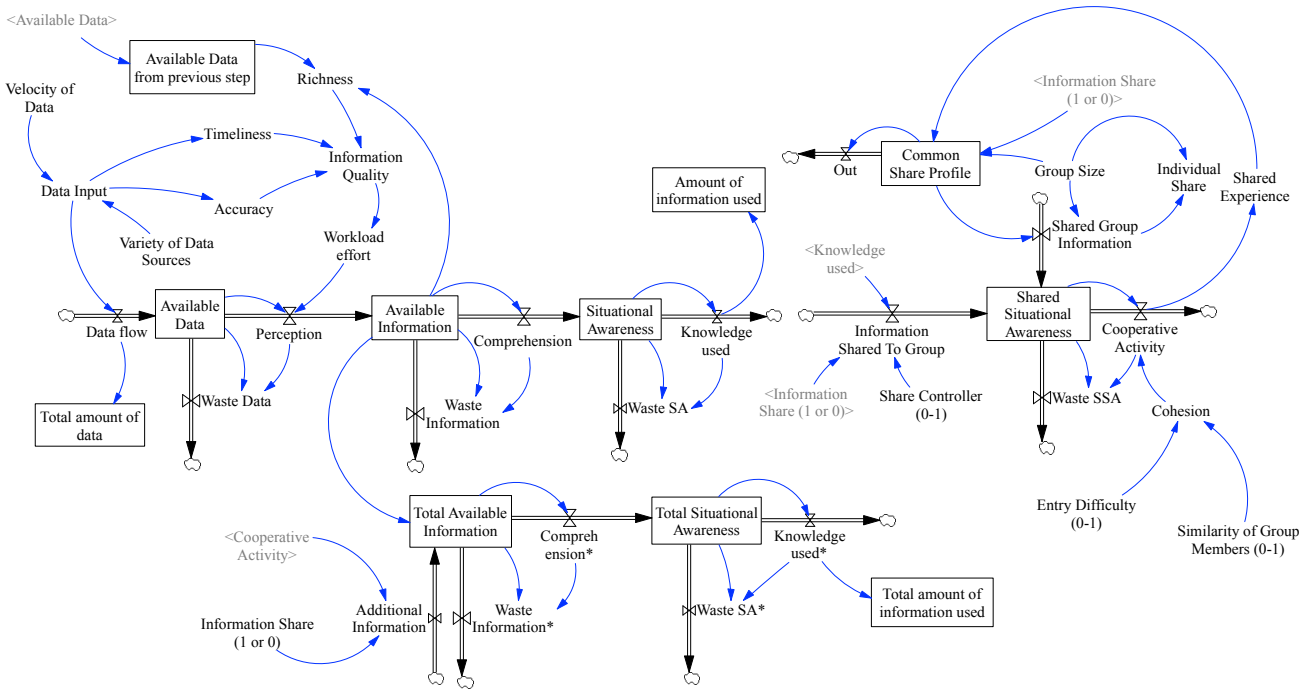

Figure 5. Improving SA within an organisation (System A) through collaboration with an information sharing community (System B)

CATWOES	System A (Node)	System B (Hub)
Customer	Decision Maker	Facilitator
Actors	Analysts, Coordinator	Analysts, Coordinator
Transformation	Analyse network information to develop organisation Situational Awareness (SA) perspective	Combine different SA perspectives into Shared Situational Awareness (SSA) across the community
World view	To better secure enterprise networks, improved SA is required	Information sharing improves SA and enables proactive action
Owner	Chief Information Officer	Decision Maker (Node)
Environment	IT Dept., Legal	CIO, IT Dept., Legal
Supplier	Information System	Organisations

Table I
CATWOES ANALYSIS OF THE TWO ROOT SYSTEMS

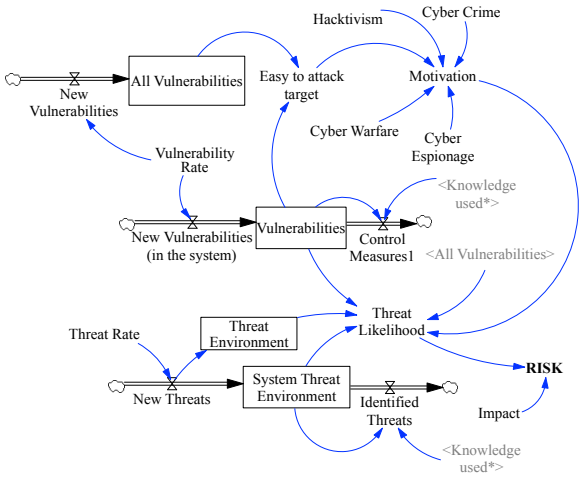

Figure 6. Risk evaluation system dynamics model.

of the cyber domain (System A), and information sharing activity within a community to create additional value through SSA (System B). An additional system that describes the risk evaluation process based on the NIST recommendations [13] demonstrates the effect of collaboration on the cyber security risk levels. The whole system represents how a net-centric approach can improve SA within an organisation and minimise risks.

As we consider System A, the output from an organisation's information system provides the initial input to our model. The quantity of information available, measured in information packets, is the output from processing 'Big Data', and the product of the variety of data sources, that produce a volume of information at some velocity. Endsley (2000) describes SA as knowing what is going on, that is of importance to people who need to achieve the goals and decision tasks for that job; While the nature of SA will vary between tasks, the mechanisms used for achieving SA can be described generally as perception, comprehension and projection [12]. As information is made available to an analyst at a given manageable work rate, their ability to comprehend value depends upon the quality of the information measured in the dimensions of timeliness, accuracy and richness. Timely information allows for a number

of cognitive cycles, before a decision must be made and a course of action taken. Accurate information is authoritative, trusted, valid, and truthful. Rich information is comprehensive, drawn from a number of sources and perspectives. The trade off between these variables for sufficient information quality is task-specific.

Awareness is generated from the comprehension of high quality information, at a manageable work rate to allow the analyst to perceive important information required to support their decision tasks. The aim is to generate awareness of sufficient quality to be of value to the decision maker. An extension of System A captures the knowledge from the cooperative activity between the members of the information sharing group and integrates it to the system's available information in order to improve SA.

System B represents the information sharing community, where members cooperate with a central 'Hub' organisation to gain enhanced SA, and share additional information with the group. Each member of the group may decide whether to share information, but there there will be an expected value proposition that will encourage participation. Initially, a member may share only small amounts of information from their own SA perspective as they may have limited trust or confidence in the group. As members share information, and see the returned value of participation, a common profile of collaboration within the group provides a measure of the additional information contributing to the SSA. An increase in shared information from each member, increases the shared experience, pushing upwards the common share profile of the group which in turn urges each member to increase its sharing activity, since more sharing results in higher shared situational awareness. However, in case some members share much less than others, the resulted common share profile urges the other members to decrease their sharing as well in order to keep a balance between the members, resulting to the decrease of the shared situational awareness.

SSA is a product of the total information shared, therefore the larger community, the greater the amount of information they share. By sharing more information, each member encourages the others to do the same enhancing collaboration and building a strong group share profile. On the other hand poor collaboration results in poor SSA levels. Cohesion represents the alignment, or shared intent of the community towards collaboration and shared goals; while the average amount of information shared within the group increases, the size of the group becomes a limiting factor. Thus, a strict difficult to enter group with members with similar goals and expectations has an increased cohesion compared to a huge group of members with high diversity. As System B performance improves, more value is created within SSA as members share more information, that is then returned to System A and contributes towards improved SA.

The risk evaluation system, depicted in Figure 6, communicates with system A and evaluates the risk level based on the threat and vulnerabilities environment and the control measures that the decision maker will take. Risk is the product of the likelihood of a threat to successfully exploit one or more vulnerabilities and the potential impact to the organisation. In general the impact, as well as the risks, may be financial, reputational, organisational, health and safety etc. For simplicity, in our model we use a general term of impact that incorporates all the aforementioned types and represents the severity of a successful cyber attack. The likelihood of a successful attack depends on the threat landscape, the vulnerabilities of the system and the attacker's motivation. As a second level of control on the system, the decision maker has the ability to patch the system's vulnerabilities based on the gained knowledge built through situational awareness. The more vulnerabilities are patched the more decreases the likelihood of a successful attack, leading to the conclusion that increased SA decreases security risks. The motivation of the attacker can vary being political, ethical or personal interest. In most cases cyber attacks are a result of hacktivism, cyber crime, cyber crime, cyber espionage or cyber warfare. In particular the probability of a cyber crime that includes personal interest is increased when the target is open to many vulnerabilities and thus easy to attack. Therefore, knowledge gained from SA has an impact on the motivation of a cyber attack. Improved SA from the act of sharing information, therefore has a great influence on the cyber security risk levels.

A. Results

For the purposes of our research, we ran several simulations using open source data to define the threat and vulnerability environment, and the different types of cyber attack motivation [14], [15]. The results of our simulation support the net-centric hypothesis that participation within an information sharing community improves the organisations own SA (Figure 7); the more information shared to a community Hub, the greater the value of information returned, improving decision making capabilities from increased SA.

If an organisation joins an information sharing group, but does not share that much compared to the other members, the shared situational awareness of the group gradually drops as shown in Figure 8 since the common share profile of the group forces the other members of the group to decrease the amount of information they share in order to keep a balance between the members. However, the more information an organisation shares the higher gets the shared situational awareness. This reveals the power that the group 'Hub' draws from its members, leading to the conclusion that the more information one shares, the better for the system as a whole.

Figure 9 depicts how the cyber security risk level is affected by the sharing act of an organisation. In general we see that when an organisation enters a sharing group and exchanges information the cyber security risk level decreases significantly. Furthermore, the more information they share the more and faster decreases the risk level; the decision cycle is improved by the additional information from the SSA. This confirms our thinking that sharing information can positively influence the risk level of the organisation.

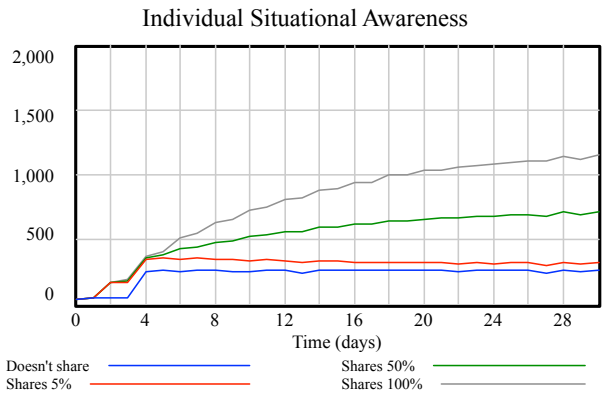

Figure 7. Individual Situational Awareness with and without sharing.

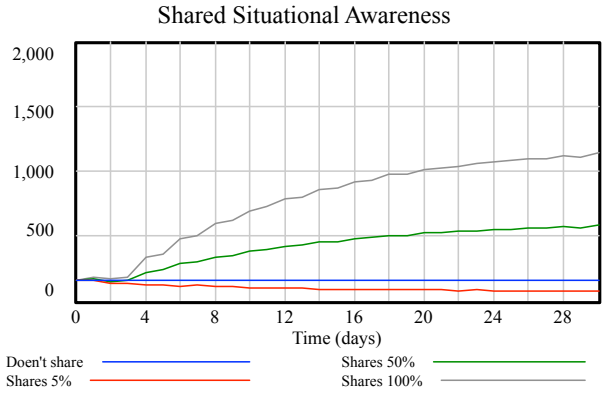

Figure 8. Shared Situational Awareness with and without sharing.

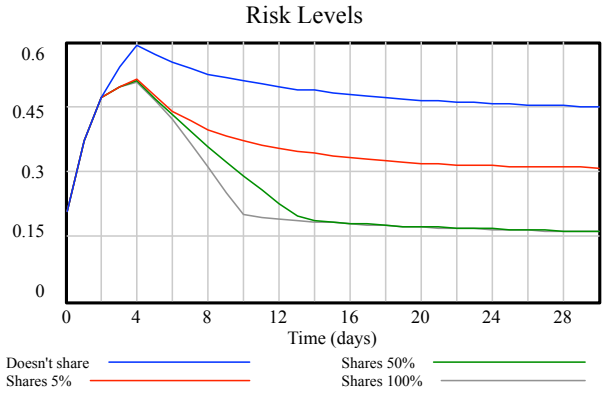

Figure 9. Risk evaluation with and without sharing.

IV. Conclusions

This paper presents a net-centric systems approach towards improving information security within an organisation, by improving Situational Awareness (SA) through collaboration with an information sharing community. Soft Systems Methodology (SSM) is used to interpret the root systems of the information security problem, and processes for developing SA, which are then realised through a system dynamics model to understand the behaviour of the human activity system and identify potential measures of performance. Results from the system dynamics model confirms the net-centric hypothesis that increased information sharing within a community, will lead to improved situational awareness within organisations, as a result of the increased information reach and additional value contribution from the group. Sharing even small amounts of information, such as 5% of existing SA, to a trusted community can return enough value to reduce risk levels. This methodology and the system dynamics model provide organisations with tools to better understand the value of a net-centric approach, a framework to determine their own situational awareness maturity and evaluate strategic relationships with collaborative communities.

Acknowledgment

This work has been supported in part by the EPSRC-funded Industrial Doctorate Centre in Systems (Grant EP/G037353/1) and Boeing Defence UK Ltd.

References

[1] Alberts, David S., and Daniel S. Papp. The information age: an anthology on its impact and consequences. Office of the Assistant Secretary of Defense Washington dc Command and Control Research Program (CCRP), 1997.

[2] The Cabinet Office, "The UK Cyber Security Strategy protecting and promoting the UK in a digital world",London: HMSO, 2011.

[3] Alberts, David S., Reiner K. Huber, and James Moffat. NATO NEC C2 maturity model. Office of the Assistant Secretary of Defense Washington DC Command and Control Research Program (CCRP), 2010.

[4] Neaga, Elena Irina, and Michael Henshaw. "A stakeholder-based analysis of the benefits of network enabled capability." Defense & Security Analysis 27, no. 2 (2011), pp. 119-134.

[5] Bolia, Robert S., Michael A. Vidulich, and W. Todd Nelson. Unintended consequences of the network-centric decision making model: Considering the human operator. Air Force Research Lab Wright-Patterson AFB OH Human Effectiveness Directorate, 2006.

[6] DoD, C. I. O. "DoD net-centric data strategy." US Department of Defense Chief Information Officer (May 2003) (2003).

[7] Deming, W.E. (1986), Out of the Crisis, Cambridge University Press, Cambridge.

[8] Alderson, D. and Doyle, J. "Contrasting Views of Complexity and Their Implications For Network-Centric Infrastructures", IEEE Transactions on Systems, man, and Cybernetics—Part a: Systems and Humans, vol. 40, no. 4, July 2010

[9] Checkland, Peter. "Soft systems methodology." In Encyclopedia of Operations Research and Management Science, pp. 1430-1436. Springer US, 2013.

[10] Checkland, P., and J. Scholes. "Soft Systems Methodology in Action: Including a 30 Year Retrospective." Journal-Operational Research Society, 51, no. 5 (2000): 648-648.

[11] Curtis, Graham, and David Cobham. Business information systems: Analysis, design and practice. Pearson Education, 2008.

[12] Endsley, M. R. "Theoretical underpinnings of situation awareness: A critical review". Situation awareness analysis and measurement, pp. 3-32, 2000.

[13] Stoneburner, Gary and Goguen, Alice and Feringa, Alexis "Risk management guide for information technology systems". Nist special publication, vol. 800, no. 30, 2002

[14] Symantec Corporation "Internet Security Threat Report for 2013", Annual Threat Report, vol. 19, April 2014

[15] Cruz, Benjamin and Greve, Paula and Kay, Barbara and Li, Haifei and McLean, Doug and Paget, Francois and Schmugar, Craig and Simon, Rich and Sommer, Dan and Sun, Bing and Walter, James and Wosotowsky, Adam and Xu, Chong "McAfee Labs Threats Report Fourth Quarter", Quarterly Threat Report, 2014