Shifting from Information Security towards a Cybersecurity Paradigm

Dr. Abraham Althonayan
Brunel Business School, Brunel University London, Kingston Lane,
Uxbridge, Middlesex, UB8 3PH, UK
Abraham.Althonayan@brunel.ac.uk

Alina Andronache
Brunel Business School, Brunel University London, Kingston Lane,
Uxbridge, Middlesex, UB8 3PH, UK
Alina.Andronache@brunel.ac.uk

ABSTRACT
The richness of terminologies in the field of Information Technology (IT), Information Security (IS) or cyber-related risks is advantageous. However, when the theoretical legacy varies between different definitions and meanings for the same term, it creates confusion and value is lost. This paper introduces the inconsistency and problems that arise when overcoming discrepancies in cybersecurity terminology; inconsistency and problems that lead to misunderstanding and misuse. This, in turn, renders insecurity for organisations. Derailing from true meaning affects the type of control in place and directly impacts on cybersecurity scope, derivations, meanings and respectively, implementation.

The authors of this paper argue that the use of a unified terminology fosters additional value and empowerment, enhancing risk oversight (countermeasures and safeguards). Therefore, as a response to the ensuing confusion, this paper explores the determinants of interchangeable terminology and meanings, and it analyses the nature of theoretical legacy as well as detrimental internal and external organisational factors. It does so with the purpose of identifying and clarifying the cause and effects of the confusion. This paper shall contribute to clarifying the scope of cybersecurity, derivation, and meanings based on a systematic literature review of prior studies.

CCS Concepts
• Computer and Information Science Education→Information System→Computer science education→Literacy.

Keywords
Cybersecurity; Information Technology; Information Security; Conceptual Shift.

1. INTRODUCTION
Cybersecurity has evolved and undergone various phases over the years, resulting in a granular theoretical legacy that currently needs to be unified in order to foster further beneficial theory and applicability. Perhaps of more concern is that many organisations use a variety of terminology to articulate cyber and IT-related risks. Some organisations use cybersecurity merely for the sake of appearance, reputation or obligated compliance without much thought about the latest jargon. Whether the granularity of the cybersecurity legacy has effects within theory and practice or not, organisations need to embark on a paradigm shift. Based on this approach, cybersecurity is found to be significantly associated with Information Security [1]. It is often debated whether information security is the same as cybersecurity or if cybersecurity represents only a subset of IS [1]. Until the present, there has been little agreement on what constitutes cybersecurity. While cybersecurity is a growing field, the drawbacks of using disconnected terminology are sustained by inherited legacy, independent variables, various interpretations and excessive business-related interests.

Specifically, literature suggests that certain consequences of misaligning terminology exist in detriment to achieving business objectives. Understanding the long-term effects and implications of cybersecurity paradigm ambiguity regarding meanings and terminologies is of utmost importance if to be properly understood and applied [2]. In the context of organisational risk oversight, there are numerous examples of a specific term being used differently depending upon the organisation's philosophy behind the term. The most used yet differently defined terms are as follows: 'information technology security', 'information assurance', 'information security', 'computer security', 'digital security', 'Internet security', 'electronic security', 'cyber security' or 'cyber-security'. Indeed, all of these terms are related to cybersecurity, but the terms are not necessarily synonyms [2], [3].

Variation in terminology and meanings in literature can generate confusion and continue to support the misuse of terms. Lack of standardisation in terminology and meanings leads to ambiguity (despite literature having some points in common; namely, cyberspace, technology [2], information, and the cornerstone of security− CIA principles (confidentiality, integrity, and availability). The evolution of cybersecurity terminology shows subjectivity and vague contributions [4] with fluctuations found in its focus (e.g., IT, information, information systems, and governance). Some authors [5] recognise the trends of the phenomenon and clarify that literature actively misguides and inaccurately informs readers regarding the meanings of cybersecurity. Thereby the compelling argument is that cybersecurity is distinctive because cybersecurity is a control function that protects not only information but also many other components instead of a single focus such as IS [5]. However, other authors (e.g., [6], [7], [8]) continue to support the traditional

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.
ICIME 2018, September 22–24, 2018, Salford, United Kingdom.
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-6489-8/18/09…$15.00
DOI: https://doi.org/10.1145/3285957.3285971

silo approach to security through their linear contribution; something that omits the wide-ranging perspective. In some cases, there is a continuation of data-driven centric security; others still use 'information security' to describe the phenomenon despite laying out a more complex security, respectively cybersecurity.

Nonetheless, both approaches fail to align their focus and consequently recognise who is responsible for security. This is partially because the first approach remains traditionally focused while the second approach uses the old terminology but applies modern concepts of cybersecurity. The evidence suggests that the evolution of cybersecurity has undergone various phases, resulting in a granular legacy. Cybersecurity represents the pillars of trust in cyberspace, a pillar of online business activities [9]. Confusion in terms of terminology can carry consequences; for example, without uniformity regarding the definitions of certain terms and agreement on which terms to adopt, organisations face considerable hurdles should they wish to collaborate [10]. Moreover, compliance with legal frameworks is also jeopardized [11]. To date, the complexity of the legacy of cybersecurity and implications of the granular disciplines are limited. Moreover, in the light of increased insecurity, it is becoming difficult to ignore such a problem and perhaps when defined, cybersecurity capabilities might be enriched.

Therefore, as a response to the confusion, this paper aims to highlight the current state of the research problem and sustain the advancement towards the new school of thought. It will decide 1) whether terminology misalignment is hindering cybersecurity, and 2) whether having a unified terminology of cybersecurity is justifiable. In turn, the paper shall explore the determinants of interchangeable terminology used amongst academics and practitioners to analyse the nature of the determinant (mandatory and discretionary) in order to outline the cause of confusion and justify the proposal for a unified, standardised legacy for cybersecurity terminology.

2. RESEARCH BACKGROUND

2.1 Research Problematic Review

Due to digitalisation and Internet connectivity developments, the last two decades have registered a significant change in the way individuals and organisations behave. Thus, security has been gaining importance due to its vital protective role [12], [4]. However, even though the security of cyberspace has evolved, its maximum efficiency is yet to be attained. The problems of applying cybersecurity are more challenging in today's context as there is a lack of a legacy of unified literature. The transformation of the IT domain as well as the digitalized business context stress the importance of understanding the risk spectrum (i.e. scale, complexity, or ripple effects) and the need for flexible risk control function. Consequently, this paper explores beyond the literature granularity of cybersecurity terminology and meanings, arguing that the use of a unified terminology will foster additional value and empowerment of risk oversights (countermeasures and safeguards) because identifying and clarifying the root cause and effects of the confusion help encapsulate the concept accurately.

Stemming from various disciplines, cybersecurity has progressively built its current position upon its early roots in computer science, information security, information assurance and risk management principles [13]. Traced back, the initial protection focus has switched over the years to become a more expanded form of a risk control function and governance. Moreover, as an effect of its varied legacy, organisations use a mixture of terminologies for cybersecurity. This can be for the sake of appearance, reputation or compliance but, commonly, without any intention to truly adopt the meanings.

The current debate about cybersecurity definitions, scope and meanings has identified an interesting viewpoint that can be divided into two main ideas: information/data-driven security and risk governance. The first viewpoint is based on the traditional driven approach of information protection only (secure data against risks) (e.g., [3], [8]). On the other hand, the second viewpoint maintains its terminology, despite addressing a broader area, so as to be the same as cybersecurity (e. g. [14]). However, it omits to adopt cybersecurity terminology and ensuing principles. Typically, these types of studies admit that information security evolves in a wider paradigm yet remains traditionally embedded. Opponents of cyber-related terminology e.g., [6], [70] reject the reformation of a new terminology yet use the principles of it.

Few studies have explored the semantics and etymology of cybersecurity terminology [5], [4], [15], [16], [2] and predominant literature lacks clarity (e. g., [6], [17]). This indicates a need to understand the various perceptions of cybersecurity. Much uncertainty exists in using the correct terminology when wishing to communicate clearly in the field of security. All confusion regarding the terminology, scope and/or meanings divides and thus inhibits the discipline of cybersecurity. From the standpoint of terms used, the generalisation of much technological-related terminology is that it has suffered variation, as is currently the case of 'cybersecurity'. The evolution of technology has determined the various use of 'buzzwords', but it stands on granular aspects of security (e.g., technological, strategical, and operational), where each perspective adds its own understanding/meaning. The question with which this paper is concerned regards how the interchangeable use of terminology leads to confusion (even for those who are familiar with such jargon).

2.2 Paradigm Shift

Henceforth, developments of the Internet have led to the creation of a 'cyber [space] ecosystem', where multiple elements interact [17]. Such perspective not only separates types of perimeters (settings) but also the mechanisms for undertaking action (interaction) are divided into two distinct parts: 'cyber' and 'space' (as can be seen in Figure 1). While terminology provides a brief illustration of variability, the evidence of definitions supplements a deeper understanding of variations and derivations that are often inappropriately used in an interchangeable manner. Many organisations use various terminologies, but terminology variation has a direct impact on cybersecurity scope, derivations, meanings, and implementation. For example, it is granted that many studies have attempted to explain cyberspace terminology and definitions, yet terms have yielded little mutual agreement regarding their etymology and meanings [16]. The term 'cyberspace' is the first start towards justifying the employment of an official terminology for cybersecurity. Confronted with a vague and granular explanation of what it exactly represents, the term 'cyberspace' has been interchangeable and synonymously associated with terms such as 'virtual world', 'virtual environment', 'cyber environment', 'cyber domain', 'online world', 'online domain', 'online realm', 'cyber ecosystem', 'electronic space', 'digital world' or 'wired world', among many others. Often, these terms have been used as a direct equivalent to 'cyberspace'.

However, the terms are not necessarily synonymous in all cases and thus imply multiple meanings [18], [19]. For example, 'virtual world' refers to the electronic environment as a three-dimensional reality where people can experience/interact (e.g., video games, interactive learning) with an artificial environment based on human-computer-interaction. It is similar to a real-life experience although intangible [20], [21]. Thus, 'cyberspace' is an impartial term employed to define and represent only some aspects of the virtual world.

While 'space' can clearly be defined as a setting/place, the word 'cyber' describes the type of interaction (namely through the means of the Internet). Consequently, the word 'cyber', incorporates the principles of cybernetics (i.e. human-computer-interaction), where interconnected computer systems embrace extensive technologies that are capable of facilitating, reshaping and exchanging electronic information and communication by connecting to an 'imaginary world' [22], [23] and relying on "the principle [of] governing or directing a technology or system" [22, p. 23]. In most cases of literature, the word 'cyber' forms part of a compound word, as do the words 'online', 'digital', 'virtual' or 'electronic' and the word 'space' has equivalents: 'world', 'realm', 'reality', 'domain', 'ecosystem' and 'environment'. Additionally, the word 'cyber' could be joined to another word synonymous to space and it would still imply 'cyberspace'. The following, Figure 1, emphasizes how the compound word', 'cyberspace' (cyber and space) proves to be the source for many terminological variations.

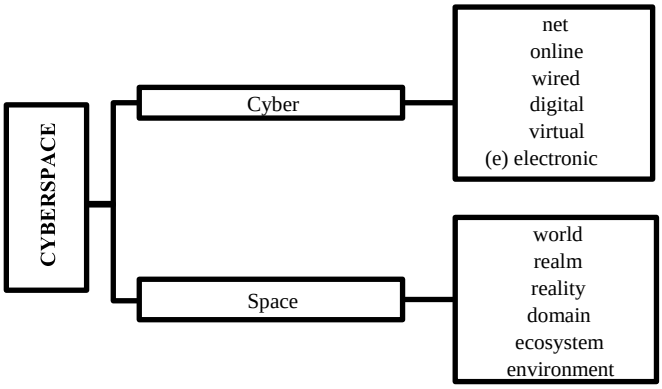


Figure 1. Ambiguity of Cyberspace Terminology

In short, Figure 1 represents an etymological map of cyber-related terminology, where 'cyber' and 'space' refer to perimeters/boundaries and the type of technology involved [22]. In particular, 'cyber' relates to control/governing aspects (Gibson cited in [24]) and articulates interaction with the Internet, computers or even robots; for example, machine learning [25], [26], [27]. Consequently, it relies on feedback, control, and communication [22], [25].

Based on the evidence discussed above, it is obvious that 'cyber' terminology plays a significant role when arguing for official terminology for cybersecurity. Some authors have suggested that

'cyber' terminology usage leads to a 'cyberization' trend (cyber-related terms developments) due to the prominent use of the terminology [16], [28]. Within cybersecurity terminology, the word 'cyber' is most broadly used as a *descriptor* (e.g., cyber warfare, cyber-crime) [16]. While a unified discipline may contribute towards the reduction of confusion and disparate use of research, common use of a unified vocabulary is still not adopted. 'Cyberization' means that the prefix 'cyber' has been fostered and established well within technology-related lexicon over the years [28] as it is used to be previously initiated with 'computerization', and later with 'informatization' terminology (computerization-informatization-cyberization paradigm shift). The remaining question is to where the evolution of 'cyber' lead–conceptually the definitions are similar, but the terminology is unclear and varies.

There is clear evidence that 'cyber' remains accepted by the research community as a general descriptor for all technology-related terminologies [16]. Until further change is made, the cyber discipline will remain scattered with a variability influx of terminologies.

2.3 Cybersecurity: a granular discipline

The implication of the word cyberspace goes beyond its mere definition because the concrete definition can be interpreted in a variety of ways. Cyberspace can imply something positive, but it can also mean something negative, the latter often relating to an organisation's online activities, namely the security side. Thus, beyond positive association and possible advantages, cyberspace developments also imply security aspects imperative for any organisation's business continuity and performance. Although in its early beginning, security was seen through the perspective of computer science (enabler). Over time, it shifted from technological security towards a separated discipline of information/data-driven security and risk management [29]. Then its broader applicability with risk governance became significant and valuable for organisations. Apart from its paradigm shift (i.e. from technological data-centric security approach to risk governance), the security research domain has registered fluctuations regarding how it is perceived and what it aims to protect [30]. The two-main paradigm shifts of cybersecurity research oriented to a business perspective with a broader applicability are discussed below.

2.3.1 Information Security paradigm

Information represents a significant asset for an organisation, and thus manipulation, storage and protection of such asset is necessary [31] and should undoubtedly be part of any organisation's culture and organisation governance. Accordingly, the following perspectives are identified from the literature:

i. Perspective One: Information Security goal oriented to protect information assets

This first perspective of Information Security mainly refers to the protection of information assets that are critical for an organisation [7] along with the systems in which assets are stored [15]. The perspective pays particular attention to the initial roots of information secrecy and securitisation and maintains its position over the years [32]. Much of the current literature only shifts regarding strategic governance but remains focused on information assets security although adopt the strategic-centric approach as a business control function to improve organisational resiliency [33]. Information values can vary across organisations yet are often characterised based on criticality and sensitivity when exposed to a threat. In general, the information can be tangible or intangible data (e.g., intellectual property information, trade secrets, employee personal information) and often proves valuable for the organisation's deployment of activities [7]; security of information is crucial for business continuity and performance [34]. It is well known that information security relies on three main principles (confidentiality, integrity, and availability) [35] to protect information. Such a statement demonstrates that

this perspective is a partial dimension of security because it limits itself to the protection of information and more specifically, on how it can be protected from malicious threats [36].

When referring to confidentiality, it needs to protect only that information by assuring that only authorised persons have access to it [2]; in other words, the information is not known by others. In the case of integrity, it again refers to information security, but this time confidentiality assures it is not to be altered by others. 'Availability of information' means it should be reliable and available upon request [2] since the principles of confidentiality, integrity and availability (also known as the CIA triad) aim to protect tangible and intangible information assets.

Thus, the view rests on the assumption that the CIA triad is to be provided through the support of tools and mechanism [36]. It is clear that the security information focused perspective has been an inherited legacy [36] since the early beginnings of the Internet and computer security. Change throughout the history of the Internet has undermined and thus limited the initial scope of information security [37]. Most often, this perspective is known as 'information protection', 'information assurance' or 'information security'; all terms being part of the information age where terms are used synonymously for the same discipline, with no distinction. Despite the importance of securing information assets, there remains paucity evidence proving current organisations' widened needs in terms of security.

ii. Perspective Two: Information Security goal oriented to protect information, information systems, technology, processes, structure, people, and organisation.

This second perspective of Information Security represents a paradigm shift from an initial silo approach of information security assets. Thus, the second perspective embodies a more comprehensive security approach that additionally includes the human side, systems, technology and processes to ensure the security of an organisation [6]. In contrast to its inclusive approach, this perspective supports the cybersecurity paradigm but prompts confusion regarding terminology. A more detailed account of terminology variations is exemplified in the following Table 1.

Table 1. Information Security Dimensions

Terms	Definitions
Information exclusive view (traditional silo approach)	"Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms" [3, p. 17]. "The protection of information against unauthorised disclosure, transfer, modification, or destruction, whether accidental or intentional" [41, p. 361].
	Information Security: It is the practice of defending information from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction [8, p. 39]. "Information security management (ISM) is a continuous, structured and systematic security approach to managing and protect the organisation's information from being compromised by irresponsible parties" [42, p. 904).
	"Information security risk management is the primary means by which organisations preserve the confidentiality, integrity and availability of information resources" [7, p. 1). "Cyber security and information assurance: Maintaining the confidentiality, integrity and availability of services and information as well as protecting services against threats" [43, p. 43].
Multidimensional view (holistic)	"Information security encompasses technology, processes, and people" [6, p. 361]. "Information security governance encompasses all business assets, as well as their risks and threats, including information, processes, people, services, IT and reputation" [70, p. 12].

As emphasised in Table 1, it is clear that the first perspective of information security supports the argument that information security has evolved, and its meaning needs to be clarified [37] in order to better respond to current risk governance challenges.

Until 2012, standard ISO/IEC 27032:2012 [38] and standard PAS 555: 2013 [39] used the term 'information security' as a reference to cyberspace security. As of 2012, information security has been referred to as a dependency of 'cybersecurity'. The argument that information security and cybersecurity are separate domains is continued later in the standard ISO 27000: 2016 [40], which makes a conclusive remark that information security is: "preservation of confidentiality, integrity and availability of information" [40, p. 6]. These facts demonstrate that the terminology needs to align with current requirements in order to avoid side effects of non-alignment. Despite BSI's attempts to promote cybersecurity terminology through the deployment of two standards in 2012, pre-2012 approaches have continued throughout other standards (e.g., ISO/IEC 27001:2013, ISO/IEC 27000: 2016).

Although the first perspective seems an outdated approach towards cybersecurity, it is still used nowadays. Insights are drawn from scholarly literature advancing the idea that security information assets and their system should be defined as 'information assurance' [44]. However, the second perspective represents a misuse of the paradigm. Certainly, these facts reiterate the need to expand the research to foster broader security focus and literature transparency instead of a fragmented field. The facts mentioned above emphasize that the disjointed research within the information security field diminishes the potential of further investigation and innovations [30].

2.3.2 Cybersecurity paradigm

Even though cybersecurity appears to be a new risk, it is actually an advancement of information security to a more complex and inclusive perspective [39], [10]. In other words, it is an old risk oversight approach that has evolved from computer-information-assurance security dimensions. The landscape of threats has changed from simple viruses, unauthorised access or misuse of information assets to substantial financial losses, disruption of business operations, and loss of reputation, intellectual property loss and loss of clients, among many other issues. Cybersecurity has become a defensive and corrective process that ensures the protection of cyberspace and any related assets that can be reached through the means of cyberspace [45].

In summary, cybersecurity refers to cyber risk, threat or vulnerability addressing individual and organisational assets that are subject to cyberspace interaction [2]. More specifically, in the case of organisations' domain the critical values and assets that need protection can range from tangible (e.g., software, computers, systems, utilities, internet networks) to intangible (reputation, intellectual property, electronic data storage, research and development data) [2].

Typically, for some organisations, some assets might be more valuable or critical than others. Consequently, defining the value of assets depends on the organisation's core activity and long-term strategy. In this context, the valuation of assets frequently relies on the CIA triad [2]. This prompts a re-think of how cybersecurity is perceived in literature and practice, deconstructing the idea that various perspectives of cybersecurity and information security rely on the same principle—the CIA triad.

There is prominent literature that spurs the idea that IS should incorporate more principles to become complete (i.e. 'accountability' as a responsibility for actions) [3]; a fact that provides support towards the worth of cybersecurity. In contrast to information security definitions, cybersecurity seems to be perceived on the assumption that it needs to prioritise the protection of cyberspace (environment) instead of protecting organisational assets [4], [34], [15]. Equally important is that in some cases the risks are unrelated with information assets [1], a fact that contradicts previous traditional schools of thought such as IS.

Following an overview of definitions in order to convey the differences in meanings, prior studies have been carried out under numerous appellations such as Information Security Management, Information Security Risk Management, IT Management, IT Governance, Information Computer Technology Security, Information Technology Governance or Cyber Risk Management [46], [47], [7], [35], [48], [49], [50], [51], [52], [53]. As an illustration, the following (Figure 2) emphasises some examples of the interchangeable use of terminology and its variations depending on technical, operational and strategic orientations.

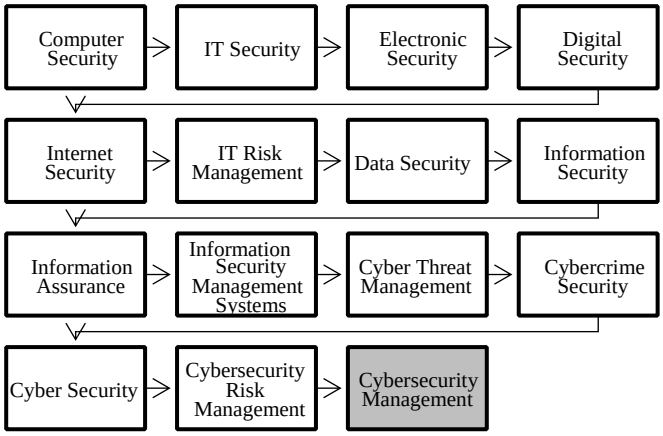


Figure 2. Terminology Fluctuations of Cybersecurity Terms

Regarding justification already discussed, Figure 2 demonstrates that in the digital age, the term 'cyber' is more appropriate [54]. Thus, it is more suitable to be used with 'security' and made into a compound word, respectively 'cybersecurity.' Despite the fact that Figure 2 shows evidence arguing cybersecurity to be a disparate discipline, it demonstrates an evolution, with its roots in technology, security and information security. Terms such as 'cyber security' or 'cybersecurity' show that despite scarce interdisciplinary cooperation, there is positive evidence proving the use of proper terminology (even if different from its condensed format). Taken together, all these terms reveal that in general, the literature identification necessitates more efforts and is consequently scattered [16]. For this reason, this paper analyses the issue under the cybersecurity umbrella.

Owing to the scarcity of clarity in terminology and meanings, [6], [55], [27], [5], and [4] are among some scholars who have identified and outlined that cybersecurity is more than information and system security. Correspondingly, it has a determination to protect against physical and electronic damage that could come through cyberspace. Cybersecurity prompts a rethink of the traditional view of IT security, IS/Information Assurance, Information System Security and incorporates tools, policies, procedures, safeguards, guidelines, culture, certifications and/or technology software [6], [5] and other safeguards designed to mitigate risks in an integrative manner. Indeed, it can be argued that if an organization avoids cyberspace, it might be interpreted as an IS approach. However, cybersecurity entails more than connectivity to the Internet; henceforth it extends its approach to additional components and strategic implications (accountability, responsibility) [1].

With particular reference to its determinants, some researchers argue that cybersecurity is a strategic mechanism that protects assets (information, ICT infrastructure, computing devices, technology applications, systems, servers, intranets), people and processes (services, telecommunication systems) in an integrated manner [6], [5]. Above all, a variation of terminology and definitions in literature continue to generate confusion regarding this discipline. The most significant confusion lies between cybersecurity and IS. Although appearing similar, they are distinct and IS refers to protection in a silo of information. Frequently, the terms are employed interchangeably, with identical meanings. Clarification on what IS represents is scarce. The BS ISO/IEC 27000: 2016 (among other standards) clarifies that IS embodies "preservation of confidentiality, integrity and availability of information" [40, p. 6]. There is a continuous, unsuitable sustenance of the traditional approach which argues on one the hand that IS is only the security of information yet on the other hand "Information Security encompasses technology, processes, and people" [6, p. 361]. However, this sustains a misguided, subjective and uninformative approach [4] with a fluctuation in its focus (e.g., information, IT or systems) due to embedded traditional approaches.

For this study, the following definition of cybersecurity is accepted: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation, and users' assets" [5, p. 97]. Through comparison Figure 3 emphasises the distinctiveness of focus and meanings, along with the correlation of information security contrasted with cybersecurity.

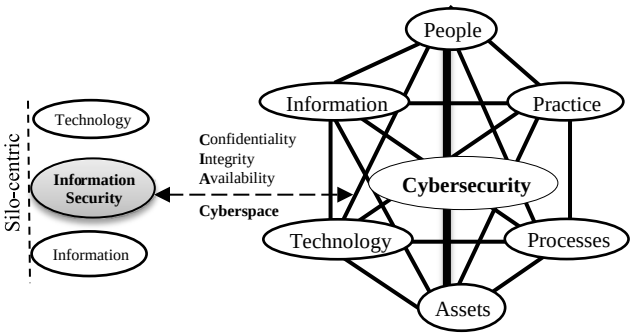


Figure 3. Contrast of IS Principles with Cybersecurity Principles and its Components

As can be seen in Figure 3, cybersecurity incorporates many more components to protect an organisation. In contrast to the information security perspective, cybersecurity moves beyond internal control to incorporate the protection of the cyberspace as well. Nonetheless, cybersecurity and information security are different in scope despite being complementary and equally important [15]. The CIA triad enforces a common point for cybersecurity-related terminologies (i.e. Information Technology Security, Information Assurance, Information Security, and cybersecurity have common principles of CIA triad) and when all together, depend on similar variables such as technology and information assets [27]. This refers to the research problem, respectively to the shift from Information Security towards cybersecurity paradigm, shedding light on the fact that 'information technology security' and 'information security' are indeed subsets of cybersecurity; not the opposite [27]. While there is conflicting evidence regarding terminology dimension, considering all the evidence, a change from initial focus is usually associated with security boundaries. Cybersecurity is a broader approach [56] to securing not only information assets but also the technology, assets, processes, people, organisation and practices with similar dependable variables. Recently, there has been evidence suggesting that the range of assets covered by cybersecurity continues to increase [10]. Additionally, the strategic-centric approach of cybersecurity demonstrates a more holistic approach to risks across the organisation while IS remains a siloed approach that protects information assets and information systems. Table 2 below represents additional evidence that captures the different path of cybersecurity.

Table 2. Cybersecurity Granular Definitions

Term	Definition, Author/s
cybersecurity	"Cybersecurity is the organisation and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" [4, p. 13].
	"Cybersecurity is the business function of protecting an institution from damage caused by cyber-attacks in the face of constraints such as other business objectives, resource limitations, and compliance requirements" [33, p. 12).
	"The ability to protect or defend the use of cyberspace from cyber attacks" [69, p. 25].
	"Cyber security can be considered systems, tools, processes, practices, concepts and strategies to prevent and protect the cyber space from unauthorised interaction by agents with elements of the space to maintain and preserve the confidentiality, integrity, availability, and other properties of the space and its protected resources." [13, p. 3].
Cybersecurity endorsed as IS	Cyber Security or Cyberspace Security has been defined as the 'preservation of confidentiality, integrity and availability of information in the Cyberspace' [8, p. 39].
	"…defines cybersecurity as the protection of investor and firm information from compromise through the use—in whole or in part—of electronic digital media, (e.g., computers, mobile devices or Internet protocol-based telephony systems)" [60, p. 3].

Table 2 shows a clear trend of cybersecurity literature. Da Vega's and Eloff's [6] study is an example of a different approach (showing the value of culture) through the interaction of information, technology, processes and people. In contrast to this perspective, some others (e.g., [8], [60]) address the issue only partially.

From a regulatory perspective, for example, European Parliament's [57] official communication clearly states a similar viewpoint: "any study of cybersecurity must reflect on challenges introduced by the different meanings of the term" [57, p. 13]. This statement constitutes confirmation yet again that disagreements regarding cybersecurity definitions exist and furthermore are acknowledged.

An underlying assumption shared by some studies is that cybersecurity terminology is perceived and influenced by industry practices and regulations [58; [59]. To analyse the nature of the mandatory and discretionary factors that influence the variations of terminology employed by academics and practitioners, differences arising in practices, standards and laws must be studied with the intention of identifying the cause of confusion. Additionally, the potential impact of the interchangeable use of terminology should be further explored hence substituting a terminology might also create uncertainty—if an organisation is compliant—due to any subjectivity that each organisation might have in understanding same terms [11].

The complete representation of what cybersecurity underpins is emphasised by the first category (cybersecurity) and indicates a pronounced significance towards a holistic applicability of preventative risk measures. On the other hand, some organisations use cybersecurity merely for the sake of appearance, reputation or obligated compliance. Most often organisations do not intentionally adopt certain terms for the meanings and scope, having first given prior thought and consideration to the jargon. For example, some organisations might have a cybersecurity department, but once its activities are reviewed closely, IT security and/or information assurance are often found to be operating in a siloed way and above all, in isolation from the organisation's overall security strategy. Even if valuable, IT security represents a partial approach of computer systems, information systems and/or IT-related resources. For many years, supporting literature on

cybersecurity has debated due to its critical and reactive responses. Likewise, Julisch's study [61] recognises the critical role played by cybersecurity failures, echoing the value of lessons learned in the direction of the organisational protection grounded on holistic strategy, not intuition. Overall, preventative security controls (safeguards) are considered proactive responses. Various approaches have been proposed. However, the practitioners' viewpoint is open to debate and controversy despite it representing a good applicability of cybersecurity as well as paying attention to guidelines, policies and standards yielded from past lessons. It also portrays the state of cybersecurity based on a general practitioner's perspective [62]. Much work on the potential of cybersecurity has been carried out by or in accordance to standards (mandatory guidance) and practitioner's frameworks. However, there has been considerable interest in assurance, protection and the establishment of an organisational structure that builds resilience and facilitates a continuity and recovery in case of an incident, as demonstrated by BS ISO 27003:2017 [63]. Such practices are also sustained by guidance that is not mandatory but usually represents the expected practices in regard to preventative security controls and also counter measuring post-events.

Notably, cybersecurity's insecurity for organisations is challenging [62] as its occurrence and sophistication have increased. Likewise, BS ISO/IEC 27003:2017 [64] recognise the critical role of cybersecurity and updated the initial hypothesis where some organisations deny its challenges. Distinguishing that a cybersecurity incident has an unforeseen aspect means it is based on an opportunistic criminal mind-set. Thus, the utility of increasing executive awareness of cybersecurity attacks highlights that more preparation and investment are needed to acquire cybersecurity maturity [17].

That is to say, both these approaches of cybersecurity demonstrate that there is no general agreement on IS/IA (information assurance/security) terminology with cybersecurity (security of people, processes, and assets) [10]. These two insights demonstrate the existence of disparate literature, distinct in meaning and purpose but with some commonalities such as the use of technology, assets protection, use of the same CIA triad principles and the use of cyberspace [13]. It also emphasises a paradigm shift from an organisational security focus to an extensive societal protection of cyberspace. Given the advances within IT domains and the way they influence how businesses act, it is imperative to recognise that the cyber 'lens' of security is a mere responsibility for organisations [71]. Whether connected to cyberspace or not, the change in terms regarding technology, behaviour or intellect fosters caution. By being online and/or engaged in any online activity such as a financial transaction, a company is exposed. Understanding behaviour and attitudes towards the continuously varied uses of terminologies for cybersecurity is yet a research field to be explored and understood.

3. RESEARCH METHODS

This paper is derived from a systematic literature review that evaluates and interprets prior studies relating to the research paper to identify the current state of state, its limitations and problematic gaps [65], [66]. Therefore, data analysis relies on a thematic analysis for studying the qualitative nature of research through a pre-planned assessment protocol [66] in order to identify the above-mentioned aspects so as to validate the position and contribution of this research paper. Being qualitative research, data is explored through an interpretive philosophy in order to understand behaviour and attitudes towards the interchangeable use of terminology for cybersecurity and its effects. Owing to the research problem being a broad field of research fragmented into disciplines, the investigation aims to identify commonalities, differences, typologies and derivations of current research trends. Therefore, both data selection and analysis have been made manually based on scope, the research paper's question and inclusion, and exclusion criteria [66]. Thus, the authors have constructed the review on qualitative evidence of academic journals and industry publications for a wider understanding of the phenomenon. Exploratory in its nature, the selection of papers is made through a database search (search string) but also through consideration of references from appropriate publications identified in terms of relevance, paradigm typology, research dimension, focus, strengths, limitations, key findings, contribution and/or omitted components.

4. ADVANCING TOWARDS CYBERSECURITY

Advancing beyond the IT domain towards a multidimensional approach to cyber resiliency, interlinked with the current business models, cybersecurity gleans a more flexible managerial and controlled function. Ever increasing reliance on connectivity leads to a digital transformation [71], respectively 'cyberization'. On these grounds, the findings of this paper suggest that having a unified/common terminology of cybersecurity is justifiable and that prior research indicates consequences of terminology misalignment.

The scale of how severely misaligned terminologies are and how drastic the eventual outcome will only come to light as time passes. The identified determinants of interchangeable terminology tend to show that amongst academics and practitioners, the nature of the determinants factors is discretionary and mandatory. For instance, the most common discretionary (voluntary) factors are the herd instinct (tendency to follow others), organisational culture [34], [6], performance need driven by standards or guidelines [10], [16], geographical area practices [61], specific laws and practices [58], [16],[59], marketing campaigns, public pressure [71], services available, and/or shareholders pressure [67]. Justification to propose a unified, standardised cybersecurity legacy seems feasible as, like literature, there are various discussions and perspectives related to cybersecurity terminology. With an appreciation of the different perspectives within academia and industry, different points of view have been considered in order to identify their validity in literature. Drawing upon two strands of research in cybersecurity, this paper validates the need for a clarified terminology of cybersecurity instead of IS and many others. It explores the determinants of interchangeable terminology used among academics and practitioners to justify the proposal of a unified terminology usage.

With the objective of analysing the nature of mandatory and discretionary factors that affect terminology variations amongst academics and practitioners based on a literature overview, the findings are qualitative in nature (no statistical evidence was found) and consequently, the following research trends have been identified:

1) There is a significant amount of literature that perceives security through the lens of Information Security. The authoritative literature related to security within the cyberspace environment of organisations is significantly predominant on

Information Security, which is defined as the security of information and information systems only (e.g., [3], [7], [8].

2) Research suggests that Information Security is Information Assurance and vice-versa. Information Security and Information Assurance are perceived as a duality and frequently used interchangeably [3].

3) Research suggests that 'cyber' terminology in the context of security follows the same pattern. The term 'cyber' has been used interchangeably with many other terms because it refers to a virtual perimeter/environment [8]. In short, 'cyber' and 'space' refer to perimeter/boundary and the type of technology involved and how this work is handled overall [25]. A significant number of papers have been found which, despite using different terminology, in most cases have a similar understanding of what is represented (e.g., [16]). On the other hand, others that use the correct term for 'cyberspace' fail to adopt the cybersecurity terminology. For instance, [8] refers to the term in two forms: cybersecurity and cyberspace security. Furthermore, cybersecurity is perceived as a mechanism whose principal purpose is first to assure the security of cyberspace [4], [34], [15]. Thus, the use of 'cyber' as an integrative part of 'security' seems more appropriate. Therefore, Information Security should be a subject under the cybersecurity umbrella.

4) The findings expose that Information Security and Cybersecurity are perceived as meaning the same thing [1]. Interestingly, it has been found that the main 'opponent' of cybersecurity is Information Security, again raising concerns over the particular lexicon cue. It is possible that this second perspective is to represent only a terminological 'mask' between these two domains. Hence, information security is defined through the viewpoint of what cybersecurity represents and not through the lens of securing information assets. Examples of studies such as Da Veiga and Eloff's 2007 study and Humphreys' 2010 study demonstrate the interchangeable use.

5) Although perceived to have the same meaning and used interchangeably, prior research of IS and Cybersecurity demonstrates the opposite and emphasise one possible reason for confusion: the CIA triad. For instance, IS, Information Technology Security and Cybersecurity rely on common objectives of confidentiality, integrity and availability. Furthermore, Information Technology Security is the third discipline with the same commonalities. If the CIA triad was initially referring to information or technology systems, how should these principles apply to current widened assets (people, assets, practice, processes, technology, infrastructure or information), considering that their confidentiality, integrity or availability are needed. The role of security seems elusive within this context. It appears that this commonality of CIA triad is unfeasible for the current context and cybersecurity components, being more a legacy perpetuated on the basis that is a good practice to follow without being challenged in terms of its current value and applicability.

6) Although identified as different disciplines and different focal nodes, IS and Cybersecurity have another three commonalities: technology, information and perimeter (cyberspace). IS and cybersecurity are distinctive, but also have commonalities despite technology and information being two different mechanisms (disparate). Evidence found validates the prevalence of technology and information commonalities within the research mainframe. Despite some views differing significantly, there is a dependable common variable: cyberspace [10], [13].

7) Both IS and cybersecurity have adopted a paradigm shift that incorporates the Risk Management approach but remains different in scope, meaning and goals. Cognizant of IS or Cybersecurity, incorporating a Risk Management approach is beneficial for organisational governance as resilience is paramount [12].

8) The side effects of misused terminology as well as inconsistent and contradictory literature are identified within the literature.

The implication of monopolistic 'information security' determines a lack of clarity between goals and mechanisms. The perspective of Cherdantseva and Hilton [44] undoubtedly gives a comprehensive account that security terminology, through the lens of meanings, scope, and goals, should be clarified for both disciplines. While cybersecurity is often used, the old terminology of Information Security seems to have strong roots in the traditional mind-set while others are influenced by the following independent variables (1) job titles (e.g., Information Security Manager, Chief Information Security Officer), (2) professional certifications specifically focused on information security (e.g., CompTIA Security+, Certified Information Security Manager), (3) standards (i.e. BS ISO/IEC 27005:2011, BS ISO/IEC 27000:2016 versus BS ISO/IEC 27032:2012), (4) regulatory frameworks (e.g., Data Protection Act 1998; Federal Information Security and Management Act of 2002; EU General Data Protection Regulation versus Cybersecurity Act of 2012), and lastly (5) by inherited legacy. Such discrepancies are also present in various terminologies used by standards, guidelines and governmental reports (i.e. NIST used terminology cybersecurity while BS ISO refers to it as Information Security). The question of variation in terminology needs to be addressed urgently as it affects theoretical legacy, industry practices, as well as professional qualification developments [10].

As a result, these facts make it difficult to move beyond the information-centric approach. Nevertheless, contradictions between the theory of information security and its practicality question its consensus of meanings and capabilities concerning risks. Understanding the consequence of granular terminology is an open debate, hence a proper understanding of implications for scholars and practitioners shall foster a unified terminology. However, literature provides reasonably consistent evidence that the most prominent effects are: (a) confusion in decision [61]; (b) granular legacy [2]; (c) fostering of numerous security risk practices instead of a holistic risk approach [14]; (d) fostering of various title jobs; (e) fostering of different professional certification for the same purpose; (f) fostering of a different understanding of scope and meanings; (g) fostering of functions that overlap with the organisational context [5], [30]; (h) obstructing the advancement of cybersecurity [61],[4]; (i) being consequential to other related terminologies due to 'cyber' being a compound word (e.g., cyber threat, cyber-crime)[68]; (j) undermining cybersecurity collaboration within states and in turn increasing business regulation constraints due to the different definition, means and scope (i.e. Russia, China, Uzbekistan promote the use of IS, whereas U.S.A., Japan, Estonia adopt the cybersecurity term; (k) proving uncertainty of compliance [11].

Furthermore, it can lead to an additional effort being required when endorsing cybersecurity/information security programmes in the context of a potential business partnership due to incompatibilities of approaches [10]. Previous studies illustrate that the semantic confusion, gap, differences in objectives, scope and meanings are necessary to determine the applicability. Understanding that IS represents a stagnation and silo risk approach is the first step organisations must adopt if wishing to advance towards a proactive layer of security (cybersecurity) that incorporates multiple components in order to mitigate risks.

The suggestion to use cyber as a compound word (no hyphenation) suggests that the same rule should be applied to all related terminology (i.e. 'cybercrime' instead of 'cyber-crime'). Aside from the proper use of cyber terminologies, the same principle should apply to cybersecurity, as a paradigm evolution from information security (IS) into cybersecurity (CS), respectively a re-conceptualisation to glean its full capability and effectiveness through the 'cyber' lens.

Without a defined cybersecurity paradigm within the business context, the aftermath is cognizant of negative side-effects; for example, adding confusion for boards of directors regarding business decisions [1]; impeding advances due to fragmentation [4]; lowering engagement within business units; fostering communication confusion; and lastly, dividing the meanings [4]. Likewise, conceptually, a varied and unclear terminology leads to a lack of consistency within knowledge [16] and renders a nonunified discipline [16] that hinders cybersecurity potential.

5. CONCLUSION

Overall, this paper suggests that various strands of the phenomenon and the interchangeable terminology used for cybersecurity may trigger interrelated consequences. Nevertheless, cybersecurity definitions seem elusive. Additionally, Information Security and Information Technology Security rely on common principles of confidentiality, integrity and availability (CIA triad). All three domains also on rely on the use of technology and the same premises (cyberspace) as well as being security-driven assets (even if partially). The paper also concludes the value proposition of understanding the benefits of a unified terminology, scope and meanings of cybersecurity rather than other interrelated terminologies.

Regarding the underpinned research method, this paper is limited to the exploration of a secondary data review based on a systematic qualitative review of scholars' and practitioners' literature analysis that has identified the research state, limitations and gap. Henceforth, the role of cybersecurity in organisation protection has received attention across interrelated disciplines (as identified in this paper), thus proving that the complexity of cybersecurity is imperative in today's organisation context if applying proper controls. Although varied in focus and meaning (e.g., information security, information assurance, computer security, Internet security, cyberspace security, to name but a few), the most prominent confusion lies between IS and cybersecurity. Therefore, the proliferation of the misleading interchangeable use of security-related-legacy needs clarification. Despite debates regarding information security being the same as cybersecurity, to date, there has been little agreement on what constitutes cybersecurity. Perhaps of more concern is that many organisations use a variety of terminologies, each having a direct impact on cybersecurity scope, derivations, meanings, and implementation. Some organisations use cybersecurity merely for the sake of appearance, reputation or obligated compliance. They do not intentionally adopt certain terms, having first given prior thought and consideration to the jargon. While cybersecurity is a growing field, the drawbacks of using a non-unified terminology continue to be sustained by inherited legacy of IT security, information assurance or information security (i.e. scholars' publications, as well as those of practitioners through the means of applicability, use of frameworks, guidelines, professional certifications or job titles) as misleading theory and practice.

These findings suggest that cybersecurity has developed from Information Security and due to its legacy (IT), it is difficult to delimitate the information-centric approach due to the time-bound aspect. Notwithstanding this limitation, it is suggested that it should be incorporated holistically with other components of cybersecurity and an organisation strategy. Nevertheless, contradictions between the theoretical dimension of cybersecurity and its applicability question its consensus of meanings and capability to manage risks in today's organisational context. Understanding that IS represents stagnation from the holistic practice of cybersecurity represents a paradigm shift and advancement towards a proactive layer of security that incorporates multiple components to mitigate risks. Further research exploration is required to determine the long-term effects and implications of the cybersecurity paradigm's ambiguity regarding meanings and terminologies. It is recommended that future research should imply empirical evidence that might determine further insight into the confusion caused and long-term implications for organisation strategy.

6. REFERENCES

[1] Von Solms, B. and Von Solms, R. 2018. Cyber security and information security – what goes where? *Information and Computer Security.* DOI: https://doi.org/10.1108/ICS-04-2017-0025.

[2] Alexander, R.D. and Panguluri, S. 2017 in Clark, R. M and Hakim, S. (eds), Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level, Volume 3 in Protecting Critical Infrastructure, pp. 19-47.

[3] Feruza, S. and Kim, T. 2007. IT security review: privacy, protection, access control, assurance and system security. *International Journal and Ubiquitous Engineering*, 2(2), pp. 17-31. DOI: 10.12691/education-6-2-10.

[4] Craigen, D., Diakun-Thibault, N. and Purse, R. 2014. Defining cybersecurity, *Technology Innovation Management Review*, 4 (10), pp. 13-21.

[5] Von Solms, R. and Van Niekerk, J. 2013. From information security to cyber security. *Computers & Security*, 38, pp. 97–102. DOI: https://doi.org/10.1016/j.cose.2013.04.004.

[6] Da Veiga, A. D. and Eloff, J. H. P. (2007) 'An information security governance framework', Information Systems Management, 24(4), pp. 361–372. DOI: 10.1080/10580530701586136.

[7] Webb, J., Ahmad, A., Maynard, S. B. and Shanks, G. 2014. A situation awareness model for information security risk management. *Computers & Security*, 44, pp. 1–15. DOI: 10.1016/j.cose.2014.04.005.

[8] Relia, S. 2016. *Cyber warfare: its implications on national security*. Delhi: Vij Books India Pvt Lt.

[9] Kotulic, A. G. and Clark, J. G. 2004. Why there aren't more information security research studies. *Information &*

Management, 41(5), pp. 597–607. DOI: 10.1016/j.im.2003.08.001.

[10] Verkerke, A. 2015. Towards a cyber approach for large organisations, Master thesis, Delft University of Technology, the Netherlands.

[11] Centre for Strategic and International Studies, CSIS 2015. The evolution of cybersecurity requirements for the U.S. financial industry. Available from: https://www.csis.org/analysis/evolution-cybersecurityrequirements-us-financial-industry (Accessed: 18 January 2016).

[12] Rahman, S. and Donahue, S. 2010. Convergence of corporate and information security. *International Journal of Computer and Information Security*, 7(1), pp. 63-68.

[13] Le, N. and Hoang, D. 2016. Can maturity models support cyber security?, *In proceeding of 2016 IEEE 35th International Performance Computing and Communications Conference* (IPCCC). DOI: 10.1109/pccc.2016.7820663.

[14] Soomro, Z. A., Shah, M. H. and Ahmed, J. 2016. Information security management needs more holistic approach: A literature review. *International Journal of Information Management*. 36(2), pp. 215–225. DOI: 10.1016/j.ijinfomgt.2015.11.009.

[15] Chang, H., C. 2016.The synergy of scientometric analysis and knowledge mapping with topic models: modelling the development trajectories of information security and cybersecurity research. *Journal of Information & Knowledge Management*, 15 (4), pp. 1650044-1-1650044-33. DOI: 10.1142/S0219649216500441.

[16] Ramirez, R. and Choucri, N. 2016. Improving interdisciplinary communication with standardized cyber security terminology: a literature review. *IEEE Access*, 4, pp. 2216-2243.

[17] Ernst & Young 2015. Enterprise risk management: an integrated approach towards effective and sustainable risk management. Available at: http://www.ey.com/Publication/vwLUAssets/EY-enterpriserisk-management/$FILE/EY-enterprise-risk-management.pdf (Accessed: 8 August 2016).

[18] Cicognani, A. 1998. On the linguistic nature of cyberspace and virtual communities. *Virtual Reality*, 3(1), pp. 16–24. DOI: 10.1007/bf01409794

[19] Min, K. S., Chai, S.W. and Han, M. 2015. An international comparative study on Cyber security strategy. *International Journal of Security and Its Applications*, 9 (2), pp. 13–20. DOI: 10.14257/ijsia.2015.9.2.02.

[20] Bainbridge, W. S. 2007. The scientific research potential of virtual worlds. *Science*, 317(5837), pp. 472–476. DOI: 10.1126/science.1146930.

[21] Gartner 2016. Tech trends 2016: innovating in the digital era. Available at: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/technology/DUP_TechTrends2016.pdf (Accessed: 10 October 2016).

[22] Mindell, D.A. 2000. Cybernetics: knowledge domains in engineering systems. Available at: http://web.mit.edu/esd.83/www/notebook/Cybernetics.PDF (Accessed: 10 October 2016).

[23] Mitra, A. and Schwartz, R. L. 2006. From Cyber space to Cybernetic space: Rethinking the relationship between real and virtual spaces. *Journal of Computer-Mediated Communication*, 7(1), pp. 0–0. DOI: 10.1111/j.10836101.2001.tb00134.x.

[24] Kurbalija, J. 2014. *An introduction to internet governance*. 6th ed. Switzerland: DiploFoundation. Available at: (http://www.diplomacy.edu/sites/default/files/An%20Introduction%20to%20IG_6th%20edition.pdf (Accessed: 11 October 2016).

[25] Henderson, H. 2009 *Encyclopedia of computer science and technology*. New York: Chelsea House Publishers.

[26] Burgess, P. J. (ed.) (2010) The Routledge handbook of new security studies. United Kingdom: Routledge.

[27] DeFranco, J. F. 2013 *What every engineer should know about cyber security and digital forensics*. Taylor & Francis Group: Boca Raton.

[28] Ma, J., Ning, H., Huang, R., Liu, H., Yang, L., Chen, J. and Min, G. 2015. Cybermatics: a holistic field for systematic study of cyber-enabled new worlds'. *IEEE Access*, 3, pp. 2270-2280.

[29] Hagen, J. M., Albrechtsen, E. and Hovden, J. 2008. Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16 (4), pp. 337-397. DOI: 10.1108/09685220810908796.

[30] Olijnyk, N. 2015. A quantitative examination of the intellectual profile and evolution of information security from 1965 to 2015', *Scientometrics*, 105(2), pp. 883-904. DOI: 10.1007/s11192-015-1708-1.

[31] Thomson, K. L. and Von Solms, R. 2005 Information security obedience: a definition. *Computers & Security*, 24 (1), pp. 69-75.

[32] Dlamini, M., Eloff, J. and Eloff, M. 2009. Information security: the moving target. *Computers & Security*, 28 (34), pp. 189-198. DOI: 10.1016/j.cose.2008.11.007.

[33] Kaplan, J., Bailey, T., Rezek, C., O'Halloran, D. and Marcus, A. 2015. *Beyond cybersecurity: protecting your digital business.* Hoboken, New Jersey: John Wiley& Sons.

[34] Reid, R. and Van Niekerk, J. 2014. From information security to cyber security cultures. *Information Security for South Africa*, pp. 1-7.

[35] Bojanc, R. and Jerman-Blažič, B. 2008. An economic modelling approach to information security risk management. *International Journal of Information Management*, 28(5), pp. 413–422. DOI: https://doi.org/10.1016/j.ijinfomgt.2008.02.002.

[36] Pieters, W. 2011. The (social) construction of information security. *The Information Society: An International Journal*, 27 (5), pp. 326-335. DOI: 10.1080/01972243.2011.607038.

[37] Spears, J. L. 2006. Defining Information Security, In *Proceedings of the 5th Security Conference*, Las Vegas: Nevada. Available at: http://www.isy.vcu.edu/~gdhillon/Old2/Old/secconf/pdfs/11.pdf (Accessed: 14 April 2017).

[38] British Standard Institution 2012. BS ISO/IEC 27032:2012 Information technology. Security techniques. Guidelines for cybersecurity.

[39] British Standard Institution 2013 PAS 555:2013 Cyber security risk-governance and management specification.

[40] British Standard Institution 2016 BS ISO/IEC 27000:2016 Information technology. Security techniques. Information security management systems. Overview and vocabulary.

[41] Kovacich, G. L. and Halibozek., E. 2003. *The manager's handbook for corporate security: establishing and managing a successful assets protection progra*m. Burlington: Butterworth-Heinemann.

[42] Zammani, M. and Razali, R. 2016. An empirical study of information security management success factors, *International Journal of Advanced Science, Engineering and Information Technology*, 6 (6), pp. 904-913.

[43] UK Cabinet Office 2015. Digital and technology skills: cyber security and information assurance. Available at: https://www.gov.uk/guidance/digital-and-technologyskills/cyber-security-and-information-assurance (Accessed: 26 April 2017).

[44] Cherdantseva, Y. and Hilton, J. 2015. Understanding information assurance and security, in "Secure*BPMN - a graphical extension for BPMN 2.0 based on a Reference Model of Information Assurance & Security" PhD Thesis, Cardiff University, UK, 2014. Available at: http://users.cs.cf.ac.uk/Y.V.Cherdantseva/UnderstandingIAS.pdf (Accessed: 21 April 2017).

[45] Deibert, R.J. and Rohozinski, R. 2010. Risking security: policies and paradoxes of Cyberspace security. *International Political Sociology*, 4(1), pp.15–32.DOI: 10.1111/j.17495687.2009.00088. x.

[46] Laudon, K. C. And Laudon, J. 2010. *Management information systems: managing the digital firm*. 11th edn. London: Pearson Education, Ltd.

[47] Turban, E. and Volonino, L. 2010. *Information technology for management: transforming organisations in the digital economy*. 7th edn. Hoboken: John Wiley & Sons.

[48] Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F. 2014. Current challenges in information security risk management. *Information Management & Computer Security*, 22(5), pp. 410–430. DOI: 10.1108/imcs-07-20130053.

[49] Rubino, M. and Vitolla, F. 2014. Corporate governance and the information system: How a framework for IT governance support ERM. *Corporate Governance: The International Journal of Business in Society*, 14(3), pp. 320– 338. DOI: 10.1108/cg-06-2013-0067.

[50] Calder, A. and Watkins, S. 2012. *IT Governance: an international guide to data security and ISO27001/ ISO27002*. London: Kogan Page Limited.

[51] Nazareth, D. L. and Choi, J. 2015. A system dynamics model for information security management. *Information & Management*, 52(1), pp. 123–134. DOI: 10.1016/j.im.2014.10.009.

[52] Singh, N. A., Gupta, M. P. and Ojha, A. 2014. Identifying factors of "organisational information security management". *Journal of Enterprise Information Management*, 27(5), pp. 644–667. DOI: 10.1108/jeim-072013-0052.

[53] Kouns, J. and Minoli, D. 2010. *Information technology risk management in enterprises environments: a review of industry practices and practical guide to risk management teams*. Hoboken: John Wiley & Sons, Inc.

[54] Hampton, J. J. 2015. *Fundamentals of Enterprise risk management: how top companies assess risk, manage exposure, and seize opportunity*. 2nd edn. New York: American Management Association.

[55] Bayuk, J. L., Healey, J., Schmidt, J., Weiss, J., Sachs, M. H., and Rohmeyer, P. 2012. *Cyber security policy guidebook*. United States: Wiley.

[56] Collards, G., Ducroquet, S., Disson, E. and Tallens, G. 2017. A definition of information security classification in cybersecurity context, In *Proceedings of the 11th International Conference on Research Challenges in Information Science* (RCIS), IEEE/IET Electronic Library (IEL), pp. 77-82.DOI: 10.1109/RCIS.2017.7956520.

[57] European Parliament, Directorate-General for Internal Policies, Policy Department Citizens's Right and Constitutional Affairs 2015. Cybersecurity in the European Union and beyond: exploring the threats and policy responses. Available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU (2015)536470_EN.pdf (Accessed: 1 April 2017).

[58] Siponen, M. and Willison, R. 2009. Information security management standards: Problems and solutions. *Information & Management*, 46 (5), pp. 267–270. DOI: 10.1016/j.im.2008.12.007.

[59] Dawson, M., Eltayeb, M. and Omar, M. 2017. *Security solutions for hyperconnectivity and the Internet of things*. 1st ed. Hershey, PA: Information Science Reference.

[60] Financial Industry Regulatory Authority 2015. Report on cybersecurity practices. Available at: https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf (Accessed: 20 January 2016).

[61] Julisch, K. 2013. Understanding and overcoming cyber security anti-patterns. *Computer Networks*, 57 (10), pp. 2206–2211. DOI: 10.1016/j.comnet.2012.11.023.

[62] Ponemon Institute 2013. *Managing cyber security as a business risk: cyber insurance in the digital age*. Available at: http://www.ponemon.org/local/upload/file/Cyber%20Insurance%20white%20paper%20FINAL%207.pdf (Accessed: 12 June 2015).

[63] British Standard Institution 2017. BS ISO/IEC 27003:2017. Available at: https://bsol-bsigroup-com.ezproxy.brunel.ac.uk/Bibliographic/BibliographicInfoData/000000000030286014 (Accessed: 26 April 2017).

[64] Ernst & Young 2014. Cyber program management: identifying ways to get ahead of cybercrime. Available at: http://www.ey.com/Publication/vwLUAssets/EYcyberprogram-management/$FILE/EY-cyber-programmanagement.pdf (Accessed: 31 March 2015).

[65] Kitchenham, B. and Charters, S. 2007. Guidelines for performing systematic literature reviews in software engineering, Evidence-Based Software Engineering (EBSE) Technical Report Engineering. Available at: https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf (Accessed: 17 September 2017).

[66] Boland, A., Cherry, G. and Dickson, R. (ed.) 2014. *Doing a systematic review: a student's guide.* Sage Publications Ltd.

[67] Posthumus, S. and Von Solms, R. 2004. A framework for the governance of information security. *Computers & Security*, 23(8), pp. 638–646. DOI: 10.1016/j.cose.2004.10.006.

[68] Finland's Cyber Security Strategy Government Resolution 2013, Available at: https://www.enisa.europa.eu/topics/national-cyber-securitystrategies/ncssmap/FinlandsCyberSecurityStrategy.pdf (Accessed: 25.04.2017).

[69] Committee on National Security Systems 2010. National information assurance (IA) glossary. Available at: https://www.hsdl.org/?view&did=7447 (Accessed: 10 October 2016).

[70] Humphreys, E. 2010. Information Security Risk Management. Available at: http://shop.bsigroup.com/upload/Standards%20&%20Publications/publications/BIP0076-Chapter1.pdf (Accessed: 21 April 2017).

[71] Federation of European Risk Management Associations 2017. At the junction of corporate governance and cybersecurity. Available at: http://www.eciia.eu/wpcontent/uploads/2017/06/OFFSET-PRINT-BrochureFERMA-2017v3-1.pdf (Accessed: 01 February 2018).