Beware Suppliers Bearing Gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks

Colin Topping[a,*], Andrew Dwyer[b], Ola Michalec[a], Barnaby Craggs[a], Awais Rashid[a]

[a] *Bristol Cyber Security Group, University of Bristol*
[b] *Department of Geography, University of Durham*

Abstract

Threat actors are increasingly targeting extended supply chains and abusing client-supplier trust to conduct third-party compromise. Governments are concerned about targeted attacks against critical national infrastructures, where compromise can have significant adverse national consequences. In this paper we identify and review advice and guidance offered by authorities in the UK, US, and the EU regarding Cyber Supply Chain Risk Management (C-SCRM). We then conduct a review of sector specific guidance in the three regions for the chemical, energy, and water sectors. We assessed frameworks that each region's sector offered organisations for C-SCRM suitability. Our results found a range of interpretations for "Supply Chain" that resulted in a diversity in the quantity and quality of advice offered by regional authorities, sectors, and their frameworks. This is exacerbated by the lack of a common taxonomy to support supply chain procurement and risk management that has led to limited coverage in most C-SCRM programs. Our results highlight the need for a taxonomy regarding C-SCRM and systematic guidance (both general and sector specific) to enable controls to be deployed to mitigate against supply chain risk. We provide an outline taxonomy based on our data analysis to promote further discussion and research.

Keywords: cyber security; supply chain; risk management; critical national infrastructure; common taxonomy

1. Introduction

The twenty-first century has witnessed an exponential increase in the digitisation and interconnectivity of computer networks and software applications that has benefited business, but this has consequently introduced greater vectors of compromise from threat actors [39]. This threat extends to a supply chain that may be more difficult to manage due to a lack of clear responsibility, the international dimension of markets they operate on, and diversity of suppliers. This results in threat actors probing for weaknesses to exploit client and supplier trust.

Concerns surrounding the supply chain have been prominent in several UK Government reports that identify minimal requirements for suppliers to adhere to cyber security standards [68]. Excellent cyber security within an organisation cannot guarantee that the same standards are applied by contractors and third-party suppliers [48], with attackers more likely to target vulnerable entry points, that include the supply chain. Similarly, the UK's National Cyber Security Centre (NCSC)

*Please address correspondence to Colin Topping
Email address: colin.topping@bristol.ac.uk (Colin Topping)

Annual Review in 2018 [47] stressed the role played by the supply chain in leaving organisations vulnerable to compromise.

One of the areas of growing concern amongst operators of various Critical National Infrastructure (CNI)[1] is the increased exposure of Industrial Control Systems (ICS). This is due in part to the decline in the practice of "air gap" architecture, exposing legacy systems to external influence through associated benefits of inter-connectivity with the Industrial Internet of Things (IIoT). This enhanced visibility and integration promotes more efficient and effective business processes by embracing real-time intelligence from ICS environments for cost improvement. This convergence between the Internet of Things (IoT) and Operational Technology (OT) used within ICS has blurred the boundaries between legacy and contemporary environments [21] and can lead to attacks, such as those on manufacturing plants as shown by the German Steel work attack [41] and against the Ukrainian Power Grid [70].

Supply chains are integral to the operations of CNI despite not being formally regarded as a component of it. A technical report to the UK parliament [51] focused on the hardware, software, and services offered by the supply chain, but did also touch upon non-contractual and contractual steps to manage supplier risk, specifically looking toward the EU Network and Information Systems (NIS) Directive [31] to assist the cyber supply chain risk management (C-SCRM) for CNI operators.

Our review of current academic literature finds that existing research has considered challenges and means to improve supply chain cyber security. For example, Williams [71] explored the increasing complexity and global interconnections of the supply chain and the challenges in securing such an environment. Davis [22] discusses how organisations can adopt an information-centric approach to deliver more cyber-resilience into supply chains. However, to date, we found no evidence of research to systematically analyse the coverage of supply chain cyber security advice given by national or supranational authorities and also sector specific guidance, how the various approaches contrast, and their strengths and limitations. This paper is the first to address this knowledge gap.

We focus on three legal authorities (UK, US, EU) and analyse the guidance offered to organisations in their CNI sectors; Chemical, Energy, and Water, relating to C-SCRM. This analysis also identifies the principle guidance, frameworks, regulations, and standards recommended and these too are analysed against the same criteria to determine whether there is a common approach to ensuring how supply chain risk management should be applied. We find that despite the abundance of both cross-sectoral and sector-specific guidance and a variety of frameworks produced over the past decade, there is significant divergence of exactly what constitutes the supply chain coupled with a variance in the depth and coverage of the advice to which organisations are exposed. Where organisations are encouraged to implement a C-SCRM program, the lack of commonality within the available guidance leads to a lack of clarity on the risks to consider. This may lead to possible weaknesses during cyber security risk assessment that, in general, follows government and sectoral guidance.

This is amplified by the lack of a common taxonomy that would allow governmental and sector-specific guidance to have the same look and feel to the end user organisation. This is tied to calls by key stakeholder documents for a harmonisation of standards. The need for the creation of a common taxonomy regarding C-SCRM to support systematic general and sector specific guidance is

[1]CNI: National Infrastructure are those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends. https://www.cpni.gov.uk/critical-national-infrastructure-0. These are referenced as Critical Infrastructure in U.S. and some EU documents.

a key finding and one that would benefit both client and supplier stakeholders in working towards a common objective.

This paper *analyses the coverage of supply chain cyber security in both sectorial and cross-sectorial CNI frameworks* to investigate the following research questions:

1. *What is meant by Supply Chain?* We evidence contrasting interpretations of what constitutes the supply chain that can lead to gaps in cyber security strategies and may lead to C-SCRM programs being vulnerable to compromise.
2. *What guidance do authorities and sectors provide?* We establish that the depth and breadth of coverage offered by authorities and sectors differs greatly. Recommended frameworks are often aligned to regional foci or regulatory requirements. This is a concern as the supply chain becomes more global and interconnected in ensuring that organisations have the optimum C-SCRM guidance appropriate for their function within a specific sector. Differing approaches to C-SCRM may require the supply chain to provide inconsistent products or assured levels of service to different sectors. This, in a global supply chain, may become unnecessarily complex, resource intensive, costly, and unsustainable.
3. *Do frameworks provide cohesive coverage?* Global frameworks are sector agnostic, but government, regulatory, sector, and industry specific objectives may influence which framework organisations adopt. Although supply chain security has been introduced in recent version releases, the underlying and repeatable need for a common language [6, 31, 50] to help deliver a common and repeatable approach to C-SCRM is still absent.

2. Related Work

In this section, we review current academic research, which identifies a gap in scholarly attention regarding the guidance offered to sectors of CNI to ensure due diligence is given to the breadth of supply chain concerns.

2.1. Supply Chains and their Security:

Bartol [5] points to C-SCRM requiring the coming together of several divergent professional communities from cyber security, system and software engineering, supply chain, and logistics, which bring differing experiences, taxonomy, frameworks, and standards. Linton et al. [43] highlight that this is a complex discipline that straddles both traditional cyber security and the supply chain management field, mitigating risks to both Information and Communications Technology (ICT) supply chains and ICT products and services. They believe that these risks traverse the supply chain and can result in organisations lacking visibility, understanding, and control of the processes used to manufacture and deliver ICT products.

Where practicable, and to remove the typical isolation in the C-SCRM process, Colicchia et al. [19] recommend that initiatives should be bi-directional to involve supply chain partners. They believe that this promotes controls beyond technical solutions and maintains engagement throughout the supply chain. C-SCRM's focus is on gaining visibility and control over an organisation's extended partners that include suppliers and customers. Boyson [7] argues that this satisfies the need of IT architects for effective control of the design, build, and deployment of systems whose hardware and software subsystems and components are increasingly sourced globally and often with an unknown pedigree. Often critical functionalities are hosted and accessed on network environments of uncertain integrity.

Ghadge et al. [35] highlight that supply chains are the backbone of the evolving technological ecosystems and there is a need to help innovate relationships between supply chain partners. They provide a detailed analysis of cyber risk types, propagation, and points of penetration together with assessing cyber security challenges. However, they do not consider what constitutes the supply chain against which the risk is being managed, nor point to any specific frameworks to assist in this. Davis [22] advocates that governance of the supply chain is critical, with organisations encouraged to map out the supply chain to understand direct and indirect suppliers, build capability aligned to agreed standards that may include sharing information and expertise to ensure risks are adequately managed and measured. The construct of a supply chain is not considered, nor is the capability of the standards referenced in adequately supporting a viable SCRM.

Young et al. [73] reference that the US Department for Homeland Security (DHS) has developed and implemented programs to seek to improve the information sharing environment for the private sector which, it acknowledges, operates the majority of CNI. Rashid et al. [55] highlight that production and distribution networks are often owned by different organisations, with a larger number of businesses forming the wider supply chain in their paper that looks at cyber security risks in CNI. This aligns with the increasingly global and complex supply chain that we also consider in our analysis.

2.2. Risk Management:

The issue of outsourcing CNI to private entities as well as possible ownership and foreign investment have not been covered in great detail elsewhere in other related work. Sajid et al. [57] do consider that the use of third-party cloud services within ICS transfers ownership privileges from the system's organisation and places them under the control of the cloud service provider.

C-SCRM is emerging as a new management construct to satisfy a need to adopt a different approach to embrace the interconnected nature of supply chains to deliver a combination of C-SCRM, resilience, and information risk management [19]. It is an integrative construct combining elements of cyber security, supply chain management, and enterprise risk management to assess and mitigate risks across the end-to-end process that constitute the supply chains for IT networks, hardware, and software systems. Boyson [7] acknowledges the increasingly global nature of the cyber supply chain, the threats that this invokes and the challenges in successfully implementing a C-SCRM program. This US-centric work reviewed current programs and the rationale for a capability/maturity model for the cyber supply chain.

Whilst not considering supply chain as forming part of a risk management approach, Pate-Cornell et al. [52] conclude that the management of cyber risks for CNI are often based on a top-down management approach, with the goal of encouraging system designers and operators to adopt best practices, but often without specific consideration of the system's structure or offering much guidance on how to do it. The insurance industry relies heavily on actuarial science to develop mathematical and statistical models that are used for empirically or technically estimating risk, and Young et al [73] attempt to develop a framework to use such techniques for cyber security CNI owners and operators, but again do not consider incorporating C-SCRM into their work. Cherdantseva et al [13] do consider system and component design and equipment supply stages for the six steps that comprise their cyber security risk assessment and to adapt relevant NIST[2] standards to the specific

[2]The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency that produces standards and guidelines. It also provides guidance documents through its Special Publications (SP) 800-Series.

system being assessed, but they do not suggest that it would provide a C-SCRM solution and the focus is contained within the business.

2.3. Frameworks and Standards:

Davis [22] asserts that standards can be used to provide a common understanding, a starting point, and terminology on how an organisation approaches its business and cyber security, but this does not expand to determine whether standards themselves are aligned to a common taxonomy and approach to support C-SCRM. In the same way that safety regulation in roads, aviation or medicine enhances their value to the community, Quigley et al. [54] state that cyber security may ultimately benefit from similar regulation and awareness and look to better understand the weaknesses in the risk regulation regime that governs cyber security within CNI. They argue that governments should be more specific in their statements around breaches in cyber security to avoid interested parties over- or under-playing risks in an attempt to modify behaviour of interested stakeholders.

There must be a workable relationship between decision makers, employees, relevant standards, technical aspects, and policy frameworks as argued by Clark-Ginsberg and Slayton [16]. They call for collaboration between regulator and system owners and state that regulatory influence is shaped by three factors - incentives, scope, and adaptability - thereby helping clarify the powers and limitations that regulations have in affecting change.

Carr [11] questions the reluctance of politicians to claim authority for the state to introduce tougher cyber security measures by law[3], aligned to the private sector's reluctance to accept responsibility or liability for national security, leaving the partnership without clear lines of responsibility or accountability. This risk ownership when the private sector delivers CNI services is something that underpins our research questions 2 and 3.

Finally, Bahuguna et al. [3] stated the need for a national cyber security assurance framework with a dedicated government cyber security bench-marking agency established to validate the cyber security posture of a specific country and its critical sectors on a continuous basis. It did not consider C-SCRM as part of this assurance framework, nor did it acknowledge established baseline national assurance certifications, such as the NCSC UK Cyber Essentials program[4], or the US NIST Cyber Security Framework [50], nor the NIS Directive [31] that European member states must adopt for operators of essential services.

3. Method

In order to address how C-SCRM is understood and constructed by various forms of documentation, we use the common technique of snowballing [72] to identify relevant documentation to subsequently categorise the forms of guidance given.

3.1. Defining the Scope

Before identifying relevant documentation, a criteria for inclusion is developed, as below:

[3]Carr's paper focused on the US and UK and predates the introduction of either GDPR or the NIS Directive by the EU. GDPR regulates personal data protection and is unrelated to C-SCRM for CNI, whilst the NIS Directive is highly applicable.

[4]Cyber Essentials is a UK Government-backed, industry-supported scheme to help organisations protect themselves against common online threats: https://www.ncsc.gov.uk/cyberessentials/overview.

1. Authority regions: In order to compare and contrast with other literature and to more easily identify material on C-SCRM, we restrict our document to the UK, the US, and the EU.
2. Time: In order to understand contemporary C-SCRM governance, we only identify papers published since 2010. This aligns with Hemsley and Fisher's [36] timeline for the increased growth and complexity of ICS cyber security incidents.
3. CNI Sectors: We include three sectors that qualified in the three authority regions. The sectors, *Chemical*, *Energy*, and *Water and Wastewater* all satisfy this requirement [45], as well as representing both consumer and supplier components of the supply chain.

We seek to define what determined a threat or risk criteria, and the governance models considered, as detailed below:

4. Defining Risk and Threat: Our approach is to identify risk as being the potential compromise to the traditional cyber security triad of *confidentiality, integrity, and availability* due to underlying vulnerabilities. The category of *compromise to safety* is also included due to the association with the CNI Sector where it is often seen as the highest priority [37]. We define "threats" as actors that take advantage of such vulnerabilities pertinent to the trust in the supply chain. This includes the attack surface being extended beyond the traditional boundaries of a business enterprise [42], and the exploitation of trust that an organisation may have with a third-party supplier.
5. Defining Governance models: Once documents that aligned with the defined scope had been identified, each was analysed for governance models [9] that align to either guidance, standards, frameworks or regulations[5]. Organisations often adopt control frameworks that map to national or international standards, or detail legislative and regulatory compliance.

3.2. Document Sampling

1. Google was the principle search engine to identify the seed documents that primarily resided on government and authority websites. These websites are then used to expand the search to identify relevant documentation through a combination of search terms pertaining to *Cyber Supply Chain Risk Management*. Search strings are constructed from the key words "cyber", "supply chain" and "risk". A second criteria is added with "CNI" and "Critical National Infrastructure". This was conducted in late 2019 and 27 November 2019 forms the cut-off date.
2. Bibliographies of the documents identified in the previous step are analysed to identify further relevant literature. As some documents do not contain a bibliography, the texts are also analysed for references to other documents. This therefore follows a "backwards" snowball. Authority and sector documents are referenced within the related work, forming an avenue to identify appropriate publications for analysis, whilst the snowball method [72] also proves effective at identifying further sources for sampling.
3. Steps 1 and 2 identified 61 documents that are considered against the specific objectives of this paper of understanding the levels of guidance that authorities and sectors are issuing regarding C-SCRM. The criteria for governance models are applied and, focusing on this criteria, allows the data set to be reduced as follows:

[5]For the remainder of this paper we will use Frameworks to act as a catch all for Guidance, Standards, Frameworks, and Regulations

Authority: 31 documents down to 11
Chemical: 6 to 6
Energy: 14 to 7
Water: 10 to 4

14 frameworks were identified during the coding of the authority and sector documents. Qualitative coding in this context is the capture of a word or short phrase to symbolically identify themes in data [58] and explained further in 3.3.2. The 5 most referenced framework documents are selected for detailed coding review and covered international, European, and US products. International documents such as the International Organization for Standardization (ISO) 27000 series and the International Society of Automation (ISA) 62443 series of documents arrived for consideration via the snowballing process.

3.3. Content Analysis

3.3.1. Reflexive Thematic Analysis:

In order to analyse the documentation, a reflexive thematic analysis is conducted [8]. This enables a bottom-up, inductive approach that leads the analysis. This is twinned with a reflection on prior assumptions by reassessing the coding process and to ensure interpretations of the textual data produce codes that are arrived at from the material as much as possible. Throughout the drafting of the paper, other authors feed into the analysis and collaborated to achieve agreement.

3.3.2. Coding

An inductive coding approach [58] is undertaken by the lead author to develop the themes of the analysis. QSR International's NVivo 11 qualitative data analysis software is used to create the code book using this bottom-up approach that consists of 10 categories and an initial 45 sub-categories were produced on the first round of coding. A full understanding of the diversity in the documents is developed after two further iterations of re-coding. These are refined and condensed to 7 categories and 20 sub-categories (Figure: 1), some are merged, whilst others cover themes that are outside of the defined scope of this paper. This bottom-up approach aimed to ensure that nothing is missed.

The second author validated the coding of the lead author, using the code book. The reviewer coded 11 of the documents, which was over 20% of the documents within each sub-folder. Documents are allocated a number in each folder and Excel used to produce a random number generator for selection to be independently coded. Validation of the inter-coder agreement is undertaken using *Cohen's κ coefficient*, which is a common quantitative measure of reliability of qualitative data [18]. We measure a κ of 0.58, which indicates a moderate level of agreement [40].

3.4. Taxonomy Outline

Following the data analysis activity in section 4.1, further research is undertaken of that output to determine the requirement for a common taxonomy, which is addressed in section 5.1. This bottom-up approach aligns with the reflexive thematic analysis approach and ensures that the output is reflective of the raw data. The resulting initial taxonomy that comprises of 4 categories and underlying sub-categories and attributes is used to map against two applicable documents [20, 15] in section 5.3.

Documents	
	Authority Documents
EU	EU Cyber - Protection measures for ICT on CNI [27]
EU	EU Rules for the protection of infrastructure relevant for security of supply [29]
EU	ENISA - EU Cyber Security Act [32]
UK	CPNI - Cyber Security Risks in the Supply Chain [12]
UK	NCSC - Supply Chain Security Collection [20]
UK	HSE Cyber Security for IACS edn 2 [37]
UK	NCSC Annual Review 2018 [47]
UK	NCSC NCA Cyber Threat to Business 2018 [48]
UK	UK Public Summary of Sector Security and Resilience Plans [10]
US	Secure Technology Act [67]
US	Worldwide Threat Assessment [17]
	CNI Sector Documents
	Chemical
EU	None
UK	NE Chemical Processing Industries Report - Cyber Security of IACS (2018) [34]
US	DHS CFATS Risk Based Performance Standards - 8 Cyber (2009) [63]
US	DHS Chemical Sector Specific Plan (2015) [62]
US	DHS Chemical CSF Implementation Guidance (2015) [61]
US	Protecting and Securing Chemical Facilities from Terrorist Attacks Act (2014) [66]
US	RCSC NIST Framework Guidance (2016) [1]
	Energy
EU	EU Policy on Critical Energy Infrastructure Protection (2012) [28]
EU	ETSI Smart Grid Information Security (2012) [27]
UK	BEIS ENA Cyber Security Procurement Language Guidance (2016) [6]
US	FERC CIP-013-1 – Cyber Security - Supply Chain Risk Management (2018) [49]
US	FERC Revised Critical Infrastructure Protection Reliability Standards (2016) [33]
US	NATF Cyber Security Supply Chain Risk Management Guidance (2018)[46]
US	DOE Cyber Security Procurement Language for Energy Delivery Systems (2014) [26]
	Water and Wastewater
EU	None
UK	DWI NIS Directive Cyber Assessment Framework Guidance (2018) [24]
UK	Water UK Cyber Security Principles (2017) [69]
UK	DEFRA Water Sector Cyber Security Strategy (2017)[23]
US	DHS Water and Wastewater Systems Sector-Specific Plan (2015) [64]
	Standards and Frameworks
EU	NIS Directive (2016) [31]
US	NIST Cyber Security Framework (CSF) Version 1.1 (2018) [50]
US	NIST SP 800-82 Rev2 (2015) [60]
Int	ISA 62443-2-1 (2009) [2]
Int	ISO 27001 (2013) [38]

Table 1: Documents selected for coding and analysis

3.5. Limitations

During the review of available regional literature for the individual sectors, it is noticeable that although they provide authority guidelines, the EU is underrepresented at a sector level. This is likely due to the European Parliament creating directives, regulations, and standards, but deferring down to the individual member states on how they are implemented and the specific guidance offered [44].

The decision to limit the sample search to the year 2010 and beyond has the drawback of limiting any historical references, although the advancement in technology and the exposure of ICS environments in recent years validates this approach [36].

The number of CNI sectors to focus on is a consideration. Our research design is to assess the depth of the available guidance rather than the breadth of sectoral guidance. Therefore we contrast three sectors, appreciating that this subsequently means that only a subset of the CNI sectors is researched.

A similar consideration is given to the frameworks selected. Focusing on a single document will create limitations as there is not a directly comparable document that is adopted by all sectors. Therefore a subset of documents is selected, although this list is not exhaustive and those discounted may enrich the research. Coding of selected guidance documents allows all framework instances to be captured. This systematic approach allows deeper analysis of frequently referenced frameworks, rather than reviewing the breadth of framework coverage.

Using the three authority areas opens up the research options beyond a single nation state, but focus remains aligned to an Anglo-centric understanding of CNI due, in part, by the location of the authors. It does however focus on key players in both technical and regulatory advancement in the sectors whilst being cognisant that the UK has since exited the EU, but continues to comply with GDPR and the NIS Directive.

Finally, it must be acknowledged that the US established the Cybersecurity and Infrastructure Security Agency (CISA) in November 2018 and it is now providing similar content to that of the NCSC. Had we run the document sampling 12 months later, there would likely have been a greater level of coverage for the US Authority following the release of relevant documents throughout 2020. We include the CISA ICT SCRM Essentials [15] document to review the C-SCRM alignment in section 5.3. It was released after the cut off date for data sampling, but is viewed as relevant to the outline taxonomy discussion.

4. Results

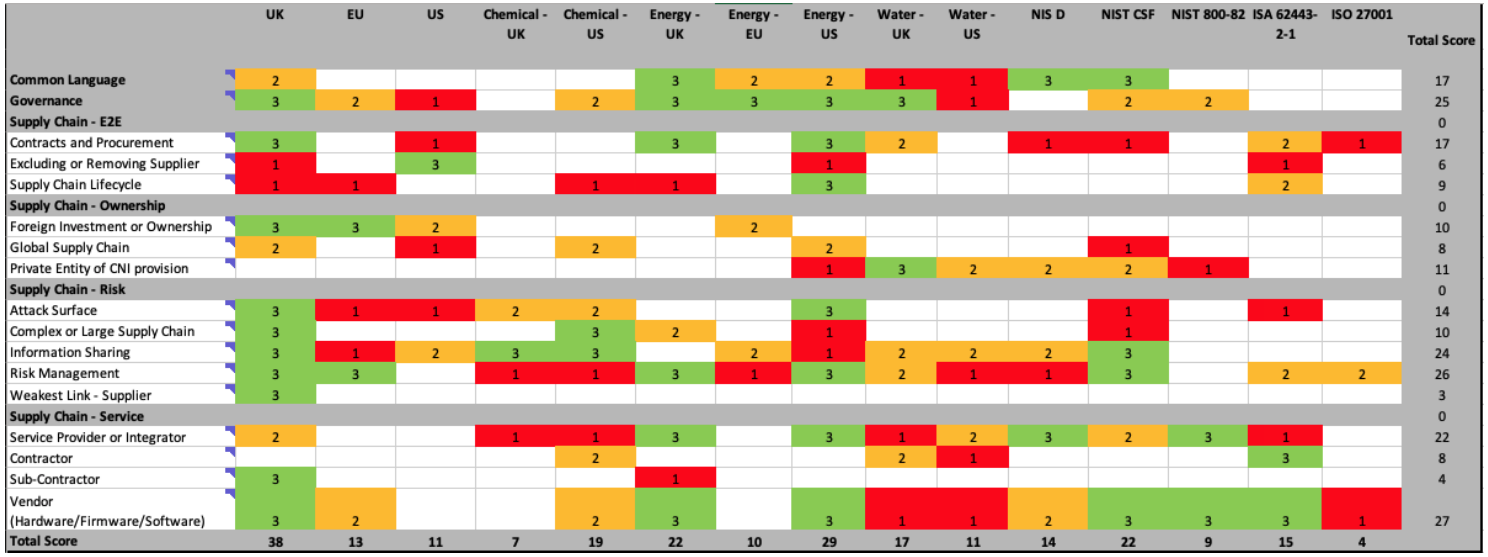
4.1. Data Analysis

Once the coding is completed, the data is subdivided into the following subject Areas of Interest (AOI):

1. Authorities (UK, US, EU)
2. CNI Sectors (Chemical, Energy, Water)
3. Frameworks (Standards, Guidance, Frameworks, and Regulations)

The coded data is analysed and assessed for quality of advice and guidance given by the AOIs pertinent to the specific coded category. This is depicted by coloured cells in Figure 1. The categories are represented along the Y axis and the AOI along the X axis.

Figure 1 uses a Red, Amber, Green (RAG) traffic light assessment heuristic. This is commonly used in many areas, such as within industry for program management [4], for assessing risk in the



	UK	EU	US	Chemical - UK	Chemical - US	Energy - UK	Energy - EU	Energy - US	Water - UK	Water - US	NIS D	NIST CSF	NIST 800-82	ISA 62443-2-1	ISO 27001	Total Score
Common Language	2					3	2	2	1	1	3	3				17
Governance	3	2	1		2	3	3	3	3	1		2	2			25
Supply Chain - E2E																0
Contracts and Procurement	3		1			3		3	2		1	1		2	1	17
Excluding or Removing Supplier	1		3					1						1		6
Supply Chain Lifecycle	1	1			1	1		3						2		9
Supply Chain - Ownership																0
Foreign Investment or Ownership	3	3	2				2									10
Global Supply Chain	2		1		2			2				1				8
Private Entity of CNI provision								1	3	2	2	2	1			11
Supply Chain - Risk																0
Attack Surface	3	1	1	2	2			3				1		1		14
Complex or Large Supply Chain	3				3	2		1				1				10
Information Sharing	3	1	2	3	3		2	1	2	2	2	3				24
Risk Management	3	3		1	1	3	1	3	2	1	1	3		2	2	26
Weakest Link - Supplier	3															3
Supply Chain - Service																0
Service Provider or Integrator	2			1	1	3		3	1	2	3	2	3	1		22
Contractor					2				2	1				3		8
Sub-Contractor	3					1										4
Vendor (Hardware/Firmware/Software)	3	2			2	3		3	1	1	2	3	3	3	1	27
Total Score	**38**	**13**	**11**	**7**	**19**	**22**	**10**	**29**	**17**	**11**	**14**	**22**	**9**	**15**	**4**	

Figure 1: RAG assessment of coded data

health sector [59], and for labelling foods against the guideline daily allowance [56]. In this instance, it is used to provide a visual representation of the level of detail attributed to each AOI relating to each category. The colours are then assigned a numerical reference to allow each row and column to be given a numerical assessment in line with the colour representation. Both the colour and number provide a simple presentation of the qualitative analysis undertaken of the data and do not depict any quantitative narrative.

- Blank cell: (No coverage). No reference to the category is found in any documents.
- Red/1: (Poor coverage). Although the category is referenced, there is no detail or definition. *Example: For information sharing category Energy-US requires the timely notification of vulnerabilities to create defences of zero-day exploits, but fails to explore the wider subject within the category.*
- Amber/2: (Moderate coverage). The category is referenced and contains elements of a term or a definition. *Example: Water-UK promotes the sharing of information amongst sector stakeholders, but doesn't consider whether this extends to the supply chain.*
- Green/3: (Good coverage). A clear level of detail with defined guidance or reference to applicable third-party documentation. *Example: Chemical-US has developed this at both classified and unclassified levels whilst collaboratively developing a new information sharing and analysis centre for public and private sectors.*

The visual and numerical representation allows for a very high-level assessment of the categories and where the AOIs concentrate their advice and guidance.

4.2. Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks

To approach the principle aim of the title, we focus on the three supplementary questions listed in the Introduction, namely:

1. What is meant by Supply Chain?
2. What are the contrasting views and guidance of the authorities and sectors?
3. Do standards provide cohesive coverage?

These supplementary questions introduce subordinate questions during analysis and an interdependence becomes apparent as categories and relationships developed.

Table 2 represents the supply category coverage of the 15 AIOs represented in the RAG table in Figure 1 and also identifies those sectors that provide good (Green) or medium (Amber) levels of detail.

4.3. What is meant by Supply Chain?

Diverse Interpretations of supply chain can undermine risk management programs
Analysis demonstrates contrasting perspectives of what constitutes the supply chain beyond the generally accepted norm of products and services. There are multiple interpretations of the term "Supply Chain" and this divergence of understanding can lead to gaps in cyber security strategies appreciating potential risks and thereby excluding the opportunity to mitigate them. Risk Management received good coverage, but that can only manage acknowledged areas of risk. Organisations are encouraged to implement a C-SCRM program, but may be unsighted to certain elements that constitute the wider supply chain categories. They may have a competent program that only covers a subset of the overall supply chain and these gaps in awareness and subsequent lack of risk management introduce vulnerabilities that threat actors can exploit to circumvent the controls in place.

4.3.1. Service

The interpretation of the supply chain at its more obvious levels is captured under "Service" and incorporates the **Vendor**, which corresponds to how we label the material components within the supply chain. This encapsulates the physical *Hardware*, but also the *Firmware* and *Software* that resides within it. This category receives wide and detailed framework coverage, with good sector coverage that varied in the level of detail offered. There is a general acceptance that the hardware asset is normally supplied and not built in-house. Consequently there is a reliance on the third-party for the provision of this. This brings in the **Service Provider** or **Service Integrator** as a key component of the supply chain, receiving similar levels of framework and sector coverage, with Energy-UK/US being consistently strong for both, and the other sectors less so. **Contractor** and **Sub-contractor** receive less coverage, but potentially play an important role within C-SCRM. This is especially relevant when considering whether to allow suppliers to sub-contract services and the controls required to manage any subsequent risk.

What is apparent in this whole category is the limited coverage from the EU (Vendor was the only category noted) and from the US documents assessed, which provided no reference to any of the categories. We observe the same practice in the Energy-EU sector.

4.3.2. End-to-End

Whether to allow sub-contracting would be covered during the **Contracts and Procurement** process and although not supply chain per se, it is an important aspect towards understanding and managing C-SCRM that is well considered by the UK authority and, again, by the Energy-UK/US sectors. **Supply Chain Lifecycle** represents the process of commissioning, through-life management, and decommissioning of the products and services. What coverage it does receive largely offered little detail or definition, with the exception of Energy-US that provides a clear level of detail of baking cyber security into implementation and onward support phases of the product lifecycle. Closely aligned to decommissioning is the **Exclusion or Removal of Suppliers** which, like the Supply Chain Lifecycle, receives little coverage but does receive detailed attention with the US Secure Technology Act [67].

4.3.3. Ownership

Foreign Investment or Ownership receives the most detailed authority coverage of all the categories, but is largely ignored by the sectors and frameworks. Conversely, **Private Entity of**

CNI Provision receives better representation by the Water-UK/US sectors and by the most current frameworks, but is ignored at authority level and by the other sectors. Every region and every sector has an increasing reliance on the **Global Supply Chain** which is only recognised to any level of detail by the Chemical-US and Energy-US sectors and by the UK authority.

4.3.4. Risk

Given that the principle question focuses on C-SCRM, we also consider the **Attack Surface** to find guidance on the threat vectors that attackers may adopt to comprise an organisation via the trust in the supply chain. This is well represented by UK authorities (which deliveres detailed coverage in all the Risk sub-categories) and Energy-US documents analysed, and also receives a good level of coverage by the available Chemical sectors. The increasingly **Complex or Large Supply Chain** only receives sector coverage from the Chemical-US and Energy-UK sector (Energy-US touched upon it), whilst consideration of whether the **Weakest Link is the Supplier** is only considered by the UK Authority. **Information Sharing** is widely represented, with all authorities and most sectors covering it to some degree and, again, by the most current frameworks. Unsurprisingly, **Risk Management** receives the widest coverage of all the categories although the level of detail varies amongst sectors with Energy-UK/US standing out for the quality of their documents. The US authority documents analysed does not cover this specific to the supply chain, although the NIST CSF does provide detailed coverage.

4.4. What are the contrasting views and guidance of the sectors and authorities?

A lack of common guidance negatively impacts clients and suppliers alike
Comparing the guidance of the national authorities and the individual CNI sectors, it is apparent that there is more variance than commonality. The level of detail and coverage of advice offered by sectors varies and, although the UK and US offer similar guidance within the Energy sector, the differences within the other two sectors analysed supports the conclusion that common guidance is limited across the sectors or similarly offered centrally by the authorities.
This variation provides challenges to sectors where advice may be lacking, whilst the supply chain and vendors are impacted if their global customer base receives conflicting advice that has implications of the type and level of service or product they supply.

4.4.1. Authority guidance

At a higher authority level, the **UK** covers most of the categories with a good level of detail, whilst both the **US** and the **EU** provide less coverage. The EU does cover *Foreign Investment and Ownership* and *Risk Management* to a good level of detail, as well as covering *Vendor* to a moderate level of detail, whilst the US gives a lot of detail in the removal or exclusion of suppliers, and also covers off *Foreign Investment and Ownership* and *Information Sharing* to a moderate level of detail. This is likely due to the different purposes and governance models of the two countries and of international organisations. The EU and US drive legislative requirements as GDPR [30] and the NIS Directive [31] can testify for the EU and the Security Technology Act [67] for the US. The EU defers adoption and guidance down to the member states (including the UK when it was a member state), whilst the US may defer to state and sector level or rely on NIST for delivery of frameworks[6].

[6]The creation of CISA in November 2018 and the product they deliver will likely improve the US Authority coverage and depth of guidance and is noted within section 3.4 Limitations

4.4.2. Sector Guidance

The guidance offered at a sector level is also variable. The Energy sector performs well with **Energy-US** providing the greatest level of output both in terms of coverage and the quality of information, whilst **Energy-UK** is similarly covered in both criteria. They both provide good detailed coverage around *Governance*, *Contracts and Procurement*, *Risk Management*, *Service Provider or Integrator*, and *Vendor*, as well as an appreciation of the *Global Supply Chain*. The **Energy-EU** sector fairs less well and although *Governance* is covered to the same level of detail, there is little other commonality. It does however address *Foreign Investment or Ownership*, which the other two fail to cover, and also provides better coverage of *Information Sharing*. While the UK and the US are closely aligned for Energy, there was a marked difference in the other two sectors. In the Chemical sector **Chemical-US** performs well against **Chemical-UK** when it comes to the sector specific advice provided by the respective government and other authorities, whereas the converse is found with the Water sector, which sees little coverage provided for **Water-US** when compared with the advice available to its sector peer **Water-UK**.

4.5. Do frameworks provide cohesive coverage?

C-SCRM is included in recent releases, but a common taxonomy is still absent
Government, regulatory, sector, or industry specific objectives or guidance may influence which frameworks are adopted within specific CNI Sectors. Frameworks analysed continue to demonstrate a disconnect when it comes to the management of cyber risk of the supply chain. The disparity in coverage and detail of the supply chain categories identified in our research suggests that there is currently no single framework that would support a detailed C-SCRM program.
Recent frameworks such as the NIS Directive and the most recent version of the NIST CSF do introduce cyber security of the supply chain, but are not aligned and cover different categories to various levels of detail. This observation underlines the risk that organisations may be ignorant of risks that are not explicitly considered within specific frameworks. This is born from a lack of harmonisation of frameworks, that would be complemented with an agreed common taxonomy.

Having established that there is little commonality amongst either the authorities or the sectors in what and how they promote cyber security and risk management of the supply chain, we look to the frameworks that are commonly referenced to establish whether there is a synergy in any of these. Our high-level analysis establishes that the category **Framework** is widely referenced, with Chemical-UK the only AOI to not consider it. This is an important observation as it evidences that sectorial guidance often involves the adoption of frameworks, validating this analysis. The **NIS Directive** [31] is often referenced by UK and EU organisations, whilst **NIST CSF** [50] is the "go to" reference for many US organisations and appears to offer a better level of coverage and detail of the categories. **NIST 800-82** [60] is specific to Industrial Control Systems (ICS) and is referenced by a smaller subset of US organisations, whereas ISA 62443 is another standard specific to ICS, but is more widely referenced on both sides of the Atlantic, with **ISA 62443-2-1** [2] repeatedly mentioned and, although it is a much older document, has wider coverage of the categories than the newer NIS Directive. Finally, **ISO 27001** [38] is a document that is frequently stated as the required standard to attain for both IT and OT environments, but this isn't reflected when looking to deliver a C-SCRM program[7].

[7] ISO 27001 only really offers any meaningful guidance for *Risk Management*

Supply Category	Coverage/15	Green/3	Amber/2
Contract/Procurement	9	Energy-UK, Energy-US, UK	Water-UK, 62443-2-1
Exclude/Remove Supplier	4	US	
Supply Chain Lifecycle	6	Energy-US	62443-2-1
Foreign Investment/Owner	4	UK, EU	Energy-EU, US
Global Supply Chain	5		Chemical-US, Energy-US, UK
Private Entity of CNI	6	Water-UK	Water-US, NIST CSF, NIS D
Attack Surface	8	Energy-US, UK	Chemical-UK, Chemical-US
Complex Supply Chain	5	Chemical-US, UK,	Energy-UK
Information Sharing	11	Chemical-UK, Chemical-US, UK, NIST CSF	Energy-EU, Water-UK, Water-US, US, NIS D
Risk Management	13	Energy-UK, Energy-US, UK, EU, NIST CSF	Water-UK, 62443-2-1, ISO 27001
Weakest Link - Supplier	1	UK	
Service Provider	11	Energy-UK, Energy-US, NIS D, NIST 800-82	Water-US, UK, NIST CSF
Contractor	4	62443-2-1	Chemical-US, Water-UK
Sub-Contractor	2	UK	
Vendor	12	Energy-UK, Energy-US, UK, NIST CSF, NIST 800-82, 62443-2-1	Chemical-US, EU, NIS D

Table 2: Supply Category Coverage

4.5.1. Service

This category exemplifies the lack of full coverage by any specific framework or of any individual category. *Vendor* receives good coverage by most frameworks, whilst the NIS Directive offers moderate coverage and ISO 27001 is poorly represented. *Service Providers* come under the NIS Directive if they provide a digital service[8] and references additional security measures, whilst NIST 800-82 provides good advice around *Service Integrator* and also introduces the role of Managed Security Service Providers. ISA 62443-2-1 provides limited coverage in this category, but is the only framework to consider *Contractors*, providing good coverage and requiring them to be part of the overall security structure and included in training and policy awareness. None of the frameworks considers the role of *subcontractors*.

4.5.2. End-to-End

ISA 62443-2-1 is the only framework that covers this category in any extensive detail. NIS Directive and NIST CSF requires compliance of security measures be undertaken through *Contractual* obligations, but relies on others to provide appropriate guidance. ISA 62443-2-1 offers greater detail for cyber security requirements during *Procurement* as well as having contracts to support business continuity, especially for products that have a long lead-in time. It is also the only framework that considers the timely *Removal of supplier* access at the conclusion of contracts, as well as being the only one to include the *Supply Chain Lifecycle*.

4.5.3. Ownership

Similarly, *Foreign Investment or Ownership* is underrepresented by the frameworks, suggesting that it resides with the Authorities to address. NIST CSF does broach upon supply chains being complex, globally distributed, and interconnected, but leaves the detail there. Both it and the NIS Directive do however provide moderate coverage of *Private Entities of CNI Provision* and provide similar requirements for the needs of all stakeholders to be considered.

4.5.4. Risk

This category is where the NIST CSF outperforms the other frameworks. Together with ISA 62443-2-1, it provides a simple consideration for the increased *Attack Surface* that is brought about by increased interconnected environment, which it also aligned to the global distribution of resources and processes within the supply chain. The Framework within NIST CSF assesses against different levels of competence to judge how an organisation *Shares Information* and collaborates with others, stipulating that communication is especially important among stakeholders up and down the supply chain. This is a similar approach that NIS Directive promotes, but the NIS CSF actually has the Framework to assess against, whilst NIS Directive relies on the member states to determine how that is undertaken [24].

When approaching *Risk Management*, the NIS Directive urges for risk mitigation controls to be proportionate to the size and role of the organisation assessed. ISA 62443-2-1 requires external suppliers that have an impact on the security of an organisation to be held to the same security policies, and for these to be extended to subcontracted entities. ISO 27001 Clause 15 specifically deals with supplier relations that the business has to evidence but, like ISA 62443-2-1, there is no actual guidance. NIST CSF version 1.1 introduced a new category on C-SCRM and this goes

[8]NIS confines this to 3 types of service; *Cloud, Online Market Places, and Search Engines*

into a great level of detail, utilising the Framework to understand and document risks associated with products and services. C-SCRM criteria was also added to the implementations tiers, whilst a special category has been added to the Framework core.

5. Discussion

Our analysis provides evidence that there is currently no simple textbook answer that offers an authoritative reference to what the supply chain consists of or the optimum approach to implementing a C-SCRM program. This inconsistency is born from a disparate view of cyber security controls as a whole and where the management of the supply chain risk should be administered and maintained.

This inconsistency is driven by what components the supply chain is considered to comprise of, but is also influenced by geographical location, the CNI sector that the business resides within, and the framework they utilise for their supply chain risk management program.

5.1. Do we need a common taxonomy?

Our thematic analysis evidences the lack of a common taxonomy for supply chain procurement and risk management that puts strain on both the supplier and the client. The supplier may have to satisfy clients from diverse sectors that are receiving contrasting advice, introducing a resource overhead on that service delivery. The client, on the other hand, may not have access to the most suitable guidance or may create ad hoc C-SCRM processes.

The analysis of the data within the documents listed in Table 1 provides the four categories represented in Figure 2 capable of forming the bedrock of a C-SCRM taxonomy.

5.1.1. C-SCRM Outline Taxonomy

The four C-SCRM categories within Figure 2 are further divided into sub-categories that represent the results shown in Figure 1. That data analysed is then used to derive more granular attributes beneath those sub-categories.

- **Ownership:**

  Controls pertaining to foreign investment or ownership is likely to be driven at an authority or regulatory level and influenced by political or threat assessments. The risk grows with the globalisation of the supply chain with trust being exponentially diluted as the visibility and control of the supply chain diminishes beyond national boundaries.

  Operators within the CNI sectors are often comprised of private sector organisations of various sizes and ownership types, including being foreign owned or part of a global organisation. Their business priorities are different to those of public sector organisations and an appreciation of this needs to be understood at all stages of the contract.

- **Risk:**

  The globalisation of the supply chain adds to the overall complexity, which is a sub-category here. This exposes the attack surface by introducing potential threats outside the traditional business boundary that is part of the wider risk management criteria that traverses all four categories. Information sharing captures detail about suppliers that may influence decisions during the procurement process and throughout the life of the contract. It also refers to sharing of best practice and threat intelligence to suppliers to ensure their protection and, by association, that of the organisation.

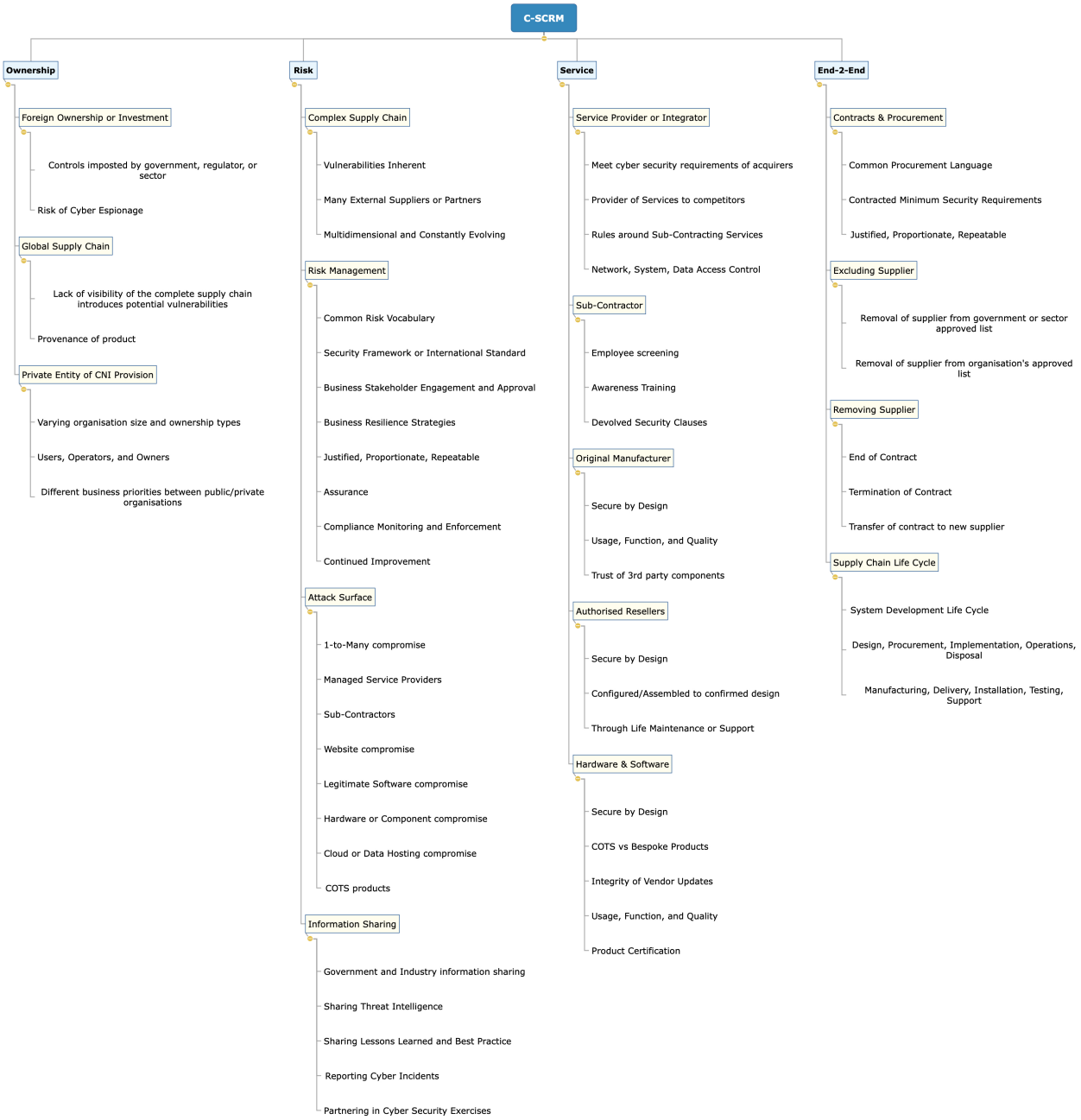


Figure 2: C-SCRM Outline Taxonomy

- **Service:**

  Outsourcing to a service provider or integrator requires security requirements to be articulated and understood. They may provide services to competitors, so separation of duties and access control is a consideration. They are also a component of the wider attack surface, especially as threat actors may look to target an organisation in the supply chain, or focus on a 1-to-many compromise over a 1-to-1 strategy. The reward of compromising many organisations upstream by focusing on a specific vendor or service provider within the supply chain is an attractive proposition to the threat actor. Hardware and Software are also covered in this category (and are also included in the attack surface considerations), whilst the relationship between client and supplier has been further defined as an engagement with the original manufacture or via an authorised reseller.

- **End-2-End:**

  Baking security requirements into the contract during procurement to ensure that minimum security standards are understood, whilst also accepting that such security requirements are fit for purpose. Adopting a common procurement language is beneficial and this extends to the whole lifecycle from initial design and procurement through the stages to product disposal at the end or termination of a contract. Some suppliers may be excluded from the approved list for a number of reasons at a government, sector, or organisation level.

The requirement for a common taxonomy is an underlying theme, both for the ability to communicate risks throughout the supply chain, and for a standard procurement approach that supports the end-to-end supply chain lifecycle. This would enable organisations to proactively introduce risk mitigation controls to cyber security related dependencies and vulnerabilities.

Such a taxonomy will enable both efficient and collaborative enhancements through the delivery of an agreed vocabulary of C-SCRM business concepts that is repeatable and authoritative. This requires involvement from all stakeholders to resolve the agreed terminology and a governance wrap to manage and maintain it.

Our research indicates that such stakeholder agreement would be challenging with varying technologies, sectors, motivations, priorities, regulations, regions, and political influences at play. There are financial incentives for finding a common approach, but there is also effort required and likely compromises to be made in order to reach that objective.

5.2. Harmonisation of frameworks

Repeated comments within the sampled documents to harmonise frameworks also supports this need for commonality. This would deliver a baseline that organisations and suppliers can aim towards, with the understanding of sector specific nuances that would need to be applied on top of this foundation level of assurance.

It may be that one-size doesn't fit all though. The CNI sectors provide very different services. They are publicly and privately owned and operated and come in various sizes. Some are foreign owned, whilst others are international companies working in multiple regions. Many rely on ICS to delivery their product and ICT to support the business and engage with the customer base. Their supply chain will likely be complex and global. It will be made up of the traditional vendor solutions and the wider supply chain components detailed in this paper. Some will have constraints placed upon them by their regulator, whilst others will have more flexibility in choosing their supplier and their levels of assurance.

Suppliers provide various solutions and services, often for multiple customers. Vendor solutions may be bespoke or COTS products with their own standards and regulations and may be national or international organisations in their own right. They may provide their product to multiple organisations within the same CNI sector, to multiple CNI sectors, and to organisations in other sectors or countries. Therefore, as businesses consider moving towards COTS solutions, cloud-based services, and automation, the ability to insist on contractual obligations may become compromised.

There may be other aspects that are not suitable for frameworks to cover, such as foreign investment or ownership that will likely sit better at a central authority level as this research indicates.

It is with this backdrop that the implementation of guidance at either an authority or sector level is challenging. Our research finds that some sectors fare better than others, with all focusing on some areas of the supply chain categories, but none on all of them. Our analysis identifies commonality in the quality and type of guidance offered by the UK and US Energy sectors, but national discrepancies within the other two sectors.

Given the repeated desired outcome for a harmonisation of standards, efforts currently happening on both sides of the Atlantic may help drive this forward. The NCSC has recently developed a CNI Hub [53] to provide advice and guidance for stakeholders in both the public and private sector CNI, whilst CISA recently produced their SCRM Essentials [15] for ICT. The strong relationship between these two organisations that extends to other international partnerships may provide the impetus needed. There is currently no equivalent EU guidance, although ENISA recently shone a light on supply chain cyber security with their guidelines for the Internet of Things (IoT) [25]. Collaboration to bring together disparate programs under a communal banner can advance the collective objective.

5.3. Mapping the C-SCRM Taxonomy

The discussion above highlights the appetite for a baseline C-SCRM framework to satisfy the varying needs and demands of companies, industries, sectors, regulators, and governments. A common and successful approach often begins in the form of an "Essentials" document, which is a very high-level requirement and an approach used to good effect by both NCSC and CISA[9].

We map the *CISA ICT SCRM Essentials* [15] and the *NCSC Principles of Supply Chain Security* [20][10] products against the initial C-SCRM taxonomy in figure 2 and find alignment (figure 3) at a sub-category level that bodes well for a common ground to take forward. The bold ticks indicate that the sub-category is referenced, whilst the clear ticks indicate that it is not evident in the referenced paper, but is covered by supplementary documents[11] within the organisation (NCSC or CISA). Where this is not the case, a cross is used to show that no reference is observed. We then provide more detailed alignment to the specific attributes within the sub-categories that can be found in Figure 4.

Figure 3 indicates the levels of coverage of the sub-categories within the C-SCRM. However, using the detail in figure 4 to drill down further and investigate the coverage of the attributes within those categories, we see gaps begin to appear.

Both organisations require suppliers adhere to a contracted minimum level of security standards. NCSC recommends that these are proportionate, whilst CISA suggests the use of an approved

[9]NCSC created Cyber Essentials, whilst CISA has recently published ICT SCRM Essentials

[10]This was published jointly with the Centre for the Protections of National Infrastructure (CPNI)

[11]CISA ICT Supply Chain Risk Management report[14]. NCSC CNI Hub [53]

C-SCRM	NCSC	CISA
End-2-End		
Contracts & Procurement	✓	✓
Excluding Supplier	⊗	✓
Removing Supplier	✓	⊗
Supply Chain Life Cycle	✓	✓
Ownership		
Foreign Investment or Ownership	✓	⊗
Global Supply Chain	⊗	✓
Private Entity of CNI Provision	✓	✓
Risk		
Complex Supply Chain	✓	⊗
Risk Management	✓	✓
Attack Surface	✓	✓
Information Sharing	✓	✓
Service		
Service Provider or Integrator	✓	✓
Sub-Contractor	✓	✓
Original Manufacturer	✓	✓
Authorised Resellers	⊗	✓
Hardware & Software	✓	✓

Legend:
- ✓ Referenced in the document
- ⊗ Not Observed
- ✓ Referenced elsewhere by the organisation

Figure 3: C-SCRM Alignment

supplier list (which is a more palatable than calling it an exclusion list). NCSC has good coverage around the removal of suppliers at the end or termination of a contract and how that may be transferred to a new supplier but, although they reference the supply chain lifecycle, they don't cover any of the attributes. CISA does, albeit not within the analysed document.

The concept of ownership and the sub-categories of it are not addressed in either paper and, although both address it in other documents, the attributes they cover are not aligned.

As one would expect with C-SCRM, risk is a category that is well covered, at least with regards to risk management. Both recommend alignment with industry standards and best practice. CISA points to NIST, without specifying any particular product, whilst NCSC highlights ISO 28000 and the Government Supplier Framework [65]. Both consider the complexity of supply chains. CISA was particularly keen to promote representation from multiple parts of the organisation when defining the SCRM program and to promote it as a business priority, whilst NCSC instead put value in information sharing. This included sharing information within the business of suppliers who continually fail to meet security or performance expectations, but also the positive aspect of the sharing of threats, vulnerabilities and best practice across the supply chain. They set out requirements for reporting security incidents and that organisations may assist and support suppliers where security incidents have a potential to affect their business or the wider supply chain. The propagation of lessons learned to all suppliers was also recommended.

Service is a C-SCRM category that looks good in Figure 3 but, when focusing on the attributes, a different picture emerges. Both have strong coverage around service provision and the need for cyber security requirements of providers and integrators. Both appreciate that services may be further sub-contracted by suppliers and NCSC recommends contracting what can be outsourced and ensuring that security requirements are flowed down. Both papers touch upon hardware and software with regards to vulnerabilities and being part of the attack surface, but neither addresses

any of the attributes for this or with regards to the original manufacturer or authorised resellers, although CISA does cover elements of this elsewhere.

What this mapping of the C-SCRM taxonomy down to an attribute level shows is that although there is commonality between CISA and NCSC documents, there are also differences in the attributes on which they concentrate. There are also significant gaps. Some of these are addressed in different products within the organisation, but there are also significant areas that are missing entirely. Further research will be required to determine whether these gaps are important, but as these attributes are derived from data extracted from the body of researched documents, it would suggest that they are valid and require addressing.

C-SCRM	NCSC	CISA
End-2-End		
Contracts & Procurement	●	●
Common Procurement Language	⊗	⊗
Minimum Security Requirements	●	●
Justified, Proportionate, Repeatable	●	⊗
Excluding Supplier	⊗	●
From Government Approved List	⊗	⊗
From Organisation's Approved List	⊗	●
Removing Supplier	●	⊗
End of Contract	●	⊗
Termination of Contract	●	⊗
Transfer of contract to new supplier	●	⊗
Supply Chain Life Cycle	●	✓
System Development Life Cycle	⊗	✓
Design, Procurement, Implementation, Operations, Disposal	⊗	✓
Manufacturing, Delivery, Installation, Testing, Support	⊗	✓
Ownership		
Foreign Investment or Ownership	✓	⊗
Controls imposed	✓	⊗
Risk of Cyber Espionage	⊗	⊗
Global Supply Chain	⊗	✓
Lack of visibility of vulnerabilities	⊗	✓
Provenance of product	⊗	✓
Private Entity of CNI Provision	✓	✓
Organisation Size and ownership type	⊗	✓
Users, Operators, and Owners	⊗	✓
Different Business Priorities	⊗	⊗
Risk		
Complex Supply Chain	●	●
Vulnerabilities Inherent (by proxy)	●	✓
Multiple External Suppliers or Partners	●	●
Multidimensional & Constantly Evolving	✓	⊗
Risk Management	●	●
Common Risk Vocabulary	⊗	●
Security Framework or Standard	●	●
Business Stakeholder Approval	⊗	●
Business Resilience Strategies	●	●
Justified, Proportionate, Repeatable	●	⊗
Assurance	●	●
Compliance Monitoring & Enforcement	●	●
Continued Improvement	●	⊗
Attack Surface	●	✓
1-to-Many compromise	●	✓
Managed Service Providers	✓	⊗
Sub-Contractors	●	⊗
Website compromise	●	⊗
Legitimate Software compromise	●	✓
Hardware or Component compromise	⊗	✓
Cloud or Data Hosting compromise	●	⊗
COTS Products	⊗	⊗
Information Sharing	●	✓
Government & Industry info sharing	●	✓
Threat Intelligence	●	✓
Lessons Learned & Best Practice	●	✓
Reporting Cyber Incidents	●	⊗
Partnering in Cyber Security Exercises	⊗	✓
Service		
Service Provider or Integrator	●	●
Meet Cyber Security Requirements	●	●
Provider of Services to competitors	⊗	⊗
Sub-Contracting Services	●	●
Network, System, Data Access Control	●	●
Sub-Contractor	●	●
Employee Screening	●	⊗
Awareness Training	●	⊗
Devolved Security Clauses	●	⊗
Original Manufacturer	●	✓
Secure by Design	⊗	✓
Usage, Function, and Quality	⊗	✓
Trust of 3rd party components	⊗	✓
Authorised Resellers	⊗	✓
Secure by Design	⊗	⊗
Configured/Assembled to agreed design	⊗	⊗
Through Life Maintenance or Support	⊗	⊗
Hardware & Software	●	●
Secure by Design	⊗	⊗
COTS vs Bespoke Products	⊗	⊗
Integrity of Vender Updates	⊗	✓
Usage, Function, and Quality	⊗	⊗
Product Certification	⊗	⊗

Legend:
- ● Observed in the document
- ⊗ Not Observed
- ✓ Provided elsewhere by the organisation

Figure 4: C-SCRM Attributes

5.4. Baseline C-SCRM Framework

There is a need for a common best practice that will allow a baseline for C-SCRM to deliver a more informed choice at a sector and organisational level.

Such an approach would promote the introduction of a common taxonomy and agreement on what constitutes the cyber supply chain, allowing further research into a baseline framework that satisfies many of the requirements, with individual refinement at a local, regional, or sector level.

Such a baseline framework, be it delivering common best practice guidance or a more detailed document set, should consider the supply chain categories identified within this work and look beyond the obvious product and service provision. Each category has good coverage from at least one AOI[12], whilst two recent frameworks analysed provide a solid foundation. The NIS Directive and, in particular, the NIST CSF have delivered on some key categories, but there are still gaps and NIST references out to other globally recognised frameworks whilst recognising the need to continually adapt the CSF to align with best practices.

Once a baseline is produced, a common processes for measuring degrees of adoption must be considered. There are established ways to assign metrics within the frameworks. NCSC has provided the Cyber Assessment Framework (CAF) to enable CNI sectors to show conformity with the NIS Directive, whilst the NIST CSF has a framework core and associated tiers to deliver such metrics as common best practice.

What rests within a framework and what is the responsibility of individual authorities needs to be addressed. *Foreign investment and ownership* would appear to sit with political authorities, whilst cyber security *procurement* guidance is quite well defined by the UK and US energy sectors and these may provide a suitable opportunity to merge and replicate out to other sectors.

6. Conclusion

The supply chain is being increasingly targeted by threat actors to take advantage of the client/supplier trust to compromise their intended victim organisation(s) via third-party risk. CNI sectors are at particular risk of attack by threat actors. The ability for organisations to conduct a comprehensive risk management program of the cyber supply chain is essential to ensure that business benefits gained from employing a global and diverse supply chain are not undermined by increasing the potential risk of compromise.

This paper focuses on the advice and guidance given to three sectors that are jointly categorised as critical national infrastructures by the UK, the US, and the EU. We scrutinised authority and sectorial C-SCRM guidance before examining frameworks that sectors were directed towards. Our detailed comparison identifies a variable understanding of what constitutes the supply chain that risk can be assessed against. This inconsistency at both authority and sectorial level promotes our conclusion that there is a requirement for a common taxonomy to support a baseline C-SCRM framework.

This research is important in underlining a recurring theme for a common taxonomy within cyber security. Our research finds that there are some significant gaps across the different sectors that should be addressed. This would be supported by a common taxonomy that permits for this coverage to be understood across different regions and authorities.

We utilise our results to create an initial C-SCRM taxonomy based on the research data. This produces four top level categories, with sub-categories and attributes that were then mapped against two relevant CISA and NCSC products. Future research will aim to validate this taxonomy leading to its evaluation and expansion.

[12] *Global Supply Chain* is the exception to this, but three AOIs do cover it to a moderate level and *Complex or Large Supply Chain* is very similar and has better coverage

This study forms the foundation to encourage future academic research into the development of a common taxonomy that can be used to create a baseline C-SCRM framework. This may be introduced through a high-level "Essentials" document that could evolve towards more detailed guidance or inclusion within established frameworks.

Our future work intends to develop and validate this initial taxonomy within C-SCRM to use as the foundation to develop a baseline framework to support systematic handling of cyber security risks in the supply chain. Consideration must be given to the competing stakeholder priorities and look to create a solution that can be broadly accepted. This will provide a rigorous discipline of C-SCRM to allow the broad cyber supply chain to be recognised and enable risks to be assessed and managed.

References

[1] American Chemistry Council. *Responsible Care Security Code Cybersecurity Guidance Chemical Sector Guidance for Implementing the NIST Cybersecurity Framework and the ACC Responsible Care ® Security Code*. Tech. rep. 2016, pp. 1–10.

[2] ANSI/ISA. *ANSI/ISA–62443-2-1 (99.02.01)–2009 Security for industrial automation and control systems. Part 2-1: Industrial automation and control system security management system*. 2009, pp. 1–237. ISBN: 978-1-934394-93-9. URL: http://isa99.isa.org/Public/Documents/ISA-62443-2-1-WD.pdf.

[3] Ashutosh Bahuguna, R. K. Bisht, and Jeetendra Pande. "Country-level cybersecurity posture assessment:Study and analysis of practices". In: *Information Security Journal* 29.5 (2020), pp. 250–266. ISSN: 19393547. DOI: 10.1080/19393555.2020.1767239. URL: https://doi.org/10.1080/19393555.2020.1767239.

[4] S. Balafif and T. Haryanti. "IT balanced scorecard (IT BSC) based strategic framework for assessing the impacts of Business Strategic-IT alignment". In: *IOP Conference Series: Materials Science and Engineering* 821.1 (2020). ISSN: 1757899X. DOI: 10.1088/1757-899X/821/1/012033.

[5] Nadya Bartol. "Cyber supply chain security practices DNA - Filling in the puzzle using a diverse set of disciplines". In: *Technovation* 34.7 (2014), pp. 354–361. ISSN: 01664972. DOI: 10.1016/j.technovation.2014.01.005. URL: http://dx.doi.org/10.1016/j.technovation.2014.01.005.

[6] BEIS. *Energy Delivery Systems - Cyber Security Procurement Guidance*. Tech. rep. 2016. URL: http://energy.gov/oe/services/technology-development/energy-delivery-systems-cybersecurity.

[7] Sandor Boyson. "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems". In: *Technovation* 34.7 (2014), pp. 342–353. ISSN: 01664972. DOI: 10.1016/j.technovation.2014.02.001. URL: http://dx.doi.org/10.1016/j.technovation.2014.02.001.

[8] Virginia Braun and Victoria Clarke. "Reflecting on reflexive thematic analysis". In: *Qualitative Research in Sport, Exercise and Health* 11.4 (2019), pp. 589–597. ISSN: 1939845X. DOI: 10.1080/2159676X.2019.1628806. URL: https://doi.org/10.1080/2159676X.2019.1628806.

[9] Peter Burnap and Awais Rashid. *Risk Management & Governance Knowledge Area. Issue 1.0*. 2019. URL: https://www.cybok.org/media/downloads/Risk-Management--Governance-issue-1.0.pdf.

[10] Cabinet Office. *Sector Security and Resilience Plans 2017*. Tech. rep. 2018, p. 23. URL: https://www.gov.uk/government/publications/sector-security-and-resilience-plans-2017-summary.

[11] Madeline Carr. "Public – private partnerships in national cyber-security strategies". In: *International affairs* 92.1 (2016), pp. 43–62. URL: https://academic.oup.com/ia/article-abstract/92/1/43/2199930?redirectedFrom=fulltext.

[12] CERT-UK. "Cyber-security risks in the supply chain". In: (2015), p. 10. URL: https://webarchive.nationalarchives.gov.uk/20160902161433/https:/www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risks-in-the-supply-chain.pdf.

[13] Yulia Cherdantseva et al. “A review of cyber security risk assessment methods for SCADA systems”. In: *Computers and Security* 56 (2016), pp. 1–27. ISSN: 01674048. DOI: 10.1016/j.cose.2015.09.009. URL: http://dx.doi.org/10.1016/j.cose.2015.09.009.

[14] CISA. *ICT Supply Chain Risk Management Fact Sheet*. Tech. rep. 2020. URL: www.cisa.gov%20https://www.cisa.gov/sites/default/files/publications/factsheet_ict-scrm_508.pdf.

[15] CISA. *Supply Chain Risk Management (SCRM) Essentials*. 2020. URL: https://www.cisa.gov/sites/default/files/publications/ict_scrm_essentials_508.pdf.

[16] Aaron Clark-Ginsberg and Rebecca Slayton. “Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards”. In: *Science and Public Policy* 46.3 (2019), pp. 339–346. ISSN: 03023427. DOI: 10.1093/scipol/scy061.

[17] Daniel.R Coats. “Worldwide Threat Assessment of the US Intelligence Community”. In: January (2019). URL: https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

[18] J Cohen. “A coefficient of agreement for nominal scales”. In: *Educational And Psychological Measurement* 20.1 (1960), pp. 37–46.

[19] Claudia Colicchia, Alessandro Creazza, and David A. Menachof. “Managing cyber and information risks in supply chains: insights from an exploratory analysis”. In: *Supply Chain Management* 24.2 (2019), pp. 215–240. ISSN: 13598546. DOI: 10.1108/SCM-09-2017-0289.

[20] CPNI. “Supply chain security collection”. In: January (2018). URL: https://www.cpni.gov.uk/system/files/documents/2e/87/Supply_Chain_Security_Collection_Jan2018.pdf.

[21] B. Craggs et al. “A reference architecture for IIoT and industrial control systems testbeds”. In: *IET Conference Publications* 2019.CP756 (2019), pp. 1–8. DOI: 10.1049/cp.2019.0169.

[22] Adrian Davis. “Building Cyber-Resilience into Supply Chains”. In: *Technology Innovation Management Review* 5.4 (2015), pp. 19–27. URL: https://doi.org/10.22215/timreview/887.

[23] DEFRA. *Water Sector Cyber Security Strategy*. Tech. rep. March. 2017. URL: https://www.gov.uk/government/publications/cyber-security-strategy-for-the-water-industry.

[24] DWI. *Drinking Water Inspectorate NIS Guidance to Water Companies*. Tech. rep. 2018, pp. 1–18. URL: http://dwi.defra.gov.uk/nis/Roles.pdf.

[25] ENISA. *Guidelines for securing the Secure supply chain for IoT*. Tech. rep. November. 2020. DOI: 10.2824/314452. URL: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot.

[26] ESCSWG. “Cybersecurity procurement language for energy delivery systems”. In: April (2014), pp. 77–79. URL: https://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf.

[27] ETSI. “TR 103 303 - V1.1.1 - CYBER; Protection measures for ICT in the context of Critical Infrastructure”. In: 1 (2016), pp. 1–18. URL: https://www.etsi.org/deliver/etsi_tr/103300_103399/103303/01.01.01_60/tr_103303v010101p.pdf.

[28] European Commission. “Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure”. In: November (2012), pp. 1–4. URL: https://ec.europa.eu/energy/sites/ener/files/documents/20121114_tnceip_eupolicy_position_paper.pdf.

[29] European Commission. *Review of national rules for the protection of infrastructure relevant for security of supply Final Report*. 2018, p. 68. ISBN: 978-92-79-70882-4. DOI: 10.2833/489902. URL: https://ec.europa.eu/energy/sites/ener/files/documents/final_report_on_study_on_national_rules_for_protection_of_infrastructure_relevant_for_security_of_supply.pdf.

[30] European Parliament. *EU general data protection regulation*. 2016. URL: https://gdpr.eu/tag/gdpr/.

[31] European Parliament. "NIS Directive". In: (2016). DOI: 10.2307/j.ctt1xhr7hq.20. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[32] European Parliament. *Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation*. 2019. URL: https://perma.cc/6ZG3-SCJW.

[33] FERC. "Revised Critical Infrastructure Protection Reliability Standards: Order No. 829". In: (2016).

[34] Tekgem Gemski. *Cyber security for industrial control & Automated Control Systems*. Tech. rep. 2018, pp. 1–17. URL: https://www.nepic.co.uk/wp-content/uploads/2018/05/NEPIC___Tekgem___IACS___Cyber___Secruity___Report___30_May___2018.v2.pdf.

[35] Abhijeet Ghadge et al. "Managing cyber risk in supply chains: a review and research agenda". In: *Supply Chain Management* 25.2 (2019), pp. 223–240. ISSN: 13598546. DOI: 10.1108/SCM-10-2018-0357.

[36] Kevin E. Hemsley and Ronald E. Fisher. *History of Industrial Control System Cyber Incidents*. Tech. rep. December. 2018, p. 37. URL: http://www.osti.gov/servlets/purl/1505628/.

[37] HSE. "Cyber Security for Industrial Automation and Control Systems (IACS)". In: (2017), Health and Safety Executive (HSE). URL: https://www.hse.gov.uk/foi/internalops/og/og-0086.pdf.

[38] ISO/IEC. *ISO/IEC 27001 2nd Edition*. Tech. rep. 2013.

[39] Omera Khan and Daniel A. Sepúlveda Estay. "Supply Chain Cyber-Resilience: Creating an Agenda for Future Research". In: *Technology Innovation Management Review* 5.4 (2015), pp. 6–12. DOI: 10.22215/timreview885.

[40] R.J Landis and G Koch. "An Application of Hierarchical Kappa-type Statistics in the Assessment of Majority Agreement among Multiple Observers Author (s): J . Richard Landis and Gary G . Koch Published by : International Biometric Society Stable URL : https://www.jstor.org/stab". In: *Biometrics* 33.2 (1977), pp. 363–374.

[41] Robert M Lee, Michael J Assante, and Tim Conway. "ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Mill Cyber Attack". In: *SANS, Industrial Control Systems* (2014), p. 15.

[42] Wenke Lee. *Malware and Attack Technologies*. Tech. rep. 2019. URL: https://www.cybok.org/media/downloads/Malware__Attack_Technology_issue_1.0.pdf.

[43] Jonathan D. Linton, Sandor Boyson, and John Aje. "The challenge of cyber supply chain security to research and practice - An introduction". In: *Technovation* 34.7 (2014), pp. 339–341. ISSN: 01664972. DOI: 10.1016/j.technovation.2014.05.001.

[44] Dimitra Markopoulou, Vagelis Papakonstantinou, and Paul de Hert. "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation". In: *Computer Law and Security Review* 35.6 (2019). DOI: 10.1016/j.clsr.2019.06.007. URL: https://doi.org/10.1016/j.clsr.2019.06.007.

[45] Rossella. Mattioli and Cédric. Levy-Bencheton. *Methodologies for the identification of critical information infrastructure assets and services : guidelines for charting electronic data communication networks.* Tech. rep. December. 2014. URL: https://op.europa.eu/en/publication-detail/-/publication/e8b32529-fae9-495c-8494-e7e6cf6e014e/language-en.

[46] NATF. "Cyber security supply chain risk management guidance". In: (2018), pp. 1–24. URL: https://www.nerc.com/pa/comp/SupplyChainRiskMitigationProgramDL/NATF%20Cyber%20Security%20Supply%20Chain%20Risk%20Management%20Guidance.pdf.

[47] NCSC. *NCSC Annual review 2018.* Tech. rep. 2018. URL: https://www.ncsc.gov.uk/news/annual-review-2018.

[48] NCSC. *The cyber threat to UK business.* Tech. rep. 2018. URL: https://www.ncsc.gov.uk/information/the-cyber-threat-to-uk-business-2017-2018-report.

[49] NERC. *CIP-013-1.* Tech. rep. NERC, 2018. URL: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf.

[50] NIST. "Cybersecurity Framework for improving critical infrastructure cybersecurity". In: (2018). DOI: https://doi.org/10.6028/NIST.CSWP.04162018. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[51] Parliament_UK. *Cyber Security of the UK's Critical National Infrastructure.* Tech. rep. 2018. URL: https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/1708.pdf.

[52] M. Elisabeth Paté-Cornell et al. "Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies". In: *Risk Analysis* 38.2 (2018), pp. 226–241. ISSN: 15396924. DOI: 10.1111/risa.12844.

[53] Deborah Petterson. *The CNI Hub goes live.* 2020. URL: https://www.ncsc.gov.uk/blog-post/cni-hub-live.

[54] Kevin Quigley, Calvin Burns, and Kristen Stallard. "'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection". In: *Government Information Quarterly* 32.2 (2015), pp. 108–117. ISSN: 0740624X. DOI: 10.1016/j.giq.2015.02.001. URL: http://dx.doi.org/10.1016/j.giq.2015.02.001.

[55] Awais Rashid et al. "Everything is awesome! or is it? Cyber security risks in critical infrastructure". In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 11777 LNCS (2020), pp. 3–17. ISSN: 16113349. DOI: 10.1007/978-3-030-37670-3{_}1.

[56] Gary Sacks, Mike Rayner, and Boyd Swinburn. "Impact of front-of-pack 'traffic-light' nutrition labelling on consumer food purchases in the UK". In: *Health Promotion International* 24.4 (2009), pp. 344–352. DOI: 10.1093/heapro/dap032.

[57] Anam Sajid, Haider Abbas, and Kashif Saleem. "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges". In: *IEEE Access* 4.March (2016), pp. 1375–1384. ISSN: 21693536. DOI: 10.1109/ACCESS.2016.2549047.

[58] Johnny Saldana. *The Coding Manual for Qualitative Researchers.* 3rd. SAGE Publications, 2015, p. 339. ISBN: 9781473902497.

[59] Gustavo Saposnik et al. "Overcoming therapeutic inertia in multiple sclerosis care: A pilot randomized trial applying the traffic light system in medical education". In: *Frontiers in Neurology* 8.AUG (2017). ISSN: 16642295. DOI: 10.3389/fneur.2017.00430.

[60] Keith Stouffer et al. "NIST Special Publication 800-82 Revision 2 - Guide to Industrial Control Systems (ICS) Security". In: *NIST Special Publication 800-82 rev 2* (2015), pp. 1–157. DOI: http://dx.doi.org/10.6028/NIST.SP.800-82r1. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[61] U.S. Department of Homeland Security. *Chemical Sector Cybersecurity Framework Implementation Guidance.* Tech. rep. 2015, pp. 1–37.

[62] U.S. Department of Homeland Security. "Emergency Services Sector-Specific Plan: An annex to the NIPP 2013". In: (2015), pp. 1–42. URL: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-chemical-2015-508.pdf.

[63] U.S. Department of Homeland Security. "Risk-Based Performance Standards Guidance (CFATS)". In: May (2009), pp. 1–194.

[64] U.S. Department of Homeland Security. *Water and Wastewater Systems Sector-Specific Plan.* Tech. rep. 2015, pp. 1–56. URL: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf.

[65] UK cert. *Supplier Assurance Framework: Good Practice Guide Version History.* Tech. rep. May. 2018.

[66] US Govermnent. *Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014.* 2014. URL: https://www.govinfo.gov/app/details/PLAW-113publ254/summary.

[67] US Govermnent. "SECURE Technology Act". In: 1 (2018), pp. 1–185. URL: https://www.govinfo.gov/app/details/PLAW-115publ390.

[68] Rishi Vaidya. *DCMS Cyber Security Breaches Survey 2019.* Tech. rep. 2019. DOI: 10.1016/s1361-3723(20)30037-3. URL: www.gov.uk/government/statistics/cyber%20security-breaches-survey-2019.

[69] Water UK. *Cyber security principles for the water industry.* Tech. rep. 2017. URL: https://www.water.org.uk/news-water-uk/latest-news/cyber-security-principles-water-industry.

[70] David E. Whitehead et al. "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies". In: *70th Annual Conference for Protective Relay Engineers, CPRE 2017* (2017). DOI: 10.1109/CPRE.2017.8090056.

[71] Colin Williams. "Security in the cyber supply chain: Is it achievable in a complex, interconnected world?" In: *Technovation* 34.7 (2014), pp. 382–384. ISSN: 01664972. DOI: 10.1016/j.technovation.2014.02.003.

[72] Claes Wohlin. "Guidelines for snowballing in systematic literature studies and a replication in software engineering". In: *ACM International Conference Proceeding Series* (2014). DOI: 10.1145/2601248.2601268.

[73] Derek Young et al. “A framework for incorporating insurance in critical infrastructure cyber risk strategies”. In: *International Journal of Critical Infrastructure Protection* 14 (2016), pp. 43–57. ISSN: 18745482. DOI: 10.1016/j.ijcip.2016.04.001. URL: http://dx.doi.org/10.1016/j.ijcip.2016.04.001.