

Literature Review of Scientific Articles about Cyber Information Sharing

J Simola

*Laurea University of Applied Sciences
RDI Espoo, Finland
University of Jyväskylä, Finland*

Email: jussi.hm.simola@jyu.fi

Abstract: *This literature review presents a review of cyber information sharing based on systematic queries in four scientific databases. Hundreds of articles were handled and clustered. Relevant publications concerning cyber information sharing are succinctly described in the paper. The findings are discussed from the perspective of how to develop a cybersecurity information sharing system and what possible features might be included in the system. The literature review will comprise a new database for the Echo Early Warning System (E-EWS) concept. E-EWS aims at delivering a security operations support tool, enabling the members of the ECHO network to coordinate and share information in near real-time.*

Keywords: *CIP, Cyber-Ecosystem, Emergency Response, E-EWS, Cyber Information Sharing*

Introduction

This research belongs to the European network of Cybersecurity centres and competence Hub for innovation and Operations project (ECHO), which is part of the Horizon2020 program. The ECHO consortium consists of several partners from different fields and sectors including: health, transport, manufacturing, ICT, education, research, telecom, energy, space, healthcare, defence, and civil protection. The main objective of the ECHO is to strengthen the proactive cyber defence of the European Union. The literature review aims to gather essential scientific articles and official materials about cyber information sharing models. The literature review is based on systematic queries in different kinds of databases, such as IRIS. The findings will be discussed from the perspective of the added value that the review will offer to the stakeholders. The literature review will comprise a new database for the Echo Early Warning System (E-EWS) concept. E-EWS aims at delivering a security operation support tool, enabling the members of the ECHO network to coordinate and share information in near real-time. Within the E-EWS, partners of ECHO can retain their fully independent management of cyber-sensitive information and related data management. The early warning system will work as a parallel part of other mechanisms in the Public Protection and Disaster Relief environment. The development of the E-EWS will be rooted in a comprehensive review of information sharing and trust models from within the cyber domain. The literature review will present occasional scientific literature and official materials concerning information sharing between partners and stakeholders.

How to share sensitive data between stakeholders? What kind of information sharing-solutions already exist? The literature review is going to answer these questions as well.

Background

Modern infrastructures include not only physical components but also hardware and software. These integrated systems are examples of Cyber-Physical Systems (CPS) that integrate computing and communication capabilities with monitoring and control of entities in the physical world. In CPS, embedded computers and networks monitor and control the physical processes. Cyber-Physical Systems enable next-generation ‘smart systems’, such as advanced robotics, computer-controlled processes, and real-time integrated systems (Lee & Seshia 2015; Hevner & Chatterjee 2010).

There are separate cyber threat functions at the national and EU levels. Lack of synergy and separated functionalities concerning artificial intelligence solutions produce more potential vulnerabilities for vital functions. Therefore, it is important to develop functionalities in the ecosystem and to gather relevant data for the next generation’s early warning solutions.

The content of the literature review is divided as follows. After the introduction, the next section handles shared situational awareness and cybersecurity information sharing. ‘Base for the Research’ covers methodologies used and the literature review process of the research. The next section discusses the overview of the findings. The last section presents conclusions.

Shared Situational Awareness and Cybersecurity Information Sharing

This section covers the notions of ‘shared cyber situational awareness’ and ‘cybersecurity information sharing’. It aims to provide a theoretical framework and to limit the area of the literature study. It defines what to share, how to share, and with whom to share cybersecurity information. Shared (cyber) situational awareness is closely related to (cybersecurity) information exchange, because, without trusted information sharing, common situation or situational awareness is insufficient. The importance of this common situational awareness can be seen in a variety of areas. For example, public safety actors such as European law enforcement agencies need a common shared situational picture for the cross-boarding of tasks so that operational cooperation is based on a reliable platform.

According to Endsley and Robertson (2000a), good team situational awareness is dependent on team members understanding the meaning of the shared information. This means that teams need to share pertinent data and a higher level of situational awareness (Endsley & Robertson 2000a, 2000b). Bolstad and Endsley (2000) write that the development of shared situational awareness consists of four factors: 1) shared SA requirements (team members’ ability to understand which information is needed by other team members); 2) shared SA devices (communications); 3) shared SA mechanisms (shared mental models); and 4) shared SA processes (effective team processes for sharing relevant information) (Bolstad & Endsley 2000). According to Munk (2018), cooperation between cybersecurity organisations is based on the effective and efficient exchange of information. Information interoperability is the joint capability of different actors—such as persons, organisations, and groups—necessary to ensure the exchange and common understanding of the information needed for their success (Munk 2018).

The Basis for the Research

In case of a hybrid incident, how can response and procedures be improved? Humans are not as good as automation at quickly and consistently processing large volumes of data. Flexible auton-

omy should provide a smooth, simple, seamless transition of functions between humans and the system (Endsley 1988). The target audience covers the ECHO partners, including several research organisations, large enterprises, industrial actors, and EU agencies across the countries. Clearly, a common platform for creating common cyber situational awareness is needed.

The fundamental needs concerning information sharing among ECHO partners are the basis for this research. The research question of the literature review is ‘What are the main features of cyber exchange models?’. Collected materials are based on scientific literature, research articles, and official publications. The following scientific databases have been used: database of the JYKDOK library at the University of Jyväskylä (wide database concerning cybersecurity that provides access to resources such as the IEEE Xplore); the IEEE Xplore library (provides web access to more than 4.5 million documents from publications in computer science and to about 200 journals and about 1700 conference proceedings); Springer link (a database area of engineering that contains 17,000 books); and AI—a tool called IRIS, which is a search engine based on 100 entered keywords. The qualitative analysis was made by using traditional half-manual processing and Glue (Orange3) Python to explore the collected databases.

Search queries

In each case, the search queries such as ‘cybersecurity information sharing’ were entered, with no temporal limitation. A query without quotation marks returns some variations where the search engine allows for permutations and inflections. The so-called Artificial Intelligence tool IRIS returns wider variations, but the search engine works well. The author had to use quotations in some queries because some combinations made the searches too comprehensive.

As an initial screening, titles and abstracts have been read and the number of clusters has been identified. The selected list of groups can be regarded as a universal description of the research area. There were four main tasks of the research:

- Identify existing early warning systems and frameworks within public safety organisations;
- Identify information sharing models and governance models in private and public safety organisations;
- Identify features of cyber exchange model—for example, best practices and defensive measures;
- Classify phenomena, such as events, incidents, vulnerabilities, threats, and others.

Following the initial analysis method, a review form is an iteratively relevant aspect of the research. The aim is to cover the most relevant aspects of cyber information sharing models. Classification areas were used after the initial screening (an independent classification apart from the title, authors, or other text fields). Selected areas are solution area of results, threats and types of cybersecurity-related information, proposals, models, artefacts, and experiments/technology.

As noted above, findings create the fundamental database for the E-EWS, which is based on the framework of CPS (Cyber-Physical System). ECHO EWS will deliver a secure sharing support tool for personnel to coordinate and to share information in near real-time. It will support information sharing across organisational boundaries, will provide the sharing of general cyber information as

a reference library, will ensure secure connection management from clients accessing the E-EWS, and will combine different kinds of functions required in the management of information sharing functions—including sector-specific cyber-sensitive data. Thus, it concerns the whole ecosystem.

The systematic literature review sources

After defining the search queries, the initial search in Springerlink returned 1612 results for ‘cybersecurity information sharing’ within content computer science, and it returned 31 researches with a quotation as **Table 1**, below, illustrates. Sharing technologies without the word ‘cybersecurity’ returned 517 results Features of cyber information sharing models without quotations returned 279 results.

Item Title	Authors	Publication Title	Year
Network Externalities in Cybersecurity Information Sharing Ecosystems	Z Rashid, U Noor, J Altmann	Economics of Grids, Clouds, Systems, and Services	2019
Risk Management Using Cyber-Threat Information Sharing and Cyber-Insurance	D Tosh, S Shetty, S Sengupta, JP Kesan, CA Kamhoua	Game Theory for Networks	2017
Using Incentives to Foster Security Information Sharing and Cooperation: A General Theory and Application to Critical Infrastructure Protection	A Mermoud, M Keupp, S Ghernaouti, D David,	Critical Information Infrastructures Security	2017
Three Layer Game Theoretic Decision Framework for Cyber-Investment and Cyber-Insurance	DK Tosh, I Vakiliinia, S Shetty, S Sengupta, CA Kamhoua, L Njilla, K Kwiat	Decision and Game Theory for Security	2017
Distributed, Collaborative, and Automated Cybersecurity Infrastructures for Cloud-Based Design and Manufacturing Systems	J Lane Thames	Cloud-Based Design and Manufacturing (CBDMD)	2014
Toward a Safer Tomorrow: Cybersecurity and Critical Infrastructure	S Karchefsky, R Rao	The Palgrave Handbook of Managing Continuous Business Transformation	2017
IoT: Privacy, Security, and Your Civil Rights	CD Mares	Women Securing the Future with TIPPSS for IoT	2019
Part 2: Legal and Regulatory Framework	RH Weber, D Staiger	Transatlantic Data Protection in Practice	2017
Cybersecurity in the U.S.: Major Trends and Challenges	B Fonseca, JD. Rosen	The New US Security Agenda	2017
Cyber Attacks, Prevention, and Countermeasures	N Lee	Counterterrorism and Cybersecurity	2015
Regulation of Cyberspace and Human Rights	K Kittichaisaree	Public International Law of Cyberspace	2017
Toward a Holistic Approach of Cybersecurity Capacity Building through an Innovative Transversal Sandwich Training	J El Melhem, A Bouras, Y Ouzrout	Industry Integrated Engineering and Computing Education	2019
Frameworks and Best Practices	B Keys, S Shapiro	Cyber Resilience of Systems and Networks	2019
Economic Valuation for Information Security Investment: A Systematic Literature Review	D Schatz, R Bashroush	Information Systems Frontiers	2017
Main Initiatives to Safeguard Cyberspace Sovereignty	B Fang	Cyberspace Sovereignty	2018
Transatlantic Cooperation in Cybersecurity: Converging on Security as Resilience?	G Christou	Cybersecurity in the European Union	2016
Learning Quasi-Identifiers for Privacy-Preserving Exchanges: A Rough Set Theory Approach	C Wafu SohL, L Njilla, KK. Kwiat, CA Kamhoua	Granular Computing	2018

Item Title	Authors	Publication Title	Year
IT-Security in Critical Infrastructures Experiences, Results, and Research Directions	U Lechner	Distributed Computing and Internet Technology	2019
Proposed Model for a Cybersecurity Centre of Innovation for South Africa	JJ van Vuuren, M Grobler, L Leenen, J Phahlamohlaka	ICT and Society	2014
Trends in Cyber Operations: An Introduction	F Lemieux	Current and Emerging Trends in Cyber Operations	2015
Cybersecurity in the U.S.	N Kshetri	The Quest to Cyber Superiority	2016
Sharing Cyber Threat Intelligence under the General Data Protection Regulation	A Albakri, E Boiten, R De Lemos	Privacy Technologies and Policy	2019
Vanishing Boundaries of Control: Implications for Security and Sovereignty of the Changing Nature and Global Expansion of Neoliberal Criminal Justice Provision	RP Weiss	The Private Sector and Criminal Justice	2018
International Cyberspace Governance	Chinese Academy of Cyberspace Studies	World Internet Development Report 2017	2019
The Role of Blockchain in Underpinning Mission Critical Infrastructure	H Jahankhani, S Kendzierskyj	Industry 4.0 and Engineering for a Sustainable Future	2019
Cyber Attacks, Prevention, and Countermeasures	N Lee	Counterterrorism and Cybersecurity	2013
Interpretation of the Concept of 'Cyberspace Sovereignty'	B Fang	Cyberspace Sovereignty	2018
Dark Web: Deterring Cybercrimes and Cyber-Attacks	FM De Sanctis	Technology-Enhanced Methods of Money Laundering	2019
Towards a Systematic View on Cybersecurity Ecology	W Mazurczyk, S Drobniak, S Moore	Combating Cybercrime and Cyberterrorism	2016
More than Humans	S Iaconesi, O Persico	Digital Urban Acupuncture	2017
Digital Security – Wie Unternehmen den Sicherheitsrisiken des digitalen Wandels trotzen	A Weise	Digitalisierung in Industrie-, Handels- und Dienstleistungsunternehmen	2018

Table 1: Relevant Springerlink research publications

IEEE Xplore returned 147 results by using the following words: cybersecurity, information, and sharing altogether. Access was obtained to 129 files of data: Conferences (82), Journals (28), Magazines (16), Courses (15), Early Access Articles (3), and Books (2). Fifteen inessential IEEE Xplore courses were removed from the results, including results for Web Server & Web Application Security, Footprinting, and Network. Features of cyber exchange models returned 29 results. Information sharing returned 36 results and both 'cyber information sharing' and 'cyber information exchange' returned 5 results in which one was the same, as **Table 2** illustrates.

Document Title	Authors	Publication Title	Year
'Cybersecurity information sharing'			
A System Architecture of Cybersecurity Information Exchange with Privacy (CYBEX-P)	F Sadique, K Bakhshaliyev, J Springer, S Sengupta	2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)	2019
Privacy-Preserving Cybersecurity Information Exchange Mechanism	I Vakulinia; DK Tosh, S Sengupta	2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)	2017

Document Title	Authors	Publication Title	Year
A Coalitional Game Theory Approach for Cybersecurity Information Sharing	I Vakiliinia, S Sengupta	MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)	2017
An Evolutionary Game-Theoretic Framework for Cyber-Threat Information Sharing	D Tosh, S Sengupta, C Kamhoua, K Kwiat, A Martin	2015 IEEE International Conference on Communications (ICC)	2015
Developing a Cyber Threat Intelligence Sharing Platform for South African Organisations	M Mutemwa, J Mtsweni, N Mkhonto	2017 Conference on Information Communication Technology and Society (ICTAS)	2017
'Cybersecurity information exchange'			
3-Way Game Model for Privacy-Preserving Cybersecurity Information Exchange Framework	I Vakiliinia, DK Tosh, S Sengupta	MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)	2017
Attribute Based Sharing in Cybersecurity Information Exchange Framework	I Vakiliinia, DK Tosh, S Sengupta	2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)	2017
Privacy-Preserving Cybersecurity Information Exchange Mechanism	I Vakiliinia, DK Tosh, S Sengupta	2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)	2017
Structured Cybersecurity Information Exchange for Streamlining Incident Response Operations	T Takahashi, D Miyamoto	NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium	2016
A System Architecture of Cybersecurity Information Exchange with Privacy (CYBEX-P)	F Sadique, K Bakhshaliyev, J Springer, S Sengupta	2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)	2019

Table 2: Specified IEEE returns

JYKDOC returned 9 results by using the following words: cybersecurity, information, and sharing together. Access was obtained to 9 files of data. Separate words cyber, exchange, and models returned 22 results. The term 'information sharing technologies' returned 268 results.

The AI tool IRIS requires the title of the research question and problem statement. The author has used the following words to describe the problem: "The research question of the literature review is 'What are the main features of cyber exchange models?' in order to capture a reasonably full range of the literature concerning the main features of cyber exchange models". Therefore, it was necessary to identify information sharing models and features of cyber exchange models. Early warning solution will deliver a secure sharing support tool for personnel to coordinate and to share information in near real-time, will support information sharing across organisational boundaries, will provide the sharing of general cyber information as a reference library, and will ensure secure connection management from clients accessing the early-warning system. The AI tool IRIS returned 270 results by using the following words in the title: cybersecurity, information, and sharing altogether, as **Figure 1** illustrates. The system calculates the relevance percentage for the results. All the results were between 78% and 95% relevant.

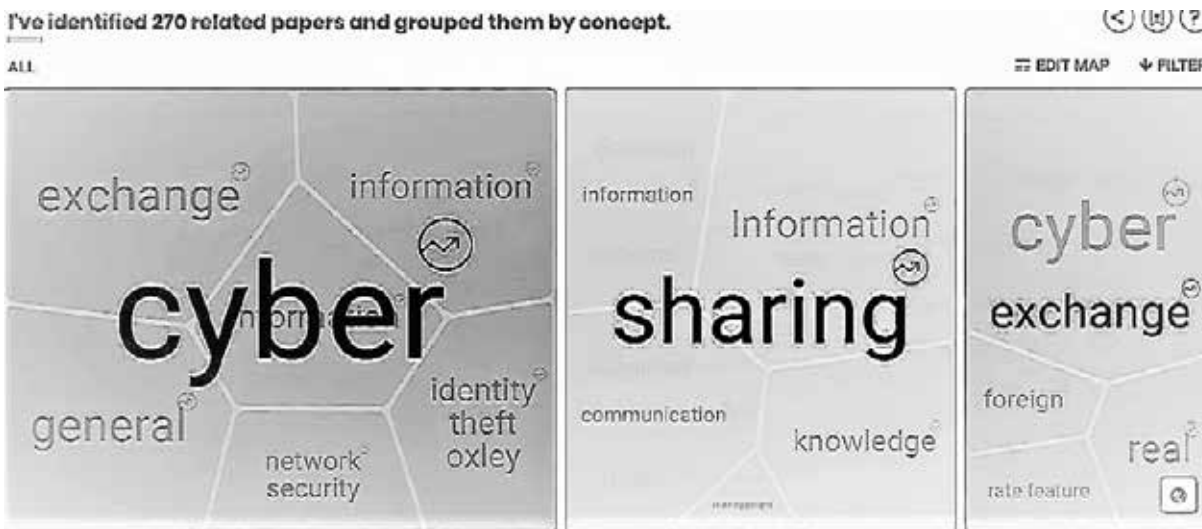


Figure 1: Identified papers by AI tool IRIS

Several studies were based on fundamental level public-related sources, which formed the main frame of the research. The most relevant public-related documents in this research are the following:

- Department of Homeland Security 2013, ‘NIPP 2013: Partnering for critical infrastructure security and resilience’, DHS, U.S.
- MITRE 2018, “Trusted Automated eXchange of Indicator Information — TAXII™ Enabling Cyber Threat Information Exchange”.
- National Institute of Standards and Technology NIST 2016, *Guide to cyber threat information sharing, Special publication 800-150*, Tech. rep., Gaithersburg, MD, U.S.
- Johnson C, Badger M, Waltermire D, Snyder J, & Skorupka C, *Guide to cyber threat information sharing, Special publication 800-150*, Tech. rep. NIST, Gaithersburg, MD, US.
- OASIS Cyber Threat Intelligence (CTI) TC, DHS (CS&C) 2017, *TAXII™ version 2.0. committee specification 01, OASIS Open*, Tech. rep. taxii-v2.0-cs01.
- OASIS Cyber Threat Intelligence (CTI) TC, DHS (CS&C) 2017, *STIX™ version 2.0. part 2: STIX objects, OASIS open*, Tech. rep. stix-v2.0-wd03-part2-stix-objects.

As the results summarise, the information-sharing related models and frameworks are widely used among public safety organisations.

Findings

Cybersecurity information sharing architectures, frameworks, and models

There are few existing cybersecurity information sharing architectures and frameworks for the warning systems within public organisations divided into main groups. As the figure below illustrates, Mitre (2018) categorises information sharing models into three main models. The fourth model comprises a combination of the others.

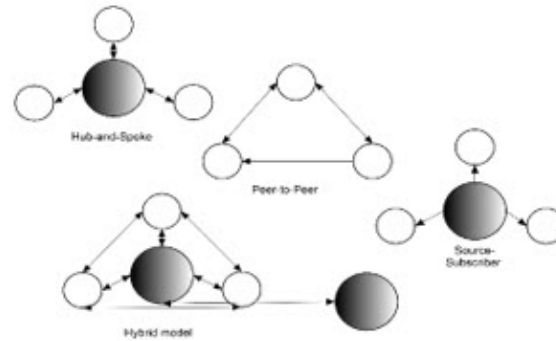


Figure 2 Traditional classification of information sharing models

- **Hub-and-Spoke:** Several data producers and consumers share information with each other; but instead of sending information directly, the information is sent to a central hub, which then handles dissemination to all the other spokes as appropriate. This model can be viewed as similar to email distribution lists, by which a sender provides a message to a mailing list service, which then forwards the message on to all list members.
- **Peer-to-Peer:** A group of data producers and data consumers organises direct relationships with each other. Members share directly with each other in a mesh pattern. The group may have a single governing policy, but all sharing exchanges are between individuals.
- **Source-Subscriber:** A single entity publishes information out to a group of consumers. This is a common model in commercial environments, where the data source is a vendor and the subscribers purchase access to the vendor's information. This is also a common model for free alerts from some authoritative source (Mitre 2018).

Despite the classification, many models are based on a hybrid structure. According to Sedenberg and Dempsey (2018), information sharing models can be divided into seven categories: government-centric; government-prompted—industry-centric; corporate—initiated-peer based (at the organisational level); small, highly vetted, individual-based groups; open-source sharing platforms; proprietary products; and commercialised services. Procedures and elements differ marginally from each other.

Government-centric is a centralised model, where one central organisation may share the information exchange or perform processing to enrich the data to others (NIST 2016; Meilin, Devine & Zhuang 2017). The Department of Homeland Security is one kind of hierarchical government-centric organisation. The central infrastructures use open, standard data formats and transport protocol (Meilin, Devine & Zhuang 2017).

Sector-Based Information Sharing and Analysis Centres (ISACs) are one kind of government-prompted, industry-centric sharing model. Centres are non-profit, member-driven organisations formed by critical infrastructure owners and operators to share information between government and industry. ISACs work through the National Infrastructure Protection Plan (NIPP) (Department of Homeland Security 2013). The National Cybersecurity and Communications Integration Centre (NCCIC) works in close coordination with all of the ISACs via the National Council of ISACs (NCI). They serve as collection and analysis points for private sector entities to share data on a peer-to-peer basis, to feed information into the federal government, and to provide a channel for federal information to flow out to the private sector. The purpose of Information Sharing and Analysis Organisations (ISAOs) is to gather, analyse, and disseminate cyber threat

information; but unlike ISACs, ISAOs are not sector-affiliated, and they are for any sector or community. ISAOs do not need to be part of the 16 critical infrastructures.

Corporate-initiated, peer-based groups are privately sponsored cybersecurity information sharing entities. These companies have undertaken their initiative without government intervention to coordinate information sharing. These information exchanges can be tailored to fit the specific needs of their members (Sedenberg & Dempsey 2018).

Individual-based groups are small online communities of peers that share sensitive information with the goal of immediate combat attacks. This kind of group requires a high degree of trust (Sedenberg & Dempsey 2018).

Open communities and platforms are open-source sharing platforms. For example, STIX indicators and open source intelligence feeds are examples of this kind of format. The Malware Information Sharing Platform (MISP) is a free, open-source platform developed by researchers from the Computer Incident Response Center of Luxemburg, the Belgian military, and NATO.

According to Sedenberg & Dempsey (2018), proprietary products and commercialised services consist of, for example, antivirus software and firewalls that disseminate cybersecurity information through software updates. Companies offering these products and services may participate in any of the other information exchanges to enhance the security of the small companies.

Features of Cyber-Threat Information Exchange Models

Automated Indicator Sharing (AIS) participants connect to a Department of Homeland Security-managed system in the Department's National Cybersecurity and Communications Integration Center (NCCIC) that allows bidirectional sharing of cyber threat indicators. A server housed at each stakeholder's location allows each to exchange indicators with the NCCIC. Participants receive and can share DHS-developed indicators they have observed in their network defence efforts, which DHS will then share back out to all AIS participants (Department of Homeland Security 2015a).

Stakeholders who share indicators through AIS will not be identified as the source of those indicators to other participants unless they affirmatively consent to the disclosure of their identities. Senders are anonymous unless they want DHS to share them (Department of Homeland Security 2015a). Indicators are not validated by DHS, as the emphasis is on velocity and volume: their partners tell the DHS they will vet the indicators they receive through AIS. The Department's goal is to share as many indicators as possible as quickly as possible (Department of Homeland Security 2015a). The U.S. Government also needs useful information about indicators (Department of Homeland Security 2015b).

AIS utilises the Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) specifications for machine-to-machine communication (Department of Homeland Security 2015a). STIX is a language and serialisation format that enables organisations to exchange Cyber Threat Intelligence (CTI) in a consistent and machine-readable manner (Oasis 2017a). Trusted Automated eXchange of Intelligence Information (TAXII™) is an application layer protocol used to exchange Cyber Threat Intelligence (CTI) over the HTTPS (Oasis 2017b).

OASIS defines several STIX Domain Objects. 1. Attack Pattern is a type of Tactics, Techniques, and Procedures (TTP) that describes ways threat actors attempt to compromise targets. 2. The campaign is a grouping of adversarial behaviours that describes a set of malicious activities or attacks that occur over time against a specific set of targets. 3. A course of action is an action taken to either prevent an attack or to respond to an attack. 4. Identities mean individuals, organisations, or groups, as well as classes of individuals, organisations, or groups. 5. The indicator means a pattern that can be used to detect suspicious or malicious cyber activity. 6. Intrusion Set is a grouped set of adversarial behaviours and resources with common properties believed to have been organised by a single entity. 7. Malware is a type of TTP (also malicious code and malicious software) used to compromise the confidentiality, integrity, or availability of a victim’s data or system. 8. Observed Data means conveyed information observed on a system or network (for example, an IP address). 9. The report consists of collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including contextual details. 10. Threat actors are individuals, groups, or organisations believed to be operating with malicious purpose. 11. The tools are software that threat actors can use to perform attacks. 12. A vulnerability is a software-based error that a hacker can directly use to gain access to a system or network (Oasis 2017a).

Cybersecurity information sharing governance and mechanisms

As **Figure 3**, below, represents, collection-based communications describe the situation when a single TAXII client requests a TAXII server and the TAXII server carries out that request with information from a database. A TAXII channel in TAXII server enables TAXII clients to exchange information with other TAXII clients in a publish-subscribe model. TAXII clients can push messages to channels and can subscribe to channels to receive published messages. A TAXII server may host multiple channels per API root (Oasis 2017b). TAXII is the main transport mechanism for cyber threat information represented in STIX. Stakeholders may share indicators with DHS through an ISAC or an ISAO without TAXII client.

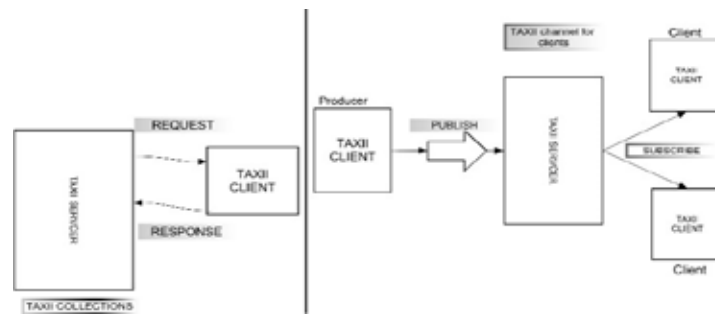


Figure 3: Flow of cyber threat information in TAXII

According to NIST (2016), cyber threat information is any information that may help an organisation identify, assess, monitor, and respond to cyber threats. Threat information is any information related to a threat that might help an organisation protect itself against a threat or detect the activities of an actor. Major types of threat information include the following:

- Indicators are technical artifacts or observables. Indicators can be used to detect and defend against threats. Indicators may consist of the Internet Protocol (IP) address of a suspected command and control server, a suspicious Domain Name System (DNS)

- domain name, a Uniform Resource Locator (URL) that references malicious content, a file hash for a malicious executable, or the subject line text of a malicious email message (NIST 2016).
- Tactics, Techniques, and Procedures (TTPs) describe the behaviour of an actor. TTPs could describe an actor's tendency to use a specific malware variant, order of operations, attack tool, a delivery mechanism (for example, phishing or watering hole attack), or exploit (NIST 2016).
 - Security alerts, also known as advisories, bulletins, and vulnerability notes, are brief and usually readable technical notifications regarding, for example, current vulnerabilities. Security alerts originate from sources such as the United States Computer Emergency Readiness Team (US-CERT), Information Sharing and Analysis Centres (ISACs), the National Vulnerability Database (NVD), Product Security Incident Response Teams (PSIRTs), commercial security service providers, and security researchers (NIST 2016).
 - Threat intelligence reports are generally prose documents that describe TTPs, actors, types of systems and targeted information, and other threat-related information that provide greater situational awareness to an organisation. Threat intelligence is threat information that has been aggregated, transformed, analysed, interpreted, or enriched to provide the necessary context for decision-making processes (NIST 2016).

Information sharing methodologies between Certs and Law Enforcement

Enhancing cooperation between EU member states and related Network and Information Security communities (NIS) as Certs is also a crucial part of the cyber-ecosystem. It is not enough that small, closed groups share information without synergy with public safety organisations.

The main goal of the Europol Information System (EIS) is to be the reference system for offenses, individuals involved, and other related data to support EU Member States, Europol, and its partners in their fight against organised cybercrime, terrorism, and other forms of serious crime. For example, the European Cybercrime Centre (EC3), as a part of Europol, uses an open-source MISIP platform (DG Home Affairs 2014). A Malware Information Sharing Platform (MISP) is a tool for information sharing about malware samples and malicious campaigns related to specific malware variants. It offers architectural flexibility, allowing the utilisation as a centralised platform (for example, CIRCL and FIRST instances), but also as a decentralised (peer-to-peer) platform (ENISA 2015). According to Europol (2019), there is a need to develop new information management architecture and to continue improving operational capabilities and tools by focusing on automation and modernisation, for example, to continue automating the direct follow-up processes through SIENA for successful (self-) searches on Europol's and EU member states' data. There is also a need to harmonise further the Technical Infrastructure Capability including Identity and Access Management (IAM) landscape of Europol by integrating more IT-systems with IAM and taking further steps towards establishing a single enterprise identity, taking into account various networks and security standards, including IAM for Basic Protection Level (BPL) business solutions (Europol 2019).

SIENA is a VPN (Virtual Private Network) designed to enable a swift, secure, and user-friendly exchange of operational and strategic crime-related information and intelligence between member states, Europol, law enforcement cooperation partners, and public safety organisations (DG Home

Affairs 2014). SIENA has been used to allow the EU member states to communicate and to share intelligence information.

In the U.S., National Information Exchange Model (NIEM) is an XML-based partnership mechanism between the U.S. Departments of Justice (DOJ) and Homeland Security (DHS) and enables information sharing focusing on information exchanged among organisations as part of their current or intended business practices (Criminal Intelligence Coordinating Council 2013).

The Federal Bureau of Investigation (FBI) hosted InfraGard's Secure Web Portal, which allows secure messaging that promotes communication among members. Members give access to iGuardian, the FBI's cyber incident reporting tool designed specifically for the private sector. InfraGard membership also allows peer-to-peer collaboration across InfraGard's broad membership and information-sharing and relationship-building with FBI and law enforcement. InfraGard engages subject matter experts and addresses threat issues across each of the 16 critical infrastructure sectors recognised by Presidential Policy Directive-21 (PPD), the Department of Homeland Security (DHS), and the National Infrastructure Protection Plan (NIPP) (Department of Homeland Security 2013).

Digital Forensics XML (DFXML) is an XML language (Garfinkel 2012) intended to represent the following kinds of forensic data: metadata describing the source disk image, file, or other input information; detailed information about the forensic tool that did the processing (for example, the program name and where the program was compiled and linked libraries); the state of the computer on which the processing was performed (for example, the name of the computer; the time that the program was run; the dynamic libraries that were used) (Garfinkel 2012); the evidence or information that was extracted (how it was extracted, and where it was physically located); cryptographic hash values of specific byte sequences; and operating-system-specific information which is useful for forensic analysis (Garfinkel 2012).

The Cybersecurity Information Exchange Framework (CYBEX) will advance the development of automating cybersecurity information exchange. The CYBEX Forensics domain is an operation domain that supports law enforcement operations by collecting evidence. The necessary information for this operation is stored in the evidence database. CYBEX provides a framework for exchange information between a network mediation point and a law enforcement facility to provide an array of different real-time network forensics associated with a designated incident or event (Rutkowski *et al.* 2010).

CYBEX-P and the Privacy-Preserving Cybersecurity Information Exchange mechanism are modified from CYBEX and both are based on an information-sharing platform with a robust operational and administration structure. The Privacy-Preserving Cybersecurity Information Exchange mechanism enables the organisations to share their cybersecurity information without revealing their identities (Vakilinia, Tosh & Sengupta 2017). CYBEX-P platform addresses the inefficiency in dealing with cybersecurity problems by an individual entity. Real-time exchange of threat data helps organisations analyse threats to predict and to prevent future cyberattacks. There are three parties involved throughout the complete lifecycle of the threat data: 1) Client organisation; 2) CYBEX-P; 3) analysts and researchers. The client organisation acts as a source of threat data. It can be

any external or internal threat data source willing to share threat data with others. CYBEX-P works as the intermediary between all organisations and data analysts. Threat data may be machine-generated or curated by a security specialist (Sadique *et al.* 2019). The processing server in CYBEX-P has a TPM Trusted Platform Module (TPM). The TPM verifies the integrity of the software and hardware running in the processing server (Sadique *et al.* 2019).

Making Security Measurable (MSM), led by MITRE categorises heterogeneous information and standardises data formats and exchange protocols (MITRE 2013). MSM presents a comprehensive architecture for cybersecurity measurement and management, where current standards are grouped into processes and mapped to the different knowledge fields. MSM standards can be grouped into six major knowledge areas, each of which refers to a process (put in parentheses): asset definition (inventory); configuration guidance (analysis); vulnerability alerts (analysis); threat alerts (analysis); risk/attack indicators (intrusion detection); and incident report (management) (MITRE 2013).

In many cases, a fundamental structure of the information-sharing mechanisms does not differ significantly. It is, therefore, suitable to continue on this issue in the conclusions.

Conclusion

This literature review indicates that ‘cybersecurity information sharing’ is not precisely defined in the area of cybersecurity. As mentioned above, the structures of information sharing models are generally very sector-specific and are created in different environments. There is a need at the EU level to determine the development of a common Early Warning Solution. Usually, the word ‘warning’ also refers to preventive functions, as U.S. intelligence services operate. The fight against hybrid threats means not only preventing cyberattacks but also identifying, tracing, and prosecuting a criminal/criminal group. This means an even deeper integration of government systems in the future.

Relevant information from the site of a major hybrid incident must be directly shared with the national participants—for example, cybersecurity centres. It is relevant to allocate additional reliable data for determining discrepancies of limits. Combining pieces of information to ensure the correct and reliable information to be shared is of primary importance. The essential information should be processed to the desired shape for the participants. In the future, cyber defence operations will be more integrated and automated according to local capabilities, authorities, and mission needs. The shared common operational picture means that real-time communication links from the local level to the national and EU level exist. A common cyber situational awareness is needed for operating CPS and emergency and crisis management. There should be a connection between cyber situational awareness functions and emergency management.

When developing an early warning system at the EU level, it is important to account for three requirements: 1) the possibility that some EU member states may leave an early warning system (Edgington 2020); 2) the need to engage participants in the values of the western world (Tidey, Gill & Parrock 2020); and 3) the possibility of combining some elements of the Cyber Threat Warning System to NATO Cyber Situational Awareness Solutions. These factors have a direct link to sharing confidential information (Simola 2019, Ilves *et al.* 2016).

It is important to consider how national Cyber Security Centres cooperate with other organisations within critical infrastructure at the national level. The state departments of the United States work closely together in the fight against threats in the field of cybersecurity. The organisations of public administration in the European Union work together more formally. This is important to notice when cybersecurity expertise is being strengthened. The fundamental problems of the European community must be solved before permanent solutions can be built. While this does not prevent the development of operating models, this factor must be taken into account when developing new systems. Confidence between member states must be on a stable basis.

As Ilves *et al.* (2016) mention, there are no crucial barriers to increase collaboration concerning, for example, early warning solutions between the U.S., NATO, and the EU. According to Dandurand & Serrano (2013), for example, Cyber Security Data Exchange and Collaboration Infrastructure (CDXI) provide a knowledge management tool for the NATO partners. The U.S. Cybersecurity Sharing Act and Europe's directive on Network and Information Security (NIS) have similar goals. In addition to this, the EU and NATO signed a technical arrangement in 2016 to increase information sharing between the NATO Computer Incident Response Capability (NCIRC) and the EU Computer Emergency Response Team (CERT-EU) (Ilves *et al.* 2016). Common E-EWS solutions would create an effective way to respond to cross-bordering hybrid threat situations. All major companies whose businesses are related to critical infrastructure should be linked to an early warning system.

Before closer cooperation on information sharing can be achieved, legislation, bilateral agreements, data management standards, and certifications need to be brought to an acceptable level of privacy. The holder of the information is the winner in the smart society. Protecting privacy is also part of the Western tradition, as is crime prevention.

References

Bolstad, C & Endsley, M 2000, 'The effect of task load and shared displays on team situation awareness', *14th Triennial Congress of the International Ergonomics Association and the 44th Annual Meeting of the Human Factors and Ergonomics Society*, Santa Monica, CA, US.

Criminal Intelligence Coordinating Council (CICC) 2013, *National criminal intelligence sharing plan; Building a national capability for effective criminal intelligence development and the nationwide sharing of intelligence and information*, Tech. rep. 2, CICC, US.

Dandurand, L & Serrano O 2013, *Towards improved cyber security information sharing requirements for a cyber security data exchange and collaboration infrastructure (CDXI)*, NATO CCD COE Publications, Tallinn, EE.

Department of Homeland Security (DHS) 2013, 'NIPP 2013: Partnering for critical infrastructure security and resilience', DHS, US.

———2015a, 'Automated Indicator Sharing (AIS)', viewed 1 July 2019 <<https://www.us-cert.gov/ais>>.

—2015b, *Automated Indicator Sharing (AIS) FAQ*, viewed April 2019, <https://www.uscert.gov/sites/default/files/ais_files/AIS_FAQ.pdf>.

DG Home Affairs 2014, *UINFC2 Project, Deliverable D.1.3: Law Enforcement Agents Requirements*, European Union.

Edgington, T 2020, *Brexit: All you need to know about the UK leaving the EU*, BBC News, viewed 20 September 2020, <<https://www.bbc.com/news/uk-politics-32810887>>.

Endsley, MR 1988, 'Design and evaluation for situation awareness enhancement', *Proceedings of the Human Factors Society 32nd Annual Meeting Human Factors Society*, Santa Monica, CA, US, pp. 97-101.

—& Robertson, M 2000a, 'Situation awareness in aircraft maintenance teams', *International Journal of Industrial Ergonomics*, no. 26, pp. 301-25.

—2000b, 'Training for situation awareness in individuals and teams', *Situation awareness analysis and measurement*, eds. M Endsley & D Garland, Lawrence Erlbaum Associates, Mahwah, NJ, US.

European Network and Information Security Agency (ENISA) 2015, 'Information sharing and common taxonomies between CSIRTs and law enforcement', ENISA, Heraklion, GR.

Europol 2019, 'Europol programming document 2019-2020', The Hague, NL.

Garfinkel, S 2012, 'Digital forensics XML and the DFXML toolset', *Digital Investigation*, vol. 8, pp. 161-74.

Hevner, A & Chatterjee, S 2010, *Design research in information systems theory and practice*, Springer, New York, NY, US.

Ilves, L, Evans, T, Cilluffo, F & Nadeau, A 2016, 'EU and Nato Global Cybersecurity Challenges', PRISM, NDU, vol. 6, no. 2.

Lee, E & Seshia, S 2015, *Introduction to embedded systems, A Cyber-Physical Systems approach*, 2nd edn., MIT Press, Cambridge MA, US.

Meilin, H, Devine, L & Zhuang, J 2017, *Perspectives on cybersecurity information sharing among multiple stakeholders using a decision-theoretic approach: Cybersecurity information sharing risk analysis*, John Wiley & Sons, Ltd, Hoboken, NJ, US.

MITRE Corporation 2018, 'Trusted Automated eXchange of Indicator Information—TAXII™: Enabling cyber threat information exchange', Department of Homeland Security, viewed 5 July 2019, <<https://makingsecuritymeasurable.mitre.org/docs/taxii-intro-handout.pdf>>.

—2013, 'A collection of information security community standardization activities and initiatives', viewed 1 July 2019, <<https://makingsecuritymeasurable.mitre.org/about/index.html>>.

Munk, S 2018, 'Interoperability services supporting information exchange between cybersecurity organisations', *Academic and Applied Research in Military and Public Management Science*, vol. 17, no. 3, pp. 131-48.

National Institute of Standards and Technology (NIST) 2016, *Guide to cyber threat information sharing, NIST Special Publication (NIST SP) 800-150*, NIST, Gaithersburg, MD, US.

OASIS Cyber Threat Intelligence (CTI) TC, DHS (CS&C) 2017a, *STIX™ Version 2.0. Part 2: STIX objects, OASIS open*, viewed 20 January 2020, <<https://oasis-open.github.io/cti-documentation/stix/intro>>.

———2017b, *TAXII™ Version 2.0. Committee specification 01, OASIS open*, viewed 20 January 2020, <<https://oasis-open.github.io/cti-documentation/taxii/intro>>.

Rutkowski, A, Kadobayashi, Y, Furey, I, Rajnovic, D, Martin, R, Takahashi, T, Schultz, C, Reid, G, Schudel, G, Hird, M & Adegbite, S 2010, 'CYBEX - The Cybersecurity Information Exchange Framework (X. 1500)', *Computer Communication*, vol. 40, pp. 59-64.

Sadique, F, Bakhshaliyev, K, Springer, J & Sengupta, S 2019, 'A system architecture of cybersecurity information exchange with privacy (CYBEX-P)', *Proceedings of the 9th Annual IEEE Computing and Communication Workshop and Conference (CCWC)*, pp. 493-8.

Sedenberg, E & Dempsey, J 2018, *Cybersecurity information sharing governance structures: An ecosystem of diversity, trust, and tradeoffs*, viewed 20 September 2019, <<https://arxiv.org/ftp/arxiv/papers/1805/1805.12266.pdf>>.

Simola, J 2020, 'Comparative Research of Cybersecurity Information Sharing Models', *Information & Security: An International Journal*, vol. 43, no. 2, pp. 175-95, viewed 20 September 2020, <<https://doi.org/10.11610/isij.4315>>.

Tidey, A, Gill, J & Parrock, J 2020, 'EU warns Turkey of quick sanctions if dialogue over Eastern Mediterranean drilling fails', *EURONEWS*, viewed 20 September 2020, <<https://www.euronews.com/2020/10/02/eu-leaders-break-deadlock-over-belarus-sanctions>>.

Vakilinia, I, Tosh D & Sengupta S 2017, 'Privacy-preserving cybersecurity information exchange mechanism', *Proceedings of the 2017 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, pp. 1-7.

Framing the Awareness Required for Maritime Information Warfare Using Historic Information Science Literature

AW Isenor¹, SA Watson²

*¹Defence Research and Development Canada – Atlantic Research Center
Dartmouth, Nova Scotia,
Canada*

Email: anthony.isenor@forces.gc.ca

*²Defence Research and Development Canada – Ottawa Research Center
Ottawa, Ontario,
Canada*

Email: susan.watson@forces.gc.ca

Abstract: *Defining Maritime Information Warfare (MIW) as truly a warfare domain implies a need for awareness of friendly and adversarial activities within the domain, with such awareness typically referred to as situational awareness (SA). Here, the components of SA in the MIW domain are clarified through a study of the historical information science literature. This study identified a conceptual model of information and its use. This model was then juxtaposed with the Royal Canadian Navy's view of MIW. A cyber example illustrates that an extremely broad set of inputs are required for SA in MIW.*

Keywords: *Situational awareness, Maritime Information Warfare, Recognized Information Picture*

Introduction

Militaries around the world have long recognized the importance of information. Arguably, this recognition dates back to Sun Tzu and *The Art of War* (Giles 2000), which notes not only that information on the adversary can be acquired through the use of spies, but also that false information can be provided to the adversary through those same spies. Although dated by the notion that adversarial knowledge can only be obtained from other men, the notion that information on the adversary is useful for the planning of upcoming battles remains valid.

Information impacts many of the functions within the Command and Control (C2) enterprise of a modern military. The Canadian C2 definition places emphasis on the decision-making enabled by information, without explicit reference to the use of information, that C2 definition being:

the exercise of authority and direction by a commander over assigned, allocated and attached forces in the accomplishment of a mission. (Department of National Defence 2020)

The definition does recognize the decision being made by the commander, and thus recognizes the human element of the decision. As such, the commander's education, life experience, and training impact the decision. Although not explicitly stated, it is widely recognized that the acquisition and use of information is important to C2 and to the overall awareness of the decision maker (Alberts, Garstka & Stein 2002).

The need to acquire and use information in the military context introduces challenges. Recently there has been considerable focus on the challenge of information volume; however, this is by no means a new challenge. In fact, historically the introduction of improved sensing capabilities has gone in lockstep with the problem of large information volumes that were recognized as difficult to manage (Bush 1945). More importantly, underlying the desire to manage this information is the recognition that the information contains value and that the management of the information is a requirement for facilitating the use of the information.

This work is not focused on the challenges of information management. Rather, this work will focus on the awareness needed to acquire and use information to support a military function. Effectively, this work deals with understanding situational awareness within the realm of information. The work is motivated by a desire to improve the understanding of situational awareness within the Maritime Information Warfare (MIW) domain. This awareness will be framed in a manner that should resonate with the naval establishment, although many of the ideas presented could be useful outside of a naval context.

The research question to be answered in the paper is: what are the components required to build the awareness needed for MIW? This question is addressed by examining the history of information science, thus grounding the effort in the foundational work in the information science field. This foundational work is still valid today, and provides a framework with which to examine MIW situational awareness from first principles. The results of this examination are presented in terms of activities that generate common naval products.

There are two goals for this paper, specifically:

- to use the historic information science literature to help identify the components of situational awareness important for MIW, and
- to juxtapose a description of these components next to more traditional naval experience.

The paper is structured as follows. First, a review of the information science literature is provided. This review is necessary to identify a conceptual model that represents the core components of information science. Next, an overview of a visual representation of the maritime domain is presented, this representation known as the Recognized Maritime Picture. This section also introduces Maritime Information Warfare. Following this introduction a discussion section serves to join the topics covered in the previous sections. This joining effectively frames the conceptual model on information and knowledge within the context of maritime information warfare. Finally, a cyber example clarifies the concepts with the final section providing a conclusion.

Information Science Perspective

Information science has library science at its foundation (Borko 1968). In fact, this foundation helps explain the common practice within universities of combining the library and information science fields under a single department. This also helps explain why early definitions of information science were very document-specific (Buckland & Liu 1998).

The association between information science and library science was arguably stronger than the association between information science and information (in a non-manuscript sense). In a post-World War II (WWII) examination of the state of research and the use of data and information, Bush (1945) identified science as a producer and consumer of information but did not identify a field of study specific to information. Bush (1945) also identified the need to enhance the production, storage, and access to the knowledge being created, effectively foretelling many of the challenges that would be faced in the coming years and decades.

Bush (1945) also referred to the volume of information being produced. In the naval setting, excessive volumes of data and information were initially attributed to the introduction of radar during WWII (Boslaugh 1999). The problem was sufficiently challenging that a specific United States (US) Navy project named CORNFIELD was stood up in 1953 with the goal of solving the radar data volume problem on platforms at sea (Boslaugh 1999). Project CORNFIELD was tasked to investigate the feasibility of outfitting an entire ship as a compute platform, with all the collected radar data from front-line platforms being sent to the compute platform for analysis. Results of the analysis would then be redistributed to the front line platforms.

Although computers were recognized as useful for information storage and processing, the volume issue also introduced the problem of information retrieval. Here, set theory mathematics drove advances in techniques to access information using specialized storage structures known as databases (Codd 1970). The challenges around information retrieval would provide an enduring research topic (Rijsbergen 1979; Frakes & Baeza-Yates 1992). Salton (1984) provided a thorough overview of retrieval methods that involved applied probabilistic retrieval, user feedback in retrieval systems, Boolean query formulations, linguistic analysis, and many other techniques.

In the 1970s, information science began a metamorphosis. One particularly notable event was an international forum that was designed to help define information science (The British Library 1975). From this forum came multiple papers on the topic of information science (Goffman 1975; Wersig & Neveling 1975; Belkin & Robertson 1976; Brookes 1980a, 1980b, 1980c, 1981). The forum also helped identify the evolution of the information scientist role (Wersig & Neveling 1975). The forum participants considered the role to evolve from a specific social need to join those producing data, findings, and discoveries, with those needing the same. The anonymous nature of the information scientist was also acknowledged, and the role was described as a go-between that served to join social communities of researchers.

In a similar line of thought, Bates (1999) introduced the information practitioner. Such a practitioner would represent and organize the information, rather than know the topic to which the information pertained. Bates (1999) also described the information science domain to be the universe of recorded information. Note that this scope is independent of the medium on or within which the information is stored.

The above historic glimpse into information science shows a past containing enduring challenges related to volume, storage, retrieval, and self-identity. However, also during this period, some information specialists were starting to wonder about the concept of information itself, and how it related to use, notably Bertram Brookes (Shaw 1990).

Brookes taught at the University College of London in the Electrical Engineering department. His publications covered a wide topic area, including information science. Brookes was part of the team that organized the aforementioned international forum on information science in 1975.

Brookes published a series of papers inspired in part by the 1975 conference. Of particular note for this examination is a paper where Brookes (1980a) presents an ‘equation’ for information usage, hereafter denoted the Brookes equation, as follows:

$$K(S) + \Delta I = K(S + \Delta S).$$

The Brookes equation illustrates how information may be used to modify one’s knowledge. The equation is not a purely mathematical expression, but rather is a symbolic representation of how information may be combined with an existing knowledge structure $K(S)$, to produce new knowledge structure $K(S + \Delta S)$. This knowledge structure is described by Brookes as a set of concepts that are linked together by relations, where information represents some smaller subset of the structure. The Brookes equation is a metaphorical representation of how information and knowledge structures are related.

Brookes formulates this equation through a series of arguments that originate with Popper’s Three Worlds (Popper 1979). Brookes explains the physical world as solely the entities that exist in Popper’s World 1. In Worlds 2 and 3, Brookes contends that the fundamental entities are information and knowledge, these entities existing within the human mind, and thus being separate from the physical world. In the following discussion, a reinterpretation of the equation is offered in the context of MIW.

Navy Perspective

In Canada, the Royal Canadian Navy (RCN) has long recognized the importance of information in the delivery of its mandate. For example, information plays a dominant role in the development of local tactical pictures and broader operational-level pictures. At the global level, the RCN has a role in the development of the Common Operating Picture (COP) (Renaud & Isenor 2011) or the Recognized Maritime Picture (RMP) (Simard, Lefebvre & Helleur 2000). The COP is a composite picture containing representations of things such as: friendly units, enemy units, important infrastructure, weather, and terrain. The RMP is a maritime-focused visual representation of vessel traffic and some land features such as ports (see **Figure 1**, below).

Information from a multitude of maritime information sources are used to construct the RMP. This information allows the tracking and identification of vessels using technologies such as Automatic Identification System (AIS) or similar vessel monitoring systems (Lapinski, Isenor & Webb 2016). Such data also allows the identification of traffic patterns for the population of vessels (Pallotta *et al.* 2014). Characteristics of these patterns are determined and are used to identify anomalous ves-

sel behaviour, and the behaviour is then further examined from a defence and security perspective. From a tactical and/or safety perspective, such a picture also aids the naval platform by providing a representation of the shipping activity in its vicinity.

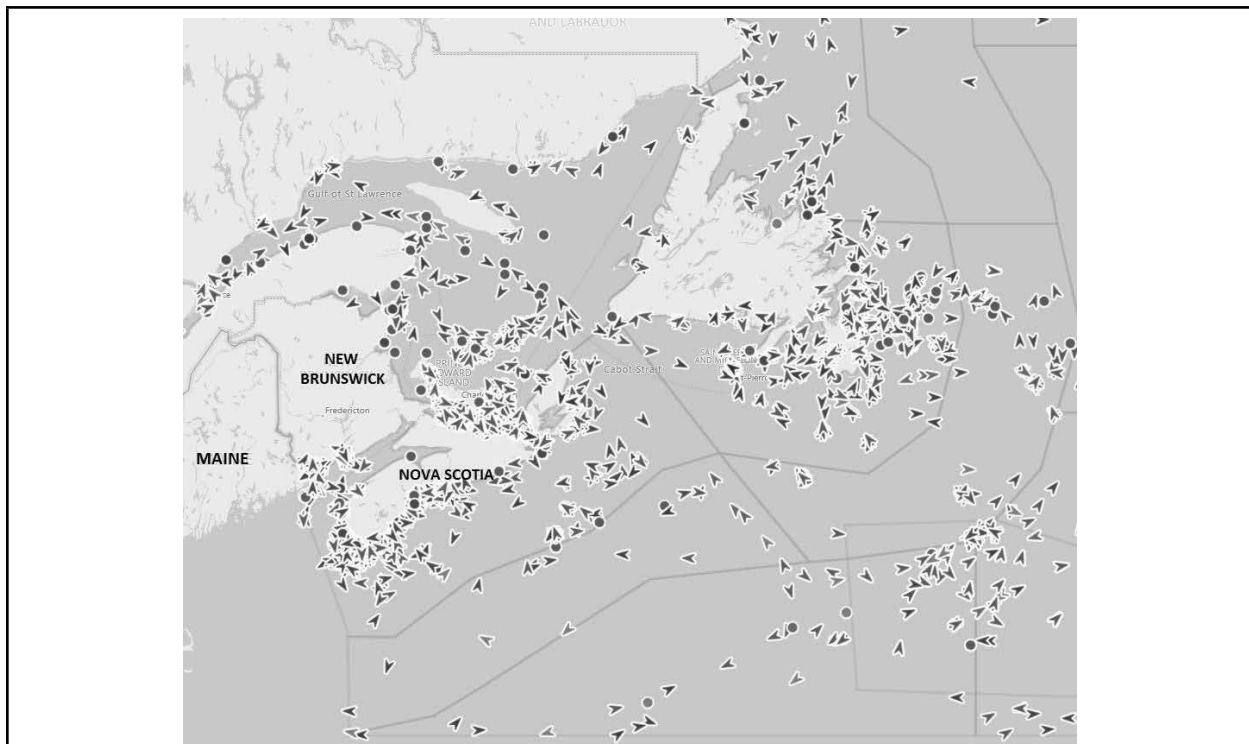


Figure 1: A representation of the RMP for the east coast of Canada. Vessels are indicated with coloured arrow heads, with colours representing the vessel type. The arrow head points in the vessel's direction of travel.

The picture is also of use from a continental defence and security perspective. For example, a land-based security operations centre mandated to maintain a watch over the vessel traffic in and near approaches to the nation (Lynch 2007), would typically use such a picture as a visual representation of the vessel traffic. These centres maintain an awareness of the purpose, origin, and destination of vessels—essentially, what the cargo is, where it is coming from, and where it is going. This is important information in the assessment of possible boarding by applicable jurisdictional authorities.

Although the visual representation of the RMP is common in the navy parlances, less common is the formal nomenclature of Maritime Information Warfare; this was only introduced by the RCN in the mid-2010s. This introduction came in the form of high-level strategy and concept papers that framed MIW as primarily being concerned with issues of data volume and variety and the need for faster processing of these data sources. In terms of definition, the RCN adopted a MIW definition in alignment with its five eyes defence partners, those partners being Australia, New Zealand, the United Kingdom, and the United States. The adopted RCN MIW definition is:

the provision, assured use and protection of information, processes, systems and networks, and the limiting, degrading and denying of that of our adversaries, to achieve operational advantage across the battlespace. (Blakeley 2017)

The definition supports the acquisition, use, and protection of the components described as making up the MIW domain. Although using slightly different terminology, Allen and Gilbert (2010) presented an argument that justified declaring the information domain (called information sphere in Allen and Gilbert [2010]), truly a domain. As with any other war fighting domains, there is a need for knowledge on the friendly and adversarial activity within the domain. As the RMP provides a representation from which SA may be generated for the maritime domain, so too must there be something within the information domain from which SA may be generated.

The two navy concepts presented above, the RMP and MIW, will now be brought together with the historic information science literature.

Discussion

From a navy perspective, the RMP represents the movement of an object from a well-defined location, a start port, to another well-defined location, the destination port. The vessel can take many different paths between start and destination, and can also carry many different forms of cargo. It can be allowed to pass freely in national jurisdictions, while in other cases its kinematic characteristics or supporting documentation can cause suspicion and result in a boarding and search of cargo. Once at the destination, the cargo can be offloaded and used locally, or can be combined with other cargo and moved onward to yet another destination.

Digital information resources can be thought of in a similar manner. Each digital resource is an object that moves from a well-defined start location to a destination. The object can take many different network paths between start and destination, and can also carry many different forms of content. From a trusted source, the object may be allowed to pass freely into a computer system, while the characteristics of other objects may cause suspicion. In extreme cases, the object can be searched for malicious or harmful cargo. The object may be used at the destination, or combined with other objects and used or moved to other destinations.

As with any analogy, there are limits. One such limit is replication, where the digital resource is much more easily duplicated as compared to its cargo equivalent. In spite of this limitation, the analogy can still be useful when considering situational awareness in the MIW domain. The analogy can help formulate the concept of a Recognized Information Picture (RIP) from the existing familiarity with the RMP. The analogy can also be used in combination with historic information science concepts, and objects noted in the MIW definition, as a way to define the pertinent objects for a RIP. A reinterpretation of the Brookes equation offers a starting point.

Consider the components of the Brookes equation in relation to the objects identified in the MIW definition. From an MIW perspective, those objects important for the RIP must in fact be those objects identified in the MIW definition—specifically, the information, processes, systems, and networks.

Linking this to a reinterpretation of the Brookes equation, the information object mentioned in the MIW definition is represented in the Brookes equation by the term ΔI . The ΔI is a solitary unit of information and can stand on its own, as it is independent from other information. As Brookes indicates, the units of the terms in the Brookes equation are only important if one thinks of the equation as a mathematical expression. This is not the case, as previously noted.

Assumed in this equation is the fact that some process has produced the ΔI . The entity producing the ΔI has been termed “the generator” (Lapinski 2019). The generator could be a person but may also be a mechanical entity, such as a sensor. In the digital space, a generator could be a computer program, such as a numerical model that predicts certain environmental conditions for a future time. In this case, the ΔI is represented by the numerical values that are the output from the numerical model.

The network object mentioned in the MIW definition may be interpreted as the Brookes equation + sign. The + sign is not discussed extensively by Brookes. From an MIW perspective, the + represents a method of transport, acquisition, or communication. It represents the active part of acquiring the unit of information, delivering it to the knowledge structure, and combining it with that structure. In practical terms, the + may represent a network through which digital information flows from provider to consumer. The + also has implications for the form of the information in that it needs to be acquired in a form that can be combined with the knowledge structure.

The remaining objects from the MIW definition are the processes and systems. Referring to the System Engineering Body of Knowledge (SEBOK), a process (System Engineering Body of Knowledge 2019a) and a system (System Engineering Body of Knowledge 2019b) are similar in that they consume something, for the purpose of producing a product or output. As well, processes and systems are higher order functions that address a higher level need. For example, processes and systems may provide monitoring, quality control, fusion, or visualization. Processes and systems use the information and knowledge, and, in the digital space, processes and systems join digital resources to typically produce a new digital resource.

Based on this description, processes and systems are represented in the Brookes equation by the equation itself. The Brookes equation indicates the merging or consuming of the information by the knowledge structure. That structure may be represented by the human mind, or by a digital resource, such as a numerical model. The combining of the information with the existing resource (human mind, numerical model) represents a process and collectively the components represent the system.

The $K(S+\Delta S)$ term in the Brookes equation represents the end structure after consumption of the ΔI . This term is the product or output of the process. In the case of a person, the ΔI has altered the person’s knowledge structure from S to $S+\Delta S$. In the case of the numerical model, inclusion of the ΔI has altered or updated the model’s state to be more reflective of current conditions.

It is also important to state that a ΔI may initially be generated for use by a specific knowledge structure; however, it may have use in other knowledge structures. A single ΔI can influence multiple knowledge structures.

Now reconsider the initial questions. If the Brookes equation represents the components of information and the processes/systems by which these components are combined, then an awareness of the MIW domain implies an awareness of all these components, plus an awareness of whether or not these components may be combined. Taking a purely digital view and thereby ignoring the human component, there emerges a requirement for an awareness of the digital resources. This

awareness identifies the existence of the resource and must include characteristics of that resource that allow an assessment of one resource's compatibility with another.

No small task—a cyber example

As noted, the + sign in the Brookes equation represents the mechanism through which the joining of the information and knowledge structure takes place. In a digital sense, the + sign can be taken to represent the network over which the information moves to the knowledge structure.

To construct SA of the network (that is, SA of the + sign), information must be produced on the state of the network. In that respect, the information transport mechanism itself is a generator of information; however, here this network information (NI) is distinguished from the ΔI (see **Figure 2**, below). The movement of the ΔI through the network introduces a purely cyber aspect to the SA generation, and with this comes the identification of numerous cyber-related challenges. For example, it may be necessary to know what has happened, and what is happening, as the digital resource ΔI is being transported. This in turn supports the identification of any unintended effect(s) on the digital resource.

Thus the information transport mechanism itself is a producer of information that contextualizes the delivered information. Typically, the information transport mechanism is a communications network and the information it generates supports the creation of network situational awareness.

In the naval environment, the information transport mechanism is typically a communications network that may in part be wireless. For example, a satellite communications network between a shore site and a mobile platform (for example, a ship), or a mobile *ad hoc* network for ship-to-ship communications. In such a situation, information delivered via wireless channels is subject to an assortment of network failures, attacks, and errors (Burbank *et al.* 2006; Zou *et al.* 2016). To mitigate these issues, the production of NI helps to maintain network service levels, and assists network managers in terms of their overall awareness and resulting action. Part of the NI is cyber security information, and may include detection of anomalous network traffic and degraded device trust levels (Srinivasan *et al.* 2008). Device trust levels represent the degree of confidence in the authenticity of the device—that is, that the device has not been spoofed or compromised.

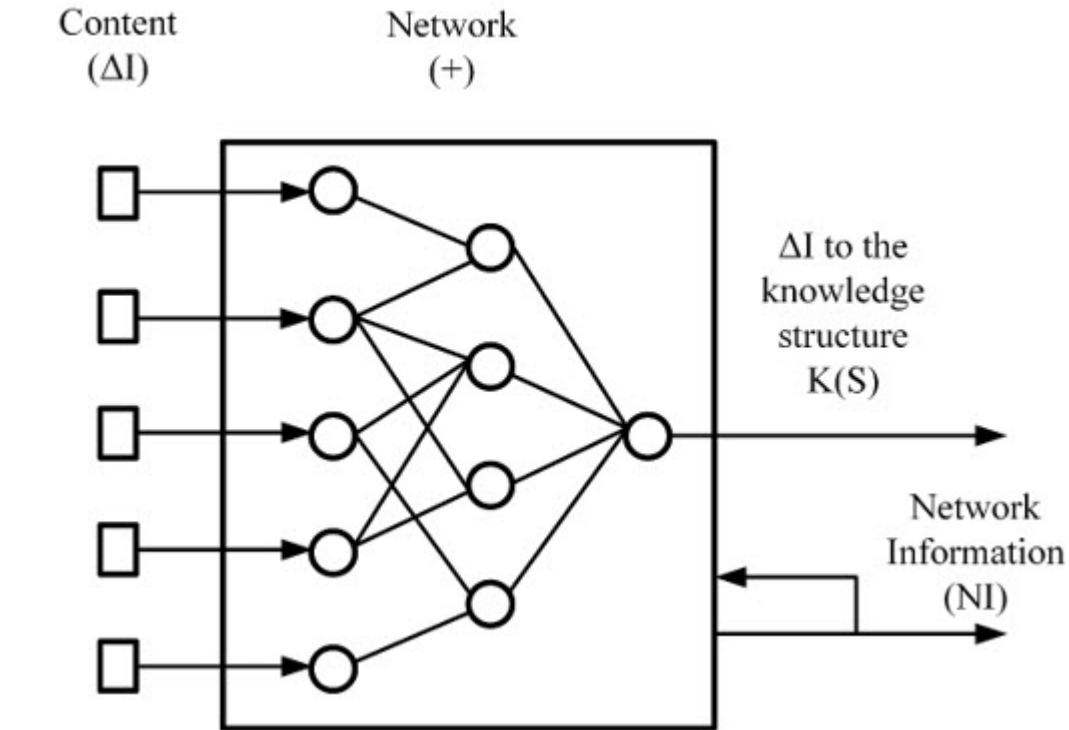


Figure 2: A depiction of content flowing through a network of nodes, with network information generated from the nodes

For large-scale networks, such as a satellite communications network, all elements in the network architecture must be monitored, including ground stations, end-user terminals, and satellite links. In this example, relevant NI may include more specific information, such as per-user traffic metrics, signal quality data, or more general information, such as global network utilization and satellite beam assignments (Miller, Taylor & Caliguirri 2019).

The sum of all the required NI results in a high volume of produced information that deals solely with the network. Often, this volume results in compromises being made between scope, scale, and timeliness—for example, how much NI is generated, how many and how broadly placed are the producers of that information, and how often the information is produced. The produced NI, once aggregated at the network-level, then gives indications of large-scale performance and allows operators to decide where to inspect further to identify faults and threats.

It is also worth noting that problems with NI volume and scope are not limited to large-scale enterprise networks. In mobile *ad hoc* networks having a moderate number of nodes (N), the scope of information distribution can be hampered by the highly connected nature of the network, which requires many-to-many communications. For example, in a mobile *ad hoc* network, all nodes are collectively responsible for routing, or relaying, packets to their destinations. To aid each relaying node in selecting the best next relay node to get the packet to its destination, the relaying nodes require knowledge of the state of all node-to-node communication links in the network. This knowledge may be acquired by each node sending its local link state to all other nodes in the network. To do so, the node may send a message to neighbouring nodes, which then relays the message to all of its neighbours, and so forth until the message eventually reaches all $N-1$ other nodes.

However, with this method, a single link state change generates $O(N^2)$ total messages (Aho & Lee 2000). Even in more efficient implementations, dissemination of link state entails significant traffic, and threatens to limit network throughput capacity for mission-critical data (Burbank *et al.* 2006). Similar scalability problems arise when disseminating other NI throughout the network to where it is needed.

In both the satellite communications network and mobile *ad hoc* network examples, the required NI for SA of the + sign, is substantial. This issue is further complicated by the realization that most military networks are limited in their bandwidth. In fact, the potential information produced in support of SA in the + can be beyond the capacity of the network itself, and requires prioritization, filtering, and strategic dissemination. Alternately stated, the network must carefully manage the volume of network traffic required to collect all network and cyber security information needed for SA. Combining the bandwidth limitations with the combinatorial issue, collecting up-to-date information regarding the network as a whole is challenging.

Although the SA required for the + sign is substantial, the conceptual model nevertheless provides a mechanism to bridge communities of interest. Specifically, the model provides a potential basis for which to understand and to develop linkages between cyber and information warfare research within the Canadian defence research community. Such linkages are already being created and, perhaps, with further promulgation, additional linkages will be recognized.

Conclusion

An historic examination of information science has provided a conceptual model for the joining of information and knowledge. Reinterpreting this model to account for the digital space has allowed an interpretation of situational awareness within the Maritime Information Warfare domain. A cyber example, representing one term in the reinterpreted model, is presented. The example indicates the complexity and breadth of SA-supporting information that is required. In fact, the challenge here is that the information required to support SA of the network, may exceed the network's capacity.

The reinterpretation of the Brookes equation allows the breadth and scope of the information domain to be better understood. In the digital space, the reinterpretation encompasses all digital resources, the network status, and sufficient process and system information to assess whether or not resources may be used in combination. This implies that SA provides both an awareness of the current information landscape, but also a method of determining whether or not information resources can be combined to form new products. This in turn implies ample metadata that describes the receiving knowledge resource, the consumed information resource, and the resulting product. These metadata descriptions must be of sufficient detail to allow the system to automatically determine if the resources can be combined, before an attempt is made to combine them.

The breadth of the reinterpretation clearly points to a need to dissect the problem space of SA in the MIW domain into smaller, more attainable components. These components may ultimately be used within the concept of a Recognized Information Picture, to improve both system and human understanding of the all-important information resources. Such a picture would be difficult to visualize due to its scale. Categorizations of information resources would be required to bring

the number of visualized entities under control—and even then the sheer number would likely be problematic.

References

- Aho, AV & Lee, D 2000, 'Hierarchical networks and the LSA N-squared problem in OSPF routing', *Proceedings of the Globecom '00-IEEE. Global Telecommunications Conference, Conference Record (Cat. No. 00CH37137)*, IEEE, pp. 397-404.
- Alberts, DS, Garstka, JJ & Stein, FP 2002, *Network Centric Warfare; Developing and Leveraging Information Superiority*, US DoD Command and Control Research Program.
- Allen, PD & Gilbert, DP 2010, 'Qualifying the information sphere as a domain', *Journal of Information Warfare*, vol. 9, pp. 39-50.
- Bates, MJ 1999, 'The invisible substrate of information science', *Journal of the Association for Information Science and Technology*, vol. 50, p. 1043.
- Belkin, NJ & Robertson, SE 1976, 'Information science and the phenomenon of information', *Journal of the American Society for Information Science*, vol. 27, pp. 197-204.
- Blakeley, D. 2017. 'Information as war: The RCN comes to grips with a new battle space', *Trident News*, 21 August.
- Borko, H 1968, 'Information science: What is it?', *American Documentation*, vol. 19, pp. 3-5.
- Boslaugh, DL 1999, *When computers went to sea: The digitization of the United States Navy*, IEEE Computer Society, Los Alamitos, CA, US.
- Brookes, BC 1980a, 'The foundations of information science Part I. Philosophical aspects', *Journal of Information Science*, vol. 2, pp. 125-33.
- 1980b, 'The foundations of information science: Part II. Quantitative aspects: Classes of things and the challenge of human individuality', *Journal of Information Science*, vol. 2, pp. 209-21.
- 1980c, 'The foundations of information science: Part III. Quantitative aspects: Objective maps and subjective landscapes', *Journal of Information Science*, vol. 2, pp. 269-75.
- 1981, 'The foundations of information science: Part IV. Information science: The changing paradigm', *Journal of Information Science*, vol. 3, pp. 3-12.
- Buckland, M & Liu, Z 1998, 'History of information science', *Historical Studies in Information Science*, TB Hahn & M Buckland (eds.), Information Today Inc., Medford, NJ, US, pp. 272-95.
- Burbank, JL, Chimento, PF, Haberman, BK & Kasch, WT 2006, 'Key challenges of military tactical networking and the elusive promise of MANET technology', *IEEE Communications Magazine*, vol. 44, pp. 39-45.

Bush, V 1945, 'As We May Think', *The Atlantic Monthly*, July.

Codd, EF 1970, 'A relational model of data for large shared data banks', *Communications of the ACM*, vol. 13, pp. 377-87.

Department of National Defence 2020, Command and Control. Defence Terminology Bank.

Frakes, WB & Baeza-Yates, R 1992, *Information retrieval: Data structures and algorithms*, Prentice Hall, Eaglewood Cliffs, NJ, US.

Giles, L 2000, *Sun Tzu on the Art of War*, Allandale Online Publishing, Leicester, UK.

Goffman, W 1975, 'On the phenomena of interest to an information science', *Proceedings of the International Research Workshop on the Theoretical Basis of Information Science*, 7.

Lapinski, A-LS 2019, 'Redefining situation awareness for the maritime information warfare domain', *1st Maritime Situational Awareness Workshop MSAW 2019*, Villa Marigola, Lerici (La Spezia), Italy.

—, Isenor, AW & Webb, S 2016, 'Simulating surveillance options for the Canadian north', *Journal of Navigation*, vol. 69, pp. 940-54.

Lynch, T 2007, 'Canadian maritime security: From the navy on patrol to the police on the beat', *Maritime Studies*, vol. 2007, pp. 22-6.

Miller, C, Taylor, F & Caliguirri, M 2019, 'Advanced enterprise situational awareness reporting for enhancing space operations', *Proceedings of the 35th Space Symposium*, Colorado Springs, CO, US.

Pallotta, G, Horn, S, Braca, P & Bryan, K 2014, 'Context-enhanced vessel prediction based on Ornstein-Uhlenbeck processes using historical AIS traffic patterns: Real-world experimental results', *17th International Conference on Information Fusion (FUSION)*, Salamanca, Spain, p. 7.

Popper, K 1979, *Three worlds*, University of Michigan Press, Ann Arbor, MI, US.

Renaud, WM & Isenor, AW 2011, 'Situational awareness: Inspiring operational clarity', *Canadian Military Journal*, vol. 11, pp. 24-31.

Rijsbergen, CJv 1979, *Information Retrieval*, 2 ed., Butterworth-Heinemann Newton, MA, US.

Salton, G 1984, 'A note about information science research', *Journal of the American Society for Information Science*, vol. 36, pp. 268-71.

Shaw, A 1990, 'BC Brookes and the development of information science: A bibliography', *Journal of Information Science*, vol. 16, pp. 3-7.

Simard, M-A, Lefebvre, E & Helleur, C 2000, 'Multisource information fusion applied to ship identification for the recognized maritime picture', *SPIE 4051, Sensor Fusion: Architectures, Algorithms, and Applications IV*, Orlando, FL, US.

Srinivasan, A, Teitelbaum, J, Wu, J, Cardei, M & Liang, H 2008, 'Reputation-and-trust-based systems for ad hoc networks', *Algorithms and protocols for wireless and mobile ad hoc networks*, pp. 375-403.

System Engineering Body of Knowledge 2019a, *Process*, viewed 1 April 2020, <[sebokwiki.org/Process_\(glossary\)](http://sebokwiki.org/Process_(glossary))>.

—2019b, *System*, viewed 1 April 2020, <[sebokwiki.org/System_\(glossary\)](http://sebokwiki.org/System_(glossary))>.

The British Library 1975, 'International research forum in information science: The theoretical basis of information science', *Proceedings of the International Research Forum in Information Science: The Theoretical Basis of Information Science*, eds. BC Vickery & SE Robertson, University College, London, UK.

Wersig, G & Neveling, U 1975, 'The phenomena of interest to information science', *The Information Scientist*, vol. 9, pp. 127-40.

Zou, Y, Zhu, J, Wang, X & Hanzo, L 2016, 'A survey on wireless security: Technical challenges, recent advances, and future trends', *Proceedings of the IEEE*, vol. 104, pp. 1727-65.