2018

Review of cybersecurity frameworks: context and shared concepts

Riza Azmi
University of Wollongong, ra873@uowmail.edu.au

William J. Tibben
University of Wollongong, wjt@uow.edu.au

Khin Than Win
University of Wollongong, win@uow.edu.au

Review of cybersecurity frameworks: context and shared concepts

Abstract

In an effort to develop strong cyber resilience, international organisations, academic institutions, corporations and countries have been actively working to develop cybersecurity frameworks (CSFs). Such efforts emphasize various perspectives depending on the organisation's intention, while their contents involve the same concept. The aim of this paper is to incorporate the many varied perspectives on CSFs and gather them into a concise view by contrasting different intentions and distilling shared concepts. To do so, this study uses the document analysis method alongside two cycles of coding (descriptive coding and pattern coding) to excerpt 12 extant CSFs. The various intentions can be cascaded with respect to four areas: 1) the promoted action, 2) the driver, 3) the framework milieu and 4) the audience. The frameworks can also be examined according to three common concepts: 1) shared actions, 2) cyber pillars and 3) the framework life cycle. A total of seven shared actions are distilled from the frameworks, while the human, organisational, infrastructure, technology and law and regulation pillar are the most frequently discussed excerpts from the CSFs. Moreover, there are three processes for securing cyberspace: profiling, delivering and assuring. The shared concepts presented in this paper may also be useful for developing a general model of a CSF.

Disciplines

Engineering | Science and Technology Studies

Publication Details

Azmi, R., Tibben, W. & Win, K. (2018). Review of cybersecurity frameworks: context and shared concepts. Journal of Cyber Policy, 3 (2), 258-283.

Review of cybersecurity frameworks: context and shared concepts

Authors:

Riza Azmi, ra873@uowmail.edu.au

William Tibben, wjt@uow.edu.au

Khin Than Win, win@uow.edu.au

Centre for Persuasive Technology and Society
Faculty of Engineering and Information Sciences
University of Wollongong
Northfield Avenue, New South Wales, Australia, 2500

Abstract

In an effort to develop strong cyber resilience, international organizations, academic institutions, corporations and countries have been actively working to develop cybersecurity frameworks (CSFs). Such efforts emphasize various perspectives depending on the organization's intention, while their contents involve the same concept. The aim of this paper is to incorporate the many varied perspectives on CSFs and gather them into a concise view by contrasting different intentions and distilling shared concepts. To do so, this study uses the document analysis method alongside two cycles of coding (descriptive coding and pattern coding) to excerpt 12 extant CSFs. The various intentions can be cascaded with respect to four areas: 1) the promoted action, 2) the driver, 3) the framework milieu and 4) the audience. The frameworks can also be examined according to three common concepts: 1) shared actions, 2) cyber pillars and 3) the framework life cycle. A total of seven shared actions are distilled from the frameworks, while the human, organizational, infrastructure, technology and law and regulation pillar are the most frequently discussed excerpts from the CSFs. Moreover, there are three processes for securing cyberspace: profiling, delivering and assuring. The shared concepts presented in this paper may also be useful for developing a general model of a CSF.

Keywords: cybersecurity framework, cybersecurity policy, cybersecurity strategy, cybersecurity shared actions, cyber pillars, framework life cycle

1 Introduction

The steep rise of digital activity in modern life has created the need for strong cyber resilience. One important aspect of developing such resilience is the creation of cybersecurity policies (CSPs) that are able to coordinate and reinforce the efforts of a range of stakeholders (Henschke and Ford 2016; Pawlak and Barmpaliou 2017; Tiirmaa-Klaar 2016). Guiding policymakers in the development of CSPs are cybersecurity frameworks (CSFs). Writing CSFs has been the work of intergovernmental organizations (IGOs), non-governmental organizations (NGOs), academic institutions, corporations and governments (ITU 2017a). From 2004 to 2015, twelve CSFs have been proposed.

CSFs are commonly advocated with the intention of helping policymakers to define cybersecurity strategy by way of a policy template. Given the proliferation of CSFs, how do policymakers adopt a normative position by which to judge their value and utility? CSFs vary widely in terms of, for example, engagement focus (global vs. regional), applicability (new vs. existing), and areas of improvement (identify vs. address) (ITU, 2016). The needs of countries and organizations vary widely in terms of economics and culture, so it is not straightforward to choose a template without understanding the underlying assumptions and goals of the framework authors. We found limited work comprehensively and systematically reviewing CSFs (i.e. the work of Sabillon et al. 2016). To that end, this paper endeavours to develop a 'bird's-eye view' on CSFs to better assist policymakers in their deliberations.

In an attempt to create a single reference outline for all existing frameworks, this paper aims to sketch shared concepts underlying the current frameworks. The paper describes the systematic extraction of shared concepts using a qualitative coding method (Saldana 2015). Accordingly, the paper enables an evidence-based appraisal of current cybersecurity policies.

2 Domain of cyber security: conundrum

Although the term cybersecurity is prominently used in modern conversations and statements (CCDCOE 2017), this term is regarded as interchangeablewith other security domain terminology, such as information security, network security and internet security. As such definitions and explanations diverge, questions arise as to whether: (1) cybersecurity is actually information security; (2) information security is part of cybersecurity; (3) cyberattacks are uniquely associated with information/data; and (4) cybersecurity is replacing information security (von Solms and von Solms 2018).

Apart from such debates, in order to clarify the position taken, we attempt to inclusively consolidate some definitions of cybersecurity while simultaneously trying not to be too broad. The following narrowed-down definition of 'cybersecurity' will be used to delineate the research in this paper. Throughout the paper, by cybersecurity we mean:

> securing a virtual digital environment by governance, management and assurance, including *its assets* (i.e. information assets and cyber assets), *entities* (such as end users, organizations, governments, societies, machines and software), and *interactions* (enabled by IT infrastructure, communications/networks, systems and devices)
>
> (acknowledging definition from ISACA 2013; ISO/IEC 2013; ITU 2012; von Solms and van Niekerk 2013; WEF 2012a).

We also consolidate the definition of 'framework' used in this study, since different terms are used in each document (see the CSF list in ITU 2016, or refer to Table 1). Although CSFs are expressed by different names, and various terms are used, by framework we mean a document that is intended to support policymakers in defining their cybersecurity strategies. Throughout this paper, CSF is defined as

> a document that is promoted with the intention of helping policymakers (i.e., the government or the C-level in an organization) to define cybersecurity strategy/policy by way of a policy template.

Therefore, the term 'framework' in this paper is inclusive of the terms 'agenda' (ITU 2017b, 2012; Schjølberg 2007), 'cybersecurity strategy' (EC 2013; OAS 2004), 'cybersecurity framework' (BSA 2010; NIST 2014), 'model' (GCSCC 2014), and 'principles', 'guideline' and 'manual' (CTO 2015; ISO/IEC 2012; Microsoft 2013; WEF 2012b).

3 Methodology

In this paper, we use the grounded theory paradigm to capture the essential concepts shared across CSFs as well as the differences between them. Grounded theory is commonly used to illuminate concepts based on empirical phenomena and is compatible with an inductive process of analysing data (Roman et al. 2017; Scott and Glaser 1967). The specific application of the grounded theory paradigm relies on document analysis (Bowen 2009). In doing so, we apply a four-step research protocol: 1) defining the research scope, 2) document selection, 3) coding and 4) synthesizing the concept (see Figure 1).

INSERT FIGURE 1

Figure 1. Research protocol

3.1 Defining the scope of research

As a guide to achieving this study's goal, we define three research questions:

RQ.1 What perspectives and contexts are perceived in CSFs?

RQ.2 What shared concepts are evident in CSFs?

RQ.3 What common life cycles are suggested when developing a cybersecurity strategy?

RQ.1 is intended to compare and contrast CSFs, as their purposes and intentions vary. RQ.2 is intended to capture the shared essential concept by distilling the frameworks. Finally, in RQ.3, we seek to identify the common lifecycle considered for securing cyberspace.

3.2 Document selection method

The method used to collect and select the research artefacts (i.e. appropriate CSF documents) for this study is divided into two filtering steps: 1) defining the search strategy and 2) filtering using the inclusion and exclusion criteria.

We limit our search strategy to documents created by IGOs, NGOs, academic institutions, corporations and governments intended to guide policymakers in defining cybersecurity strategies

by way of a policy template. Therefore, the search strategy incorporates the following keywords, which are input into internet search engines (e.g. Google, Bing): *cybersecurity framework*, *cybersecurity manual*, *cybersecurity guideline*, *cybersecurity standard* and *cybersecurity principle*.

We found 26 documents that are relevant to our search strategy. See Table 1 for a list of the documents.

Table 1. Cybersecurity framework documents

INSERT TABLE 1

Next, to narrow our scope, we apply inclusion and exclusion criteria. We define these as follows.

1. Inclusion criteria:
    a. The document is intended for use as a policy template for cybersecurity strategy, issued by any organization;
    b. The document is a complementary document matched to one included under inclusion criterion (a) that takes the form of a report, matrix or evaluation; and
    c. The document appears in a publicly available data source.
2. Exclusion criteria
    a. The document serves as a policy template for another security domain (i.e. information security, network security, internet security);
    b. The document is solely intended as a cybersecurity report, matrix or evaluation;

In selecting the relevant framework we decide to omit those which are not aligned to our definition (see section 2). For example, the ISO/IEC 27001 framework focuses largely on information security but limitedly recognizes the global importance of interaction in cyberspace (ISO/IEC 2013). Similarly, some CSFs focus exclusively on IT infrastructure, such as NERC Critical Infrastructure Protection (CIP) (NERC 2017). We also omit overly operational and overly technical frameworks, since we aim to study a policy template. Therefore, there are some frameworks that are not included in this paper such as the ETSI Cyber Security Standard (TC CYBER 2018) and RFC 2196 (IETF 1997). Since our definitions in section 2 imply that cybersecurity works across national and organizational borders (the ITU definition[1]), this study embraces frameworks that are purposely designed to address national interests, such as the Microsoft CSF (Microsoft 2013).

After applying the inclusion and exclusion criteria, we were left with 17 documents, which fall under 12 frameworks, as shown in Table 2. The CSF documents for the following analysis were compiled from 2004 to 2014. Table 2 shows the list of frameworks sorted by their year of initial creation.

Table 2. Cybersecurity frameworks from IGOs, NGOs, academic institutions, corporations and governments

INSERT TABLE 2

3.3 Coding technique

Along with the document analysis method, we employ a two-cycle coding technique (Saldaña 2013). In the first cycle of coding, we group the concepts using *descriptive coding*. Concepts are gathered and grouped according to the pattern that emerged in each document.

[1] "Cybersecurity is information security with jurisdictional uncertainty and attribution issues." (ITU 2012, p. 11)

To develop a general understanding, a context is derived based on the patterns that appeared from the first cycle. In the second cycle, we use a *pattern coding* technique (Saldaña 2013). Codes from the first cycle are grouped if they share a similar understanding. We used NVIVO software to facilitate the coding process.

Thus, in the next sections, we divide our discussion into two main parts. The first part, which is presented in section 4, includes our findings as we compare and contrast the existing frameworks. The discussion in this part focuses on elaborating the descriptive coding outcomes: the strategic actions, drivers, framework environments and audience of the different CSFs. The second part, which is presented in section 5, reports our findings elaborating similar concepts shared across the frameworks (coding and synthesis).

4 Cybersecurity frameworks: the various contexts

Differences can be detected in every CSF that depend on the framework setting or context. We define the *context* that influences the framework, as each framework has unique aspects or distinctive circumstances. We typify the context into four background factors: 1) promoted action, 2) driver, 3) milieu and 4) audience.

The promoted action is the desired or recommended action that links to the core cybersecurity programme. The driver is the factor that motivated the creation of the cyber strategy. The milieu is the situational setting in which the CSF can be used. The audience is the intended user of the CSF. These contexts are summarized in Table 3. Each aspect will be discussed in sub-sections 4.1 to 4.5.

Table 3. Various contexts of cybersecurity frameworks

INSERT TABLE 3

4.1 The promoted action

The promoted action is the approach that the framework recommends the organization take before implementing its cybersecurity strategy. The overall defined direction of the promoted action further describes the conduct of the cyber strategy. The promoted actions in CSFs can be classified into two main categories. The first category promotes collaborative action (*outward strategy*), while in contrast, the second type advocates increasing the cyber capacity of the organization (*inward strategy*).

The first type, positive interdependence, which emphasizes collaborative action, promotes cooperation among the entities in cyberspace. It adopts the idea that cybersecurity is a shared responsibility given the challenges associated with the interdependencies of all cyberspace stakeholders (BSA 2010; EC 2013; ISO/IEC 2012; Schjølberg 2007). Therefore, securing cyberspace is not solely the responsibility of one organization; instead, it should become a shared endeavour and thus requires partnership among the stakeholders (WEF 2012a). This type includes CSFs such as the ISO/IEC 27032, WEF Principles and Guidelines, ITU Global Cybersecurity Agenda, OAS Cybersecurity Strategy and CTO Cybersecurity Guidelines.

In contrast to externally-directed strategic action, the other type of promoted action advocates an inward process and promotes fortifying the organization internally through cyber capacity-building. While the outward promoted action focuses on collaborating to combat cyberthreats, it is also

essential for an organization to have sufficient cyber capacity to be a trusted and strong entity within the network (WEF 2012b). Therefore, some CSFs, such as Oxford University CMM and the NIST Framework, advocate increasing organizational capacity-building, for example by building human resource capacity, strengthening critical information infrastructures, and strengthening internal systems (i.e. regulations, laws and organizational structure).

4.2 The drivers

The analysis of CSFs suggests that cybersecurity strategy can be driven by two factors: risk and values. Risk-centric and value-centric drivers are found to influence actions and the overall development of a cybersecurity strategy. The goal of the first factor, the risk-centric driver, is to minimize the risks caused by cyberthreats. This common driver holds a justified role within cybersecurity strategy because cyberspace is characterized by uncertainty, and risk needs to be assessed and managed (ISACA 2013; Microsoft 2013; NIST 2014).

While some CSFs emphasize preventing the risks caused by cyberthreats, others advise focusing on aligning the values of the organization such as a national commitment or business goals with the cybersecurity strategy. Therefore, the second factor, the value-centric driver, appears in certain contexts to indicate that the creation of the cybersecurity strategy was driven or framed by a certain value (or the country's commitment/outcome-focus thereto (CTO 2015; Klimburg 2012)). For such, drivers that are influenced by the country's commitment can be derived from a state declaration, whether it is directed by the state or by other states (i.e. through treaty) to organizations/communities (i.e. mandates and charters), to private entities/societies (i.e. expectations and political considerations) (Klimburg 2012, pp. 146–90), or based on national values (Schaake and Vermeulen 2016). Within this value-centric context, creating cyber policy means regarding cyberspace not only as an insulated single domain but also as a domain involving the political situation and national strategy (Klimburg 2012). Therefore, securing cyberspace implicates a dynamic situation. For example, the Commonwealth CSF encourages alignment with Commonwealth values, such as protecting fundamental human rights, preserving an open, free and secure cyberspace, increasing democracy, maintaining international peace and security, and encouraging sustainable development (CTO 2015). Within the organization, this can take the form of aligning the business strategy to the security strategy (ISACA 2013; NIST 2014), meaning attaching the cybersecurity function based on the business environment, business values, business purposes, business objectives and security purposes (ISACA 2013; NIST 2014).

The CSFs that advocate for value-centric drivers can be found primarily in the IGO CSFs, such as in the Commonwealth Cybersecurity Strategy Guidelines, EU Cybersecurity Strategy, CCDCOE Cyber Security Framework and ITU-GCA (see Table 4), where the main intention is to promote their institutional values.

Table 4. Aspiring value-centric drivers for developing cyber strategy

INSERT TABLE 4

4.3 The framework milieu

Within the range of CSFs, a single framework cannot be adopted and directly implemented by an organization without knowing whether the environment is suitable. For example, the NIST Framework is not suitable for promoting interdependence, as it was developed for implementation

by the owner of national critical information infrastructure (NIST 2014). Each framework has a different context and scope, which we call the *framework milieu*. The framework milieu is the background and the context for the framework.

Viewing the scope of the milieu, some frameworks are intended to provide a solution at the *organizational level*, while others are intended for use at the *regional level* or the *international level* (which requires a positive interdependence between international cyber entities). At the organizational level, taking the NIST Framework and CMM as examples, the framework can be appropriately implemented given only a narrow scope within the internal organizational setting, such as to strengthen the organization's cyber capacity or critical information infrastructure. Other frameworks, such as the ITU-GCA, have a broad scope, which can only work in international circumstances that need positive interdependence between each entity, such as through international cooperation and collaboration. Further frameworks only work for particular audiences. These are usually frameworks that are built for a member of an IGO that has shared institutional values, such as the Commonwealth Cybersecurity Guidelines and the CCDCOE Manual. In this case, the primary purpose of this framework is to engage with each member sharing the institutional values.

Based on those cases, we can divide the environmental setting (*milieu*) into three levels with respect to their different circumstances, engagement and scope: the first level is the organizational level, the second is the regional level, and the third is the international level. The organizational level typically addresses increasing the capacity of the organization, while the other two target positive interdependence. The organizational framework can be used as a framework complementary to a higher-level framework; for example, the CMM, ISACA and NIST frameworks can be used to strengthen the organizational level, while the organization may also implement another high-level framework alongside an organizational type framework. The regional framework is typically built to address the specific needs of the country members, which have similar shared institutional values, such as the OAS Cybersecurity Strategy for OAS members or the Commonwealth Cybersecurity Guidelines for Commonwealth countries. Finally, the international framework type emphasizes positive interdependence that is cooperative and collaborative with any organization with the same interests.

4.4 The audiences

The audience or the intended users of CSFs can be divided into two audience categories: (1) the audience-specific CSF and (2) the across-the-board CSF. CSFs with the first type of audience are primarily devoted and addressed to specific organizations that share institutional values within the originating organization. Therefore, these CSFs are created for a specific type of audience. For example, the NIST Framework was developed in response to Presidential Executive Order 13636[2], as this framework was initially built for the critical information infrastructure operator in the United States of America. Other examples include CSFs that were built by an IGO, such as the OAS Cybersecurity Strategy, the EU Cybersecurity Strategy and the Commonwealth Cybersecurity Guidelines, which were created for their country members by an IGO and aligned with the IGO's mission. This occurred because most IGOs, such as OAS, ITU, EU/ENISA, NATO/CCDCOE and CTO,

[2] The Presidential Executive Order 13636 ("Improving Critical Infrastructure Cybersecurity,") was issued on 12 February 2013 and calls for the development of a voluntary risk-based Cybersecurity Framework (NIST Framework).

developed their CSFs with a focus on advocating their country members' creation of a cybersecurity strategy.

The second type of CSF has general applicability in terms of its audience and focuses on helping organizations increase their capacity to reduce cyberthreats; these can be used by any organization, without them needing to share a similar institutional value background. This type of CSF is usually built by NGOs and academic institutions, such as the University of Oxford, ISO/IEC, Microsoft or the BSA.

While the context of CSFs can be divided into four categories, which are the promoted action (*positive independence* vs. *increasing capacity*), the drivers (*risk-centric* vs. *value-centric*), the framework milieu (*organizational*, *regional* and *international*), and the audience (*audience-specific* vs. *across-the-board)*, frameworks can have demi-classifications, meaning that it is possible for classifications to fall between categories. For example, while the NIST Framework was developed based on the Presidential Executive Order, it can be used by organizations or critical infrastructure companies outside the USA. A similar situation is observed for the WEF Framework, which is intended for its members who focus on securing economic relationships. However, the principles and guidelines in the framework can potentially be adopted globally by any organization.

5 Cybersecurity frameworks: shared concepts

Although there are various perspectives on and contexts for CSFs, we also see that there are some similarities shared across the frameworks. For example, the CMM Section D2-1 mentions the *Cyber Security Mindset* (GCSCC 2014, pp. 19–20), which is similar to the Commonwealth Cybersecurity Guideline '*developing a culture of Cybersecurity awareness among citizens*' (CTO 2015, p. 11). Considering these two concepts, we can see that they share a similar principle, which is developing a *cyber culture*. To extract this shared concept, we use two cycles of coding as described earlier: *descriptive coding* and *pattern coding*.

The first cycle is descriptive coding, which aims to excerpt similar concepts from the frameworks into codes. We find that there are thirty shared concepts from the documents (see Figure 2 and Table 5).

The second cycle summarizes the thirty concepts into a smaller number of sets or themes to gain a better normative position of the current frameworks. Using *pattern coding,* we assemble the thirty codes into two main themes, which are 1) *based on similar actions* and 2) *based on objects that need to be secured* (we call this a cyber pillar).

The process behind these two cycles of coding is presented in Figure 2. The middle figure represents shared concepts identified in the documents. The figure on the left represents the cybersecurity pillar. These pillars are used to support and underpin cybersecurity. The figure on the right represents the shared actions. The frameworks commonly promote these actions to secure cyberspace.

We also highlight the common life cycle of securing cyberspace, which is called the *cybersecurity life cycle*. The *cybersecurity life cycle* is a series of processes and a step-by-step routine for securing cyberspace as a project that usually comprises the processes of initial planning, process implementation and evaluation.

These findings will be elaborated upon in the next sections.

INSERT FIGURE 2

Figure 2. Theme development process

5.1 Cybersecurity framework actions

Table 5 shows the concepts shared among CSFs. We have composed the shared concepts from the 12 frameworks using NVIVO and descriptive coding. In Table 5, we group the shared concepts into themes based on their similarity of action (see the shaded columns) using pattern coding. We found that there were seven themes that contribute to the CSF: building online trust, creating coordination, cooperation and collaboration, profiling the cyber state, promoting uptake, reviewing, establishing a legal environment, and creating standards. A detailed discussion will be elaborated in sections 4.1.1 to 4.1.7.

Table 5. Shared concepts of cybersecurity frameworks

INSERT TABLE 5

5.1.1 Building online trust

In creating a cybersecurity strategy, some CSFs recommend that policy creation should focus on enhancing the confidence of stakeholders in the online environment or building online trust. It means not only giving stakeholders (e.g. consumer, business and the government) confidence in the online form (BSA 2010) but also ensuring the availability of infrastructure (in other words, increasing the resilience of infrastructure and servicing critical information infrastructure (ITU 2012)). This can be achieved, for example, by providing a data protection and privacy regulation framework (BSA 2010), developing a national cyber contingency plan/national crisis management (EC 2013; Klimburg 2012), and providing critical information protection (Klimburg 2012).

There are three shared concepts that contribute to building online trust:

1. Increasing digital redundancy: to maintain resilience and capabilities of services that are impaired due to a cybersecurity event.
2. Protecting critical assets in cyberspace: to protect intangible and tangible critical assets, such as privacy, data and infrastructure.
3. Promoting privacy online: to protect personally identifiable information against unauthorized access and disclosure.

5.1.2 Coordination, cooperation and collaboration

Given the wide range of cybersecurity protection necessary, including protection at the personal, societal, organizational, national and international levels as well as securing global cyberspace, it cannot be handled solely by one entity. Protecting cyberspace requires cooperation from every entity, and moreover, the cyber environment needs a cumulative defence. This means that each entity needs to continually work to maintain (and improve) its cyber capacity in order to be a trusted player in cyberspace (WEF 2015). As a result, protecting cyberspace demands action to ensure coordination, cooperation and collaboration with all cybersecurity stakeholders.

There are two types of recommended actions on coordination, cooperation and collaboration (CCC). We can divide the actions related to the organizational relationship into external and internal actions. The first category involves outreach to other entities through cooperation and collaboration. Outreach can be achieved, for example, through alliances and partnerships with other organizations, empowering cyber diplomacy and soft power, conducting information sharing on combating threats,

sharing responsibility by promoting inclusion, and increasing the cyber capacity of neighbouring entities (or uptake by third parties).

The second category involves increasing internal coordination (or inward coordination) within an entity's organizational structure. This type of action is intended to increase communication to all of the entity stakeholders, coordinate all entity stakeholders regarding the cybersecurity mandate, and create cyber governance with clear roles and responsibilities.

5.1.3 Profiling the cyber state

Some CSFs recommend measuring the needs and objectives at hand before taking action on protecting cyberspace; this is called profiling the cyber state. The profiling action includes setting goals and related resources that are needed to secure cyberspace, which is a preliminary, preparatory action before the next action begins. Three actions are part of profiling the cyber state: aligning strategy with core values; budgeting and preparing related resources; and formulating assumptions.

The first advised action, aligning strategy, is intended to establish conduct that is coherent with the current core values. The core values should apply as much in cyberspace as in the physical world; for example, they should align with the current business processes (ISACA 2013; NIST 2014). When used at a higher level, such as at the country level, such core values may refer to an existing arrangement (or country commitment), which can be derived from a state declaration such as a treaty, mandate, charter, public expectation or political decision (Klimburg 2012, pp. 146–90).

The second action, budgeting and resourcing, entails defining budgets and resources prior to implementation, such as people, service and infrastructure, and funding. This includes, for example, allocating and ensuring adequate resources (BSA 2010; CTO 2015; GCSCC 2014; ISACA 2013; Microsoft 2013), taking stock of the status of key elements of the strategy (ENISA 2012a), and pairing and assigning goals to resources using metrics (ISACA 2013; Klimburg 2012; NIST 2014).

The third action, formulating assumptions, means assessing what the organization needs in the context of the cyber environment. This includes, for example, creating risk profiles, profiling the assets that should be protected, determining what security requirements are needed, assessing vulnerabilities, establishing pre-conditions, and setting the overall goals or target to be achieved. Actions in this step are intended to describe the organization's cybersecurity posture and target its cybersecurity state as well as to identify and prioritize the context.

5.1.4 Promoting uptake

Promoting uptake means increasing an entity's cyber capacity by promoting the adoption of CSF. In addition to CCC, it is also important to consider actions in relation to other entities in cyberspace (which is discussed in section 5.1.2). Promoting uptake can be considered a significant aspect of this relationship because, to strengthen cybersecurity, it is important to be a trusted organization in cyberspace. The CCC actions and promoting uptake are intertwined. While the CCC reflects outward action to collaborate with all entities and stakeholders, the primary intention of promoting uptake is internally directed strategic action to strengthen the entity so that it is trusted in cyberspace (WEF 2012b).

Promoting uptake means creating a strong cyber environment by empowering various entities (people, the society, organizations and the country). Such action can take the form of increasing awareness, building a cyber culture, investing in research and innovation, using innovative

technology, increasing cyber responsiveness, and conducting training and education on cybersecurity.

5.1.5 Reviewing

Action taken to secure cyberspace also needs to be reviewed to ensure that the cybersecurity programme is delivering on its targets. Reviewing is intended to readjust the strategy and to realign the programme to achieve the intended goal. Examples of such actions include creating audits and logs, receiving feedback, conducting self-assessments, and refining the programme.

Creating audits and logs entails establishing due care and analysis of the current implementation. Audits and logs make it possible to record security incidents, which in turn allows the organization to better apprise, understand and react to the current threat landscape and readjust its strategy to achieve the goal (CTO 2015; ENISA 2014; GCSCC 2014; NIST 2014). Audits and logs can also be used to verify compliance relevant to cyber risk exposure (WEF 2012b).

Aside from creating audits and logs, action also needs to be assessed. Programme assessment can be conducted internally or by involving an outside observer. The first approach is pursued by conducting self-assessments, for example, by creating metrics or key performance indicators (KPIs) (CTO 2015; ENISA 2012b; Microsoft 2013), continuous monitoring (WEF 2012b), and benchmarking (GCSCC 2014). The second approach is pursued by receiving feedback. Receiving feedback means involving an outside observer to report on incidents or misconduct activities. An internal observer might miss certain weaknesses, so by receiving feedback from an outsider the organization gains the advantage of using another perspective to improve the programme. Taking this feedback can take the form of organizing cyber exercises (ENISA 2014), receiving feedback from an individual expert or receiving feedback from societies (GCSCC 2014). Programme refinement is the ultimate goal of this step. The aim here is to refine the programme and evaluate it to improve strategy to the extent that continuous improvement is achieved. Evaluating and adjusting the cybersecurity strategy can be achieved by identifying lessons, good practices and bad practices during each activity (ENISA 2012b), and by creating audits and logs and through assessment.

5.1.6 Establishing a legal environment

The legal environment provides a basis for conduct in cyberspace that draws a border between what is permissible and what is misconduct. Appropriate laws and regulations are needed to prevent and deter misconduct (OAS 2004). Most CSFs advise the organization to determine what legal conduct is and to establish a legal environment. Establishing a legal environment involves creating a legal framework as a basis for distinguishing between legal and illegal activities in cyberspace. Establishing a legal environment can also be used as a rationale to take corrective action against malicious activities in cyberspace. The theme of establishing a legal environment is distilled from the shared action included in some frameworks, ranging from defining policies to creating strategies and frameworks to policy enforcement.

Defining policies means creating a legal rationale for conduct. When defining such policy, the CSFs recommend considering some specific aspects:

1. The policy should recognize the nature of the internet (BSA 2010; EC 2013), meaning that it should preserve openness and the free flow of information (EC 2013; OECD 2012).
2. The policy should keep pace with all aspects of modern cybercriminal activity (BSA 2010; NIST 2014).

3. The policy should encourage cooperation and be designed using existing international and regional frameworks as references (EC 2013; GCSCC 2014; ITU 2012; NIST 2014; OAS 2004; Schjølberg 2007).
4. The policy should be used to minimize risk and as a form of deterrence against misuse (CTO 2015; ISO/IEC 2012; OAS 2004; WEF 2015).

Policy implementation should also create a strategy and framework, meaning it must develop a strategy, mechanism and roadmap that function as a tactical or even a direct mandate to secure cyberspace. Implementation is intended to actually deliver operational national cybersecurity (Klimburg 2012). The strategy and framework should responsively adapt to changing socio-political, threat and technology environments and integrate across all policy domains (GCSCC 2014; ITU 2017b; WEF 2014).

One important pillar in establishing the legal environment is enacting laws, which can be done by law enforcement. Law enforcement means enacting cybersecurity law by taking corrective action in response to misconduct. Since cybercrime rings span the globe and have a broad set of stakeholders and a broad scope, there are some advised considerations for law enforcement:

1. Law enforcement should be employed as a tool to deter and punish cybercrime (BSA 2010; Schjølberg 2007).
2. Law enforcement must engage across jurisdictions; therefore, addressing cybercrime demands international cooperation and coordination (BSA 2010; ENISA 2012b; Schjølberg 2007).
3. Enforcing the law in cyberspace requires a comprehensive understanding of both innovative technology and appropriate legal approaches, as well as sufficient specialized resources and capabilities (i.e. investigators, prosecutors and judges) to cover cybercrime offences (BSA 2010; GCSCC 2014; Schjølberg 2007; WEF 2014).

5.1.7 Creating standards

Protecting cyberspace requires effective and efficient action, which can be realized by adopting best practices and standardizing conduct. These can be accomplished by creating a standard, which also means promoting interoperability and systemizing conduct.

Promoting interoperability means following recognized cybersecurity standards that are accepted internationally. There are some recognized standards from standards organizations that can be employed as a policy template, guideline or technology (OAS 2004).

Organizations can also standardize their conduct by developing and establishing a minimum requirement of conduct. An example of this is creating practical and effective implementation programmes and technical guidelines. This action aims to minimize overlapping action between one entity and others. For example, the Law Enforcement Governance Framework, which standardizes legal conduct, is used to minimize overlapping functions and structures across investigatory, policymaking and regulatory bodies against cybercrime (ITU 2012).

5.2 Cybersecurity pillars

In addition to grouping shared concepts into certain themes, we can also see that, from another perspective, the CSFs discuss securing similar objects. In this context, we call these objects pillars. As in a building's structure, these pillars are used to support and underpin cybersecurity, and they need

to be strengthened together. The shared concepts of the CSF can be merged into similar objects or pillars.

Through the theme development process, as depicted in Figure 2 and Figure 3, we conclude that there are five main pillars that build cybersecurity: *human*, *organizational*, *infrastructure*, *technology* and *law and regulation*.

INSERT FIGURE 3

Figure 3. The five pillars of cybersecurity

The *human* pillar is the most fundamental, and arguably the weakest, element of cybersecurity that needs to be secured. While the cyberspace foundation is built by technology, the human drives and controls it (ISACA 2013, pp. 72–4). Since humans represent the main actor enabling cybersecurity, lack of awareness and insufficient knowledge makes humans the major challenge and the most vulnerable pillar relative to the others. In addition, addressing knowledge inadequacies is not a straightforward task as it requires education, training and time. This is the reason why CSFs recommend promoting uptake by increasing awareness, developing a cybersecurity culture, and providing training and education to strengthen this pillar.

The *organizational* pillar focuses on the institutions inside cyberspace. It is the functional structure that controls cyberspace. Strengthening this pillar can be further separated into two tactics, namely, (1) internally directed strategic action such as increasing the capacity and capability of the organization and (2) externally directed strategic action, which is intensifying cooperation to secure cyberspace. For example, the first tactic can be realized by securing the budget and resources for the organization and increasing responsiveness to cyberthreats. However, each organization in cyberspace also needs to cooperate with the others, such as by creating clear roles and responsibilities for each organization, coordinating stakeholders, sharing information on threats, and creating alliances and partnerships.

The *infrastructure* pillar is the most critical element of cyberspace. It is the environment that constitutes cyberspace. Without infrastructure, cyberspace is nothing; therefore, strengthening this pillar is necessary for supporting the cyber environment. If this pillar is weak, transactions in cyberspace could collapse. Therefore, most CSFs address infrastructure issues, including how to secure critical information infrastructure. The NIST Framework is the most pertinent for securing the critical information infrastructure. In most cases, the CII differs from one organization to another, depending on each organization's needs and cyber profile.

The *technology* pillar is the pillar that empowers cyberspace. As cyberspace comprises the most advanced technology (ITU and ABIresearch 2014), strengthening this pillar primarily entails adopting the leading technology, such as by espousing technology that supports cybersecurity and enabling research and development.

The *law and regulation* pillar structures cybersecurity and creates a coercive environment in cyberspace. This pillar focuses on strengthening the systems within cyberspace, such as creating a national cyber ecosystem by creating a regulatory framework and creating norms and standards, as well as law enforcement. Although some argue that cyberspace should not be regulated and should remain free from government and politics (Barlow 1996), legal conduct is still needed to maintain stability in cyberspace.

It is interesting to reflect on the ITU pillars and contrast these with the pillars outlined above. The ITU pillars divide cybersecurity into five working areas – legal, technical and procedural, organizational, capacity-building and international cooperation.

We argue that the five above-mentioned pillars may best describe the critical cyber aspects inside an institution that need to be strengthened. The pillars depicted in Figure 2 cover comprehensive aspects of building cybersecurity and are grounded in 12 recognizable frameworks.

Three of the five ITU working areas (technical and procedural, organizational and international cooperation) can be covered by the organization pillar. This organization pillar acts as the functional structure that controls cyberspace, which according to the finding overarches two main functions: inward strategic action (increasing the capacity and capability of the organization, which encompasses the technical and procedural, capacity-building and organizational pillars of ITU), and outward strategic action (intensifying cooperation to secure cyberspace, as in the international cooperation pillar in the ITU work area).

We also note that there are two main aspects that are not covered by the ITU work areas: the infrastructure and technology pillars. These two pillars are the foundation that build cyberspace. While we recognize that capacity-building is important for building up cybersecurity, we tend to include it as an embedded aspect in the human and organization pillars.

5.3 Cybersecurity framework life cycle

Implementing a cybersecurity project is not straightforward, with the organization building a strategy and deploying actions, and the programme being run as planned; accordingly, it must be a repeatable process, incorporating continuous improvement, monitoring and analysis (ENISA 2014; ISACA 2013). Therefore, some CSFs recommend following a continuous, step-by-step process. We define this as the *cybersecurity life cycle.*

Accordingly, the *cybersecurity life cycle* is a series of processes and a step-by-step routine for securing cyberspace as a project; it comprises the processes of initial planning, process implementation and evaluation. The output of the evaluation phase is used to maintain and adjust the strategy (ENISA 2012b, p. 7) and as an input for replanning cyber strategy. As we can associate securing cyberspace with a project, this process can be found in nearly every framework. An example of this life cycle is shown in Table 6.

Table 6. Cybersecurity framework life cycle

INSERT TABLE 6

From Table 7, we can see that the life cycle process comprises three common steps: profiling the cyber state, delivering the strategy, and evaluation. The profiling process is intended to profile the current cyber situation, i.e. to identify, plan, determine requirements, set targets, profile and assess the current situation of the cyber state. The second step, which is the main step, is to deliver the programme, namely, to execute the programme and facilitate implementation. The last step is an evaluation of the programme, a review of the results, and an adjustment of the strategy. Evaluation results from the final step are employed to refine the programme and used in cybersecurity replanning. Those steps are found in all CSFs; they are excerpted from the various terms but refer to similar concepts.

Table 7. Cybersecurity life cycle map

INSERT TABLE 7

Since the overall life cycle comprises important life cycle processes, the common understanding of the life cycle can be divided into *profiling, delivering* and *assuring*, allowing the life cycle to be mapped (as shown in Table 7). The three processes combine into a continuous process, which is drawn as a cyclic process model in Figure 4.

INSERT FIGURE 4

Figure 4. Three processes of cybersecurity

The *profiling* process is intended to define the current cyber state. Various terms are used to refer to profiling. For example, ISO uses 'plan', ITU uses 'ends', NATO uses 'preliminary consideration', WEF uses 'starting assumption', Microsoft uses 'establishing clear priorities and security baselines', CTO uses 'approach' and ISACA uses 'plan and design'. These common terms refer to a process taken before cybersecurity is implemented. The profiling process is a *planning process created by developing the assumptions, aligning with core values, budgeting, gathering resources and establishing a legal environment*.

The *delivering* process is the core action for securing cyberspace. This process should be pursued based on the assumptions listed in the profiling process. Some CSFs use an explicit term such as 'protect' (NIST), 'do' (ISO), 'ways-means' (ITU) or 'implement and operate' (ISACA), while others use implicit terms that primarily describe the main actions in the CSF. The delivering process entails implementing actions for securing cyberspace based on the assumptions developed in the profiling process, such as building online trust, creating CCC and promoting uptake.

The *assuring* process is the review of the overall process of delivering and the result of feedback gathered to ensure a better cybersecurity process. Cyber assurance is a way to reshape the quality of cybersecurity output that meets the desired goal. The assuring process entails reappraisal (i.e. audit, feedback, self-assessment and creating metrics), modification (in response to the internal and external situation) and refinement (of operation and strategy).

5.4 Cybersecurity framework: shared concept mapping

The two perspectives of pillars and life cycles can be combined to create a generalized cybersecurity strategy (See Table 8). The first view is of the *process* to secure cyberspace, which mainly falls into *profiling, delivering* and *assuring*. The second view considers what objects need to be strengthened in cyberspace or the *cybersecurity pillars*, namely, *human, organization, infrastructure, technology,* and *law and regulatory*.

As we can see in Table 8, strengthening the five cyber pillars can be divided into (1) profiling the current cyber state, (2) delivering the security actions based on the profile, and (3) ensuring that the security delivery is on track and provides feedback to the first process. Table 8 shows the overall shared concept of a CSF.

Table 8. Summary of cybersecurity framework

INSERT TABLE 8

6 Concluding remarks and limitations

This paper began with the aim of identifying shared concepts across 12 CSFs and classifying their differences. Using the grounded theory paradigm, we divide the CSFs into two main parts: context and shared concepts.

In seeking cybersecurity policy, one noteworthy question to ask is what drives its development (Pawlak and Barmpaliou 2017, p. 124). This question leads to comprehending organizations' initiatives on developing CSFs through apprehending the CSFs' distinctive features. In this study, we found that the development of CSFs can generally be reflected by: 1) *promoted action* (positive interdependence vs. increasing capacity), 2) *driver* (cyber risk vs. promoting values), 3) *framework milieu* (organizational, regional and international), and 4) *audience* (audience-specific vs. the across-the-board CSF).

In addition, understanding CSFs as a normative concept is an ongoing endeavour. As indicated in the work of the ITU (2018) there is a desire to develop generic strategies that can be applied globally, such as by creating a cybersecurity toolkit. Therefore, addressing the question that leads to the development of general cybersecurity concepts contributes to the development of a general model of cybersecurity policy.

Attempting to respond to that inquiry, this study has mapped the normative position of CSF onto three central concepts, encompassing the *seven action themes*, *five pillars/objects* and *three-process life cycle*. The seven action themes that are frequently discussed in the CSFs are, namely, 1) *building online trust*; 2) *coordination, cooperation and collaboration*, 3) *profiling the cyber state*, 4) *promoting uptake*, 5) *reviewing*, 6) *establishing a legal environment*, and 7) *creating standards***.** We also raise five pillars or cybersecurity objects that are most often discussed in CSFs, namely, *human*, *organization*, *infrastructure*, *technology* and *law and regulation*. In addition, the three-process life cycle includes *profiling*, *delivering* and *assuring*.

This work contributes in several ways. Policymakers or C-level executives could benefit from the depiction of distinctive features summarized in section 4, which may help them in choosing the right policy template for their organizational purpose. Section 4 provides a normative position on existing CSFs. By narrowing down the organizational purpose and searching for the best-fit context for their organization, policymakers and C-level executives can select a suitable CSF for their organization. For example, a company may use the NIST framework, CMM or ISACA framework as their policy template, as these are suitable for increasing the cyber capacity of the internal organization, rather than emphasizing an international relationship, which we would find in other CSFs such as the ITU framework and Microsoft Cybersecurity Manual. To that end, policymakers seeking to develop a cybersecurity strategy can allocate resources to areas that will contribute to its successful implementation. It is also potentially possible to allocate these resources over a time period to account for the different areas of development of the life cycle.

Researchers could benefit from reviewing the mapping concept of the CSF summarized in Table 8. The seven shared actions, the five pillars and the three life cycles are mapped in this table, providing researchers with a bird's-eye view of current CSFs. This mapped table can also be used for

developing a general model of a CSF, since the finding comprehensively covers all elements in every CSF strategy.

In future development of this work, the five pillars, three life cycles and seven shared actions identified in Table 8 may be used as an instrument to benchmark cybersecurity progress in an institution as a Cybersecurity Balanced Scorecard. A dashboard containing the five pillars can be used to monitor the development of cybersecurity, since these pillars thoroughly cover all aspects of CSFs that need to be watched, while at the axis, the three life cycles can be used to monitor state progress for developing cybersecurity, such as in the beginning state (profiling), executing state (delivering) and reviewing state (assuring). In addition, the seven shared actions in the cross-section cell can be used to advocate a direction to policymakers or C-level executives when taking required action. Features in the finding were simplified and summarized but embrace all strategies.

While the distinctive features and shared concepts raised in this paper reflect a number of themes identified in the CSFs and represent several contributions of this paper, the paper also has some potential limitations. First, although this paper did not intend to oversimplify the concepts involved in securing cyberspace in all CSFs, grouping a number of concepts and paragraphs into a concise view, however, potentially detracts from the essential concept brought by each CSF. Consider the example of when we discussed the profiling theme: we defined profiling the cyber state as generically as we could. It can refer to profiling the cyber state of the organization as well as profiling the cyber state in a larger institution, such as a country. However, we attempted to avoid oversimplifying the concepts gathered from the CSFs. Second, this work has been conducted by a group of researchers. Therefore, the discussion reflects the researchers' views of the overall CSF during the work. Third, we made limited use of document analysis alone as the main methodology in this work (Bowen 2009). However, the literature suggests using document analysis alongside other methodologies to corroborate findings, such as by triangulating data or employing mixed-methods studies.

Acknowledgment

The first author would like to acknowledge the Indonesia Endowment Fund for Education (Lembaga Pengelola Dana Pendidikan – LPDP) for its scholarship funding support.

References

Barlow, J. P. 1996. "A Declaration of the Independence of Cyberspace". https://projects.eff.org/~barlow/Declaration-Final.html (accessed January 11, 2018)

Bowen, GA. 2009. "Document analysis as a qualitative research method." *Qualitative Research Journal* ;9:27–40. doi:10.3316/qrj0902027.

BSA (Business Software Alliance). 2010. *BSA Global Cybersecurity Framework.* Washington DC, USA: Business Software Alliance (BSA).

CCDCOE (Cooperative Cyber Defence Centre of Excellence). 2018. Cyber Definitions. Resources 2017. https://ccdcoe.org/cyber-definitions.html (accessed February 1).

CTO (Commonwealth Telecommunications Organisation). 2015. *Commonwealth Approach for Developing National Cybersecurity Strategies: A Guide to creating a cohesive and inclusive approach to delivering a safe, secure and resilient cyberspace.* 2015th ed. London, United Kingdom: Commonwealth Telecommunications Organisation (CTO).

EC (European Commission). 2013. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Brussels: European Commission (EC); 2013. doi:10.4271/2010-01-1021.

ENISA (European Union Agency for Network and Information Security). 2014. *An evaluation Framework for National Cyber Security Strategies*. Heraklion, Greece: European Union Agency for Network and Information Security (ENISA). doi:10.2824/3903.

ENISA (European Union Agency for Network and Information Security). 2012a. *National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace*. Heraklion, Greece: European Network and Information Security Agency (ENISA).

ENISA (European Union Agency for Network and Information Security). 2012b. *National Cyber Security Strategies: Practical Guide on Development and Execution*. Heraklion, Greece: European Network and Information Security Agency (ENISA). doi:10.2824/3903.

GCSCC (Global Cyber Security Capacity Centre). 2014. *Cyber Security Capability Maturity Model* (CMM). Version 1. Oxford: Global Cyber Security Capacity Centre (GCSCC), University of Oxford.

Henschke A, Ford SB. 2016. "Cybersecurity, Trustworthiness And Resilient Systems: Guiding Values For Policy". *Journal of Cyber Policy* 8871:1–14. doi:10.1080/23738871.2016.1243721.

IETF (Internet Engineering Task Force). 1997. RFC 2196. Req Comment 2196. https://www.ietf.org/rfc/rfc2196.txt (accessed May 28, 2018).

ISACA (Information Systems Audit and Control Association). 2013. *Cybersecurity Nexus: Transforming Cybersecurity*. Illinois, USA: Information Systems Audit and Control Association (ISACA).

ISO/IEC (International Organization for Standardization/International Electrotechnical Commission). 2013. ISO/IEC 27001:2013 - *Information Security Management*. Geneva: ISO/IEC.

ISO/IEC (International Organization for Standardization/International Electrotechnical Commission). 2012. ISO/IEC 27032:2012 *Information technology — Security techniques — Guidelines for cybersecurity*. Geneva: ISO/IEC.

ITU (International Telecommunication Union). 2018. National Strategies. ITU-D Cybersecurity. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx (accessed July 12, 2018).

ITU (International Telecommunication Union). 2017a. National Strategies. ITU-D Cybersecurity. http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx (accessed August 17, 2017).

ITU (International Telecommunication Union). 2017b. *Global Cybersecurity Index* (GCI) 2017. Geneva, Switzerland: International Telecommunication Union (ITU).

ITU (International Telecommunication Union). 2016. *National Cyber Security Strategy (NCS) Toolkit*. http://www.itu.int/en/ITU-D/Cybersecurity/Documents/National Strategy Toolkit introduction.pdf (accessed August 17, 2017).

ITU (International Telecommunication Union). 2012. ITU *National Cybersecurity Strategy Guide*. Geneva: International Telecommunication Union (ITU).

ITU (International Telecommunication Union) and ABIresearch. 2014. *Global Cyber Security Index*. New York: ITU and ABIresearch.

Klimburg A, editor. 2012. *National Cyber Security Framework Manual*. Tallin: NATO Cooperative Cyber Defence Centre of Excellence. doi:9789949921119.

Microsoft. 2013. *Developing a National Strategy for Cybersecurity: Foundations for Security, Growth, and Innovation*. Microsoft.

NERC (North American Electric Reliability Corporation). 2017. NERC Critical Infrastructure Protection (CIP) Standard. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (accessed May 28, 2018).

NIST (National Institute of Standards and Technology). 2014. *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1. New York: National Institute of Standards and Technology (NIST).

OAS (Organization of American States). 2004. "A Comprehensive Inter-American Cybersecurity Strategy: Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity". In: *Inter-Americaan Committee Against Terrorism*. Montevideo, Uruguay: Organization of American States (OAS).

OECD (Organisation for Economic Co-operation and Development). 2012. *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*. vol. 211. No.322. OECD Publishing. doi:http://dx.doi.org/10.1787/5k8zq92vdgtl-en.

Pawlak P, Barmpaliou P-N. 2017. "Politics of cybersecurity capacity building: conundrum and opportunity." *Journal of Cyber Policy* 2:123–44. doi:10.1080/23738871.2017.1294610.

Roman DJ, Osinski M, Erdmann RH. 2017. The construction process of grounded theory in administration. Contaduría y Adm. doi:10.1016/j.cya.2016.06.012.

Sabillon R, Cavaller V, Cano J. 2016. "National Cyber Security Strategies: Global Trends in Cyberspace". *Int J Comput Sci Softw Eng* 5:2409–4285.

Saldaña J. 2013. *The Coding Manual for Qualitative Researchers*. Second Edi. Singapore: SAGE Publications Asia-Pacific Pte Ltd.

Schaake M, Vermeulen M. 2016. "Towards a values-based European foreign policy to cybersecurity". *Journal of Cyber Policy* 1:75–84. doi:10.1080/23738871.2016.1157617.

Schjølberg S. 2007. *The Report of the Chairman of High-Level Experts Group (HLEG) on the ITU Global Cybersecurity Agenda* (GCA). Geneva, Switzerland: International Telecommunication Union (ITU).

Scott JC, Glaser BG. 1967. The Discovery of Grounded Theory: Strategies for Qualitative Research. vol. 36. 2006th ed. New Brunswick. doi:10.2307/2094063.

von Solms B, von Solms R. 2018. "Cybersecurity and information security – what goes where?" *Inf Comput Secur* 26:2–9. doi:http://dx.doi.org/10.1108/ICS-01-2015-0001.

von Solms R, van Niekerk J. 2013. "From information security to cyber security". *Comput Secur* 38:97–102. doi:10.1016/j.cose.2013.04.004.

TC CYBER (Technical Committee Cyber). ETSI 2018. Cyber Security Standard. ETSI Cyber Secur Stand.

Tiirmaa-Klaar H. 2016. "Building national cyber resilience and protecting critical information infrastructure". *Journal of Cyber Policy* 1:94–106. doi:10.1080/23738871.2016.1165716.

WEF (World Economic Forum). 2015. *Global Risks 2015: Insight Report*. 10th Editi. Cologny/Geneva Switzerland: World Economic Forum (WEF).

WEF (World Economic Forum). 2014. *Risk and responsibility in a hyperconnected world: Implications for enterprises*. Geneva, Switzerland: World Economic Forum (WEF).

WEF (World Economic Forum). 2012a. *Risk and Responsibility in a Hyperconnected World: Pathways*

to Global Cyber Resilience. Geneva, Switzerland: World Economic Forum (WEF). doi:270912.

WEF (World Economic Forum). 2012b. *Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World - Principles and Guidelines*. Geneva, Switzerland: World Economic Forum (WEF).

Table 1. Cybersecurity framework documents

Years	Documents
2004	A Comprehensive Inter-American Cybersecurity Strategy: a Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity (OAS 2004)
2007	The Report of the Chairman of High-Level Experts Group (HLEG) on the ITU Global Cybersecurity Agenda (GCA) (Schjølberg 2007)
2009	Cybersecurity Guide for Developing Countries (ITU 2009)
2010	BSA Global Cybersecurity Framework (BSA 2010)
2012	Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the internet Economy (OECD 2012)
2012	Risk and Responsibility in a Hyperconnected World Pathways to Global Cyber Resilience (WEF 2012)
2012	National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace (ENISA 2012b)
2012	ITU National Cybersecurity Strategy Guide (ITU 2012)
2012	Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World - Principles and Guidelines (WEF 2012a)
2012	Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience (WEF 2012b)
2012	National Cyber Security Framework Manual (Klimburg 2012)
2012	ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity (ISO/IEC 2012)
2012	National Cyber Security Strategies: Practical Guide on Development and Execution (ENISA 2012a)
2013	ISO/IEC 27001:2013 - Information Security Management (ISO/IEC 2013)
2013	Transforming Cyber Security (ISACA 2013)
2013	Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (EC 2013)
2013	Developing a National Strategy for Cybersecurity: Foundations for Security, Growth, and Innovation (Microsoft 2013)
2014	An Evaluation Framework for National Cyber Security Strategies (ENISA 2014)
2014	Risk and Responsibility in a Hyperconnected World: Implications for Enterprises (WEF 2014)
2014	Framework for Improving Critical Infrastructure Cybersecurity (NIST 2014)

2014	Cyber Security Capability Maturity Model (CMM) (GCSCC 2014)
2014	Commonwealth Cybergovernance Model (Commonwealth 2014)
2015	Cyber Maturity in the Asia-Pacific Region 2015 (ASPI 2015)
2015	Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats (WEF 2015)
2015	Commonwealth Approach for Developing National Cybersecurity Strategies: A guide to creating a cohesive and inclusive approach to delivering a safe, secure and resilient cyberspace (CTO 2015)
2017	Global Cybersecurity Index (GCI) (ITU and ABIresearch 2014, 2015; ITU 2017a)

Table 1. Cybersecurity frameworks from IGOs, NGOs, academic institutions, corporations and governments

ID	Year Started	Framework	Document(s)
[1]	2004	Organization of American States (OAS) Cybersecurity Strategy	A Comprehensive Inter-American Cybersecurity Strategy: a Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity (OAS 2004)
[2]	2007	Global Cybersecurity Agenda (ITU-GCA)	• The Report of the Chairman of High-Level Experts Group (HLEG) on the ITU Global Cybersecurity Agenda (GCA) (Schjølberg 2007) • ITU National Cybersecurity Strategy Guide (ITU 2012) • Global Cybersecurity Index (GCI) (ITU and ABIresearch 2014, 2015; ITU 2017a)
[3]	2010	Business Software Alliance (BSA) Framework	BSA Global Cybersecurity Framework (BSA 2010)
[4]	2012	World Economic Forum (WEF) Principles and Guidelines	• Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World – Principles and Guidelines (WEF 2012a) • Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience (WEF 2012b) • Risk and Responsibility in a Hyperconnected World: Implications for Enterprises (WEF 2014)
[5]	2012	Cooperative Cyber Defence Centre of Excellence (CCDCOE) Manual	National Cyber Security Framework Manual (Klimburg 2012)
[6]	2012	ISO 27032	ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity (ISO/IEC 2012)
[7]	2012	European Union (EU) Cybersecurity Strategy	• National Cyber Security Strategies: Practical Guide on Development and Execution (ENISA 2012a) • Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (EC 2013)
[8]	2013	Microsoft Cybersecurity Manual	Developing a National Strategy for Cybersecurity: Foundations for Security, Growth, and Innovation (Microsoft 2013)
[9]	2013	ISACA Cybersecurity Nexus	Transforming Cybersecurity (ISACA 2013)
[10]	2014	National Institute of Standards and Technology (NIST) Framework	Framework for Improving Critical Infrastructure Cybersecurity (NIST 2014)
[11]	2014	Cyber Security Capability Maturity Model (CMM)	Cyber Security Capability Maturity Model (GCSCC 2014)
[12]	2015	Commonwealth Cybersecurity Guidelines	• Commonwealth Approach for Developing National Cybersecurity Strategies: a guide to creating a cohesive and inclusive approach to delivering a safe, secure and resilient cyberspace (CTO 2015)

ID	Year Started	Framework	Document(s)
			• Commonwealth Cybergovernance Model (Commonwealth 2014)

Table 3. Various contexts of cybersecurity frameworks

Year	Framework	Promoted action	Driver	*Milieu*	Audience
2004	OAS Cybersecurity Strategy	Positive interdependence	Risk-centric	Regional	OAS member country
2007	ITU-GCA	Positive interdependence	Value-centric	International	ITU members
2010	BSA Framework	• Positive interdependence • Increasing cyber capacity	Risk-centric	International	Government
2012	WEF Principles and Guidelines	• Positive interdependence • Increasing cyber capacity	Risk-centric	International	WEF members
2012	CCDCOE Manual	• Positive interdependence • Increasing cyber capacity	Value-centric	Regional	NATO members
2012	ISO27032	Positive interdependence	Risk-centric	International	Organization
2013	Microsoft Cybersecurity Manual	• Positive interdependence • Increasing cyber capacity	Risk-centric	International	Government
2013	EU Cybersecurity Strategy	Positive interdependence	Value-centric	Regional	EU members
2013	ISACA Cybersecurity Nexus	Increasing cyber capacity	• Value-centric • Risk-centric	Internal Organization	Organization
2014	NIST Framework	Increasing cyber capacity	• Value-centric • Risk-centric	Internal Organization	Organization
2014	CMM	Increasing cyber capacity	Risk-centric	Internal Organization	Organization
2015	Commonwealth Cybersecurity Guidelines	Positive interdependence	• Value-centric • Risk-centric	Regional	Commonwealth country

Table 4. Aspiring value-centric drivers for developing cyber strategy

Frameworks	Aspiring drivers
CCDCOE Manual	National security drives the creation of the National Cybersecurity Strategy, which should account for the following: • The 5 mandates • The 5 dilemmas
Commonwealth Cybersecurity Guidelines	Applying the Commonwealth principles
EU Cybersecurity Strategy	• Promoting EU values • Protecting fundamental rights • Access for all • Democratic and efficient multi-stakeholder governance • A shared responsibility to ensure security
ITU-GCA	Mandated from the High-Level Experts Group (HLEG) meeting, which is asking for a commitment by member countries to a Global Cybersecurity Agenda (GCA) to work on five key Work Areas: • Legal • Technical and procedural • Organisational structures • Capacity-building; and • International cooperation.
OAS Cybersecurity Strategy	Mandated by the following resolutions: • AG/RES. 2004 Cybersecurity Strategy (RESOLUTION) • AG/RES. 1939 (XXXIII-O/03) Development of an Inter-American Strategy to Combat Threats to Cybersecurity
NIST Framework	Business Strategy
ISACA Framework	Business Strategy

Table 5. Shared concepts of cybersecurity frameworks

Shared concepts	Definition	Doc	Freq
Building online trust	To enhance the confidence of all stakeholders in using cyberspace	15	228
Digital redundancy	To maintain resilience and capabilities or services that were impaired due to a cybersecurity event	3	11
Protecting critical assets of cyberspace	To protect intangible and tangible critical cyber assets, such as privacy, data and infrastructure	11	27
Promoting privacy online	To promote protection of identifiable information against unauthorized access and disclosure	13	170
Creating coordination, cooperation and collaboration	To coordinate, cooperate and collaborate with cyber security stakeholders including external and internal organizational entities	17	371
External	Outward actions	16	167
Alliancing and partnering	To cooperate with other entities with the same mutual benefit to combat cyber threats and respond to events and incidents	12	62
Diplomacy and soft power	To use the ability to define international norms and standards relevant to international behaviour in cyberspace, representing a form of 'soft power'	3	4
Information sharing	To cooperate by sharing information regarding threats and attacks to keep up-to-date with the latest threats and developments	12	50
Promoting inclusion	To promote inclusion and share responsibility across all stakeholders in cybersecurity	12	32
Third-party uptake	To ensure that third parties not directly subject to internal organizational policies adhere to cybersecurity	8	23
Internal	Inward actions	16	202
Communication	To engage with all actors to communicate the strategy	6	17
Coordination	To coordinate across the internal system on cybersecurity mandates	12	64
Creating a governance	To create set of frameworks and boundaries for security management including an organizational structure, a coordinator or leader, formal policies and guidelines for some aspects of cybersecurity	12	54
Roles and responsibility	To minimize overlapping functions between each organization by creating clear roles and responsibilities	13	66
Profiling the cyber state	To set the goals and budget	14	249
Aligning strategy with core values	To establish a coherent implementation of the current core values	11	87
Budgeting and setting up resources	To define budgets and resources prior to implementation	12	46
Setting up the assumption	To assess what the organization needs and define its context	12	109
Promoting uptake	To fill the gap between unsecure and secure conditions by increasing cyber capacity, capabilities and the resilience of internal stakeholders to achieve the same conditions	16	270

Shared concepts	Definition	Doc	Freq
Awareness	To increase peoples' capacities in and awareness of cyberspace, such as creating security guidance, helping stakeholders understand their roles and responsibilities in cyberspace, and social engagement	13	76
Culture	To promote a cybersecurity culture or a national mindset on cybersecurity	4	14
Research and innovation	To foster research and innovation	10	24
Innovative technology	To update or advance technologies and techniques that are used as reliable tools to fight cybercrime	8	31
Responsiveness	To identify threats early and increase capacity, preparedness and engagement when adapting to threats. This includes creating incident response teams	8	48
Human empowerment	To enhance human resource capacities	13	62
Reviewing	To ensure that the cybersecurity programme is delivered on target	12	173
Audit and log	To establish due care and analysis of the current implementation	7	52
Feedback	To involve outside observers to report incidents of misconduct	5	9
Programme refinement	To refine the programme and evaluate it to achieve strategy improvements, routinely investing effort to continuously improve	9	52
Self-assessment	To identify the emerging trends and needs of evolving cyberspace by developing cyber matrices	10	51
Establishing a legal environment	To develop a legal environment as a basis for drawing legal and illegal activities in cyberspace	16	132
Defining policies	To create a legal rationale to conduct action in cyberspace	13	55
Developing strategy and framework	To develop a strategy, mechanisms and a roadmap that function as tactical and direct governance to secure cyberspace	9	20
Law enforcement	To enact cyber security law by taking corrective action in response to misconduct	10	42
Creating standards	Having best practices and a standard of conduct	15	117
Promoting interoperability	To follow recognized standards, guidelines, conduct, norms and best practices which are open, global and accepted internationally, by relying on global standards, guidelines and practices developed, managed and updated by industry	13	49
Standardizing conduct	To develop and establish minimum conduct requirements, such as creating a practical and effective implementation programme and technical guidelines	8	42
Sources/References		**18**	**1544**

Table 6. Cybersecurity framework life cycle

Framework	Lifecycle
ITU-GCA	Plan-do-check-act
CCDCOE Manual	The NATO Defence Planning Process, which comprises • Step 1 - Establish political guidance • Step 2 - Determine requirements • Step 3 - Apportion requirements and set targets • Step 4 - Facilitate implementation • Step 5 - Review results
ISO27032	Plan-do-check-act

Microsoft Cybersecurity Manual	Risk assessment and management
	• Risk assessment
	  • Risk identification
	  • Risk analysis
	  • Risk evaluation
	• Risk management
	  • Prevention
	  • Detection
	  • Response
	  • Recovery

EU Cybersecurity Strategy	Developing-executing-evaluating-adjusting
NIST Framework	Identify-protect-detect-respond-recover
Commonwealth Cybersecurity Guidelines	Development-delivering-reviewing
ISACA Cybersecurity Nexus	Plan-design-build/acquire/create/implement-use/operate-evaluate/monitor-update/dispose

Table 7. Cybersecurity life cycle map

	Profiling	Delivering	Assuring
ITU-GCA	Plan	Do	Check-Act
CCDCOE Manual	Step 1 - Establish political guidance	Step 4 - Facilitate implementation	Step 5 - Review results
	Step 2 - Determine requirements		
	Step 3 - Apportion requirements and set targets		
EU Cybersecurity Strategy	Developing	Executing	Evaluating
			Adjusting
ISO27032	Plan	Do	Check-act
Microsoft Cybersecurity Manual	Risk identification	Prevention	Recovery
	Risk analysis	Detection	
	Risk evaluation	Response	
NIST Framework	Identify	Protect	Recover
		Detect	
		Respond	
Commonwealth Cybersecurity Guidelines	Development	Delivering	Reviewing
ISACA Cybersecurity Nexus	Plan	Implement	Evaluate
	Design	Operate	Update

Table 8. Summary of cybersecurity framework

	Profiling	**Delivering**	**Assuring**
Human	Budgeting and setting up resources	Awareness	Feedback
	Setting the assumption	Culture	
		Promoting privacy online	
		Training and education	
Organizational	Aligning with core values	Alliancing and partnering	Programme refinement
	Budgeting and setting up resources	Communication	Self-assessment
	Creating governance	Coordination	
	Creating roles and responsibilities	Diplomacy and soft power	
		Information sharing	
		Promoting inclusion	
		Responsiveness	
		Third-party uptake	
Infrastructure	Setting the assumption	Digital redundancy	Audit and log
	Setting the resources	Innovative technology	
		Protecting critical asset of cyberspace	
		Responsiveness	
		Standardising conduct	
Technology	Setting the assumption	Innovative technology	Audit and log
	Setting the resources	Promoting interoperability	
		Research and innovation	
		Responsiveness	
Law and regulatory	Defining policies	Legal investigation	Legal investigation
	Developing strategy and framework	Standardizing conduct	

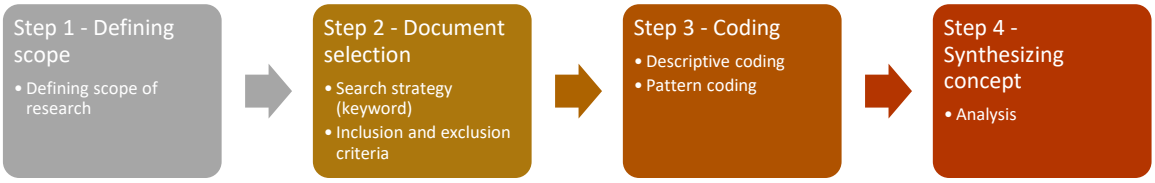

Figure 1. Research protocol

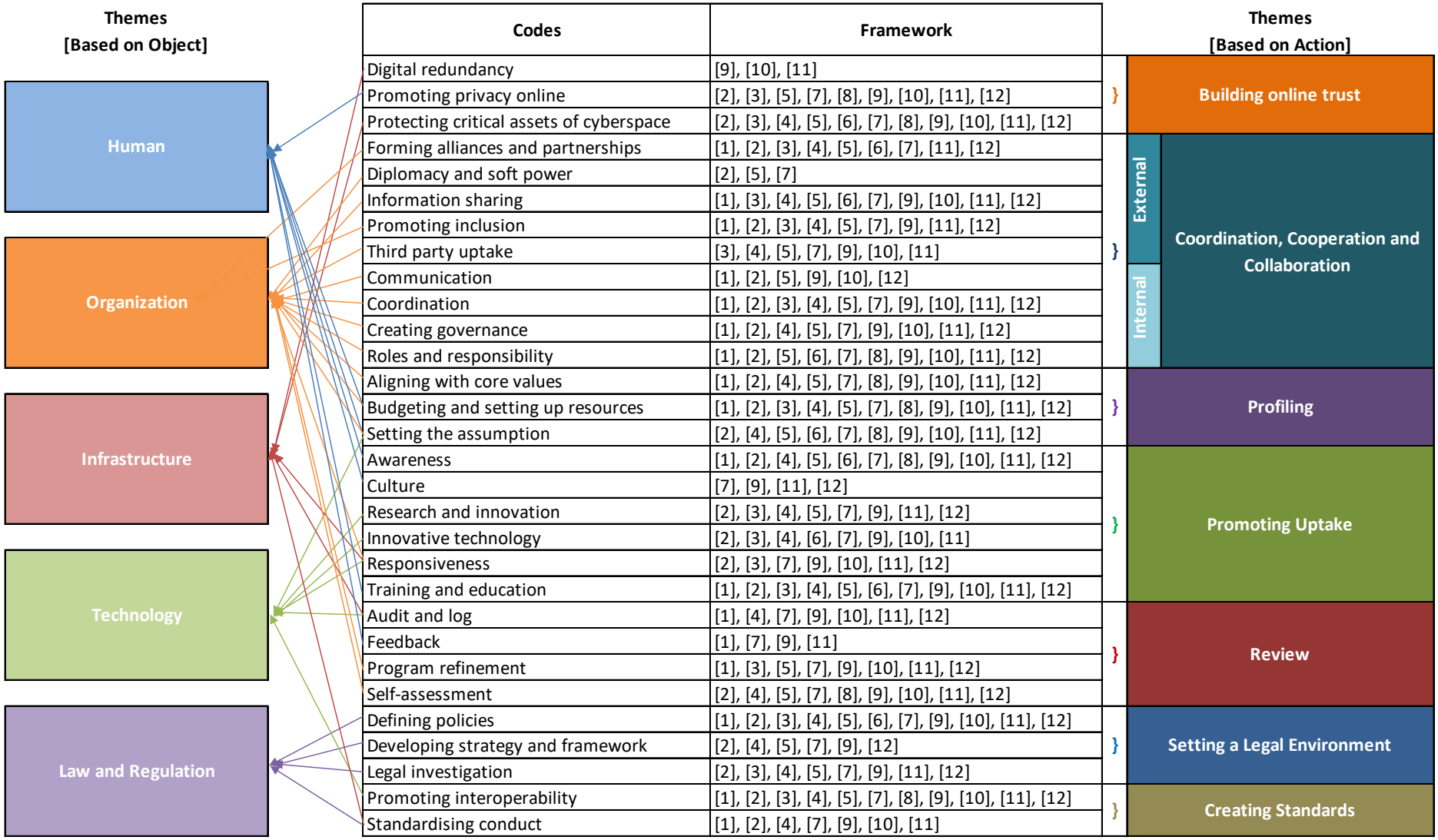

Figure 1. Theme development process

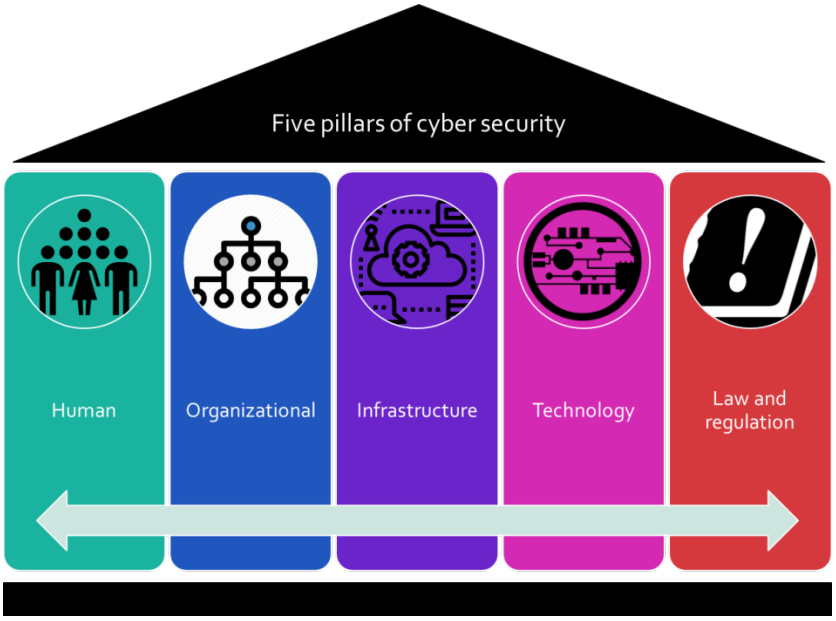

Figure 1. The five pillars of cybersecurity

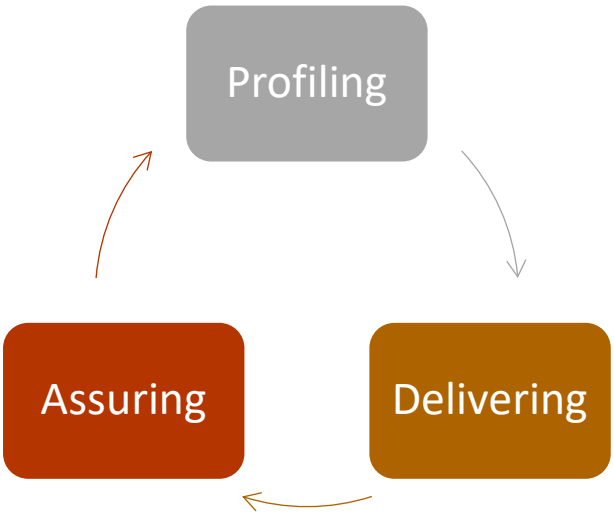

Figure 4. Three processes of cybersecurity