Emerald Information Management and Computer Security

Key Competencies for Critical Infrastructure Cyber-Security: a Systematic Literature Review

Journal:	*Information and Computer Security*
Manuscript ID	ICS-07-2020-0121.R2
Manuscript Type:	Original Article
Keywords:	Skills, Competencies, Cyber-security, Critical infrastructure, Review

Noname manuscript No.
(will be inserted by the editor)

Key Competencies for Critical Infrastructure Cyber-Security: a Systematic Literature Review

the date of receipt and acceptance should be inserted later

Abstract Design/Methodology: This work is based on a systematic literature review (SLR) conducted to identify scientific papers discussing and evaluating competencies, skills and essential attributes needed by critical infrastructure (CI) workforce for cyber-security (CS) and preparedness to attacks and incidents. A total of 29 articles were collected and reviewed during this research, while an additional 8 articles were discussed in the related work section.

Purpose: The purpose of this review can be summarized as to *identify and analyze essential competencies and skills required by CI personnel in CS roles.* More specifically, the objectives of the literature review can be encapsulated in the following points:

- Identify research papers published on the topic: competencies and skills necessary for CI CS;
- Determine main focus areas within the identified literature and evaluate the dependency or lack thereof between them;
- Make recommendations for future research;

Findings: After a comparative analysis of the articles reviewed in this work, a variety of skills and competencies was found to be necessary for CS assurance in CIs. These skills have been grouped in four categories: technical, managerial, implementation and soft skills. Nonetheless, there is still a lack of agreement on which skills are the most critical, and further research should be conducted on the relation between specific soft skills and CS assurance. Also, researchers have not agreed on which methods for training of these skills are most effective.

Research Limitations/Implications: This research relies on the information available from online literature and other documentation to find which skills and competencies are required for CS assurance of CIs. Investigating which skills are required by industry for specific CS roles, by conducting interviews and sending questionnaire/surveys, would allow to consolidate whether literature and industry requirements are equivalent.

Practical Implications: Findings from this literature review suggest that more effort should be taken to conciliate current CS curricula in academia with the skills and competencies required for CS roles in the industry. Additionally, further research should be conducted to understand which are the most effective solutions for CS awareness and training and what other possible solutions could be developed for the same goal.

Originality/Value: This work provides a previously lacking current mapping and review of literature discussing skills and competencies evidenced as critical for CS assurance for CI. The grouping and analysis of skills conducted in this work is also useful to identify the relationships between different skills. The findings of this research are useful for development of comprehensive solutions for CS awareness and training.

Keywords Review · Cyber-security · Critical Infrastructure, Competencies · Skills

1 Introduction

Critical infrastructures(CI) are paramount to the sustained functioning of most sectors of modern societies, to the point where having a robust network of critical infrastructures and providing services through this network has become one of the metrics of judgement for quality of life in advanced nations(Hashim 2011). However, the disruption of any critical infrastructure and their supported social functions can result in devastating financial losses and safety breaches to both individuals and communities. These security concerns

Address(es) of author(s) should be given

have urged nations to make significant investments in protecting critical infrastructures. While physical protection of critical infrastructures used to be the top priority a few year past, nowadays these infrastructures are equally, or arguably more, threatened by cyber-attacks(Hurst, Merabti, and Fergus 2014). To combat this threat, many security standards and guidelines have been developed(Leszczyna 2018) and organizations are adopting an increasing number of security measures, including firewalls, virtual networks, computer forensics tools(Sklyar 2012), intrusion detection and prevention systems(Ibrahim Ghafir, Husák, and Prenosil 2014) and other cybersecurity tools(I. Ghafir et al. 2016). Unfortunately, this has not stopped many malicious parties from conducting successful cyber-attacks on CI.

It has been reported that in 2019 more than half of US organizations have faced successful phishing or ransomware attacks(Davis 2020), with many of them losing data, facing account compromises and providers facing downtimes. The success of these attacks has often not been linked to inadequate implementation or lack of security tools, but to user unawareness and personnel lack of training(Davis 2020; I. Ghafir et al. 2016). In a 2015 study, it has been noted how 20% of security breaches in the same year were the result of infrastructure assets misuse, and 31% were due to human errors(IRM 2015). Another study has found that the root cause of 80% of data breaches can be attributed to stolen data, often obtained through social engineering attacks such as e-mail phishing(Chris 2015). This types of incidents and data have highlighted how the human factor can have as significant of an impact as technical factors(U. Ani, H. He, and Tiwari 2018) and that a systems' security is as weak and vulnerable as the workforce that develops and operates it(U. Ani, H. He, and Tiwari 2018).

Improving the security of CI thus means effectively improving the workforce's security capacity. This can be achieved by increasing the awareness, knowledge, skills and competencies(U. Ani, H. He, and Tiwari 2018) of the personnel, by offering targeted and tailored educational and training modules. To effectively develop successful training programs and other types of educational offerings, it is fundamental to understand which type of competencies and skills are to be developed by the workforce, additionally to knowledge requirements. This means taking into consideration sector and role-specific requirements, as well as individual human traits and behaviours that may influence the ability to respond to incidents and other cyber security duties (Gratian et al. 2018).

In this work, we conduct a systematic literature review with the intent of mapping skills and competencies required by cyber-security personnel to deal with security attacks and threats, with a focus on critical infrastructure.

2 Related Work

To the best of the author's knowledge, a systematic literature review that analyzes and reviews competencies, skills, and other necessary attributes specific to CI cyber-security (CS) has not been conducted yet. Nevertheless, several reviews and surveys have been conducted focusing on CI, industrial control systems and smart grid security measures. These articles have provided useful insight into state of the art regarding CI cyber-security, with some providing comprehensive related work sections and evaluation methodologies which were partially integrated into this work.

Dawson and Thomson (2018) review current research that has been conducted on cyber expertise and which attributes individuals operating in the cyber domain need. In their work, they discuss both technical and social-related skills needed by the cyber-security workforce. Different skills are associated with the different roles that each individual may cover in their work environment. In the review, it is argued that certain personality traits may play a role in the fitness of personnel for specific roles and responsibilities. The authors provide a detailed argumentation for promoting further research in understanding the role of human behavioural traits in cyber-security assurance. In particular, they show that current frameworks for CS awareness and training, such as the NICCS framework, are lacking when it comes to dealing with non-technical aspects of training for CS workforce.

A similar conclusion was also reached by Jacob et al. (2018). In their work, the authors argue that for less technological-related roles in cyber-security, the framework does not provide sufficient job descriptions for specific work roles, provides inadequate competencies and training and career guidance, no predictable outcomes or metrics to determine effectiveness and has other lackluster areas.

Leszczyna (2018), in his study, seeks to identify all standards that define cyber-security requirements applicable to smart grids. The author identifies seventeen standards and analyzes the relationship between the standards to find points of overlap or independency. The author's study was produced according to a systematic literature review based on the approach by Webster and Watson (2002).

The review was composed of three main parts: literature search, literature analysis and standards' selection. The standards' selection was based on a secondary literature search on evaluation criteria of standards, which identified the following criteria: scope, type applicability, range and publication. The author concludes that the requirements specified by different standards differ mostly by the level of technical

detail and thematic coverage. Some standards are found to be complementary to each other while others are independent. He also observes that specific standards are applicable to multiple components of smart grids, while others are limited to one. He finally identifies NISTIR (2014) to be the standard that amalgamates the most requirements and is applicable to a broader range of smart grid components.

Y. Yan et al. (2012) surveys the most common solution on cyber-security for smart grid communications. The author lists the major security requirements in privacy, availability, authentication, integrity, authorization, auditability, non-repudiation, third-party protection, trust components for smart grids as well as high-level security requirements. After identifying current challenges in smart grid cyber-security, the authors survey existing solutions for smart grid communications in each area previously mentioned. The author concludes that solutions for smart grid communication security require a holistic approach that includes traditional schemes, trusted computing elements and authentication mechanisms based on industry standards. Additionally, he highlights the need for cohesive standards and requirements, suggesting to continue the work currently being conducted by the NIST project.

Hurst, Merabti, and Fergus (2014) surveys current and future critical infrastructure security strategies. The author discusses the defence-in-depth strategy as the most adopted solution for critical infrastructure protection. The strategy involves the implementation of multiple layers of security so that even if an attack penetrates one layer, there will be other layers of protection. Finally, the author concludes that integrating conventional security strategies with innovative mechanisms is the only option to avoid attacks from having devastating effects.

Knowles et al. (2015) surveyed the most recent methodologies and research for managing and measuring risk in industrial control systems (ICS) cyber-security. The authors discussed six areas covered by literature on managing risk: maturity model framework approaches for securing ICS through component and architectural design, security evaluation tools, standards and best practices for ICS security, standards and guidelines applicable to specific processes and technologies and finally an examination of security metrics. The author also analyzes the publication. The analysis tries to identify metrics and the extent to which the safety and security relationship is covered. Finally, the author uses the results obtained by the survey and analysis of literature to produce two crucial outputs: the concept of functional assurance to bring together safety and security requirements and an agenda for future research related to ICS security metrics.

Igor et al. (2018) presented in their work the design and results of a survey conducted in order to identify the cyber-security competence centres in Europe. The goal of the survey was to contact and register all cyber-security competence centres across the EU, also sharing information about their work and expertise. The survey was composed of 27 questions, divided in five sections:

- General information;
- Cyber-security expertise;
- Sectors, applications and technologies;
- International collaborations and joint programs;
- Confirmation and agreement with the privacy policy;

The survey was completed a total of 665 times, with 61 centres providing supporting documents. Of particular interest is the analysis of the domains of research of the responders, which shows education and training together with data security and privacy being the two domains covered by most centres. As it can be noted, all these works provide analysis of technical requirements and standards that are either adopted or should be adopted for CI protection. What is neglected or not given enough detail on are the non-technical skills and competencies that need to be directly acquired by CI personnel for effective cyber-security.

Rahim et al. (2015) have conducted a systematic review of approaches to assess cyber-security awareness. The review collected key findings regarding three fundamental aspects of these approaches: methodologies, target audiences and scope of assessment of these approaches. The author narrowed down the review to 23 pertinent articles, which were divided and reviewed based on which of the aspects previously mentioned they focused. The author concluded that although there are several suitable methodologies for cyber-security awareness, there is still a lack of flexibility with using multiple methodologies when conducting one single study. Regarding the audience, the author finds that categorizing users when developing cyber-security messages is fundamental to guarantee reaching the right audiences. Lastly, regarding scope, the author identified areas with high potential of research output, which are currently underdeveloped. In his analysis, the author does not provide a categorization of the various assessment methods analyzed based on the industry sectors of application, leaving unspecified whether the methods would be sufficient for CI cyber-security and which sectors or roles of CI they would be best suited for.

3 Motivation

What motivated the development of this work is the lack of scientific articles determining and reviewing competencies and skills needed for CI cyber-security. As it can be noted in section 2, current literature

does not provide reviews or surveys that are focused on both CI cyber-security and evaluate human competencies specifically instead of technical requirements. Such an evaluation would allow to determine and characterize critical skills for CI cyber-security, based on methodology, application sector, audience and scope. Accordingly, this would permit the development of effective training modules and programs to increase cyber-security awareness and preparedness of future CS workforce.

4 Research Method

This work is based on a systematic literature review (SLR) conducted to identify scientific papers discussing and evaluating competencies, skills and essential attributes needed by CI staff for cyber-security and preparedness to attacks and incidents. The literature review was conducted based on the approach presented by Okoli and Schabram (2010). According to this method, the literature review should be divided into eight major steps:

- Establishing the purpose of the literature review;
- Protocol and training (for any review that employs more than one reviewer);
- Searching of the literature;
- Practical screen;
- Quality appraisal;
- Data extraction;
- Synthesis of studies;
- Writing the review;

4.1 Purpose of the Review

The purpose of the review can be summarized as *identify and analyze essential competencies and skills required by CI personnel in CS roles*. More specifically, the objectives of the literature review can be encapsulated in the following points:

- Identify the research papers published on the topic: competencies and skills necessary for CI cyber-security protection;
- Analyze and evaluate research papers that conduct reviews or surveys on the topic of skills and competencies for CI cyber-security and summarize the methodology and results in a related work section;
- Determine main focus areas within the identified literature and evaluate the dependency or lack thereof between them:
- Make recommendations for future research;

4.2 Protocol and training

Before commencing the systematic literature review, an analysis of the most appropriate methodology was conducted. Several scientific papers that followed Okoli's approach had been consulted. It was found that the methodology adopted by Yamin, Katt, and Gkioulos (2020) shared research and methodology requirements that were aligned with the objectives of our literature review. Accordingly, this work's methodology has been based on the methodology of their work and adapted to our scope and evaluation criteria. As one sole reviewer conducted the literature review, there had been no need for training of other individuals to ensure protocol conformity.

4.3 Searching for the literature

As indicated in section 4.1, the first task to be completed for this literature review was to identify and gather the appropriate papers. To identify and collect scientific articles to be evaluated, the following databases were consulted for extraction of related literature: IEEE Xplore, ACM Digital Library, ResearchGate, Google Scholar, ScienceDirect, Scopus, ProQuest and Semantic Scholar. Different combinations of the following keywords were used to maximize the search output: skills, competencies, cyber security (or cybersecurity), critical infrastructure, energy, nuclear, aviation. While the initial focus of this research was to investigate on skills and competencies for CS in the three previously mentioned sectors of CI (energy, aviation and nuclear), the low amount of research found that focused in these fields and the compatibility of CS skills for these sectors with general skills for CS motivated the expansion of the research focus. The

following conditional logic statement describes how the keywords were combined to create the search combinations: ((Cyber-security OR Cybersecurity) AND (Critical Infrastructure OR Aviation OR Energy OR Nuclear) AND (Skills OR Competencies)). This produced a total of 16 keyword combinations. Examples of possible combinations of keywords used for the literature search are the following:

- Skills + Cyber Security + Critical Infrastructure;
- Competences + Cybersecurity + Energy;

Although we expected this high number of keyword combinations to produce an elevated number of results, with a high likeliness of duplicates, unrelated articles and poor quality articles, this was necessary to avoid omitting any relevant article as part of the review. Articles that were found to be non-valuable to the research were omitted during the next steps. The total number of papers that were found using the keywords combinations was 28100.

4.4 Practical screening

A set of inclusion and exclusion rules was put in place to screen the result of the literature search:

- Only articles written in English were selected;
- Duplicates found through multiple databases were excluded;
- Articles before the year 2000 were excluded, to avoid the use of antiquated data;
- Only scientific articles published in conferences, workshops and journals were selected;
- Articles that were not accessible to the author;

Only articles that followed the complete list of rules were selected, although not all the results of the screening were used for the SLR, as many were discarded in the next steps.

4.5 Quality Appraisal

At this point, two more exclusion rules were set to facilitate the selection of papers. Articles that did not include any combination of keywords in their title, abstract or introduction were discarded. The second round of exclusion was conducted to eliminate further articles that did not contribute to the initial goal: "Identify key competencies and other attributes necessary by cyber-security personnel for critical infrastructure protection". This was done because many of the articles found focused on topics unrelated to this goal or did not provide a comprehensive section or discussion of skills and competencies for CI CS. In fact, many of the results focused on statistical data on cyber-security workforce and threats, cyber-security incident prediction and prevention in the form of software or other tools' usage, cyber-security training and awareness solutions without comprehensive discussions on skills and competencies required and other topics outside of the original scope. For this, articles that did not adequately focus on discussing competencies and skills necessary specifically for cyber-security fields were excluded.

4.6 Data Extraction

To extract and map the key findings of each paper that was utilized in this review, a data extraction review form was created. This form was organized as a table with eight columns representing key attributes that were deemed necessary and sufficient to identify and summarize each paper.

- Title and Year: title of the paper and year of publishing;
- Authors: List of contributing authors;
- Competencies and skills: Any competency and skill specific to CI cyber-security or in some cases general to cyber-security described in the content of the paper;
- Target: Group of individuals that are in need of the competencies and skills mentioned. This usually included cyber-security workforce and students;
- Areas: fields of study, cyber-security and industry areas that the research focuses on or identifies;
- Skill acquisition methods: Methods and tools discussed or developed in the research conducted in each individual paper that can aid in acquiring the skills and competencies that are discussed. The vast majority of studies reported some methods or programs that could be of use, with the exception of a few papers;
- Description: Brief description of the content of the paper;
- Conclusions: Final conclusions and outputs discussed by the authors of the papers;
- Discussion: Our personal discussion and evaluation on the content of the individual paper. This includes any criticism or any unique findings;

4.7 Synthesis of Studies

For the synthesis of the studies, we utilized the qualitative material collected in the data extraction and in the writing of the reviews. The data was later utilized to map skills and competencies in Section 6. Observations on each category of this mapping are then given in the same sections, followed by general recommendations regarding both individual and groups of skills and competencies.

4.8 Writing the Review

Writing this systematic literature review has been conducted in accordance with the standard principles for writing research articles, utilizing the method described by Okoli and Schabram (2010). After the initial search, a total of 28100 articles that satisfied the search criteria was found. This was followed by rounds of practical screenings, to eliminate any non-English result, duplicates, articles before 2000 and other articles that did not respect the criteria described in 4.4. This greatly reduced the number of articles to 2331. After the practical screening, quality appraisal of the remaining articles was conducted with the two rounds described in 4.5 done in the same order as in the description. The first round of quality appraisal reduced the number of articles down to 129. After the second round of quality appraisal, the number of articles, which also composed the final literature review, came down to 29, with an additional 8 articles discussed in the related work section. Additionally, another 32 works were consulted for the purpose of the review and for additional information regarding CI cyber-security. These included articles that provided descriptive or statistical information about CI CS(Davis 2020)(I. Ghafir et al. 2016; Sklyar 2012; U. Ani, H. He, and Tiwari 2018; Luiijf et al. 2011), articles regarding methodologies for systematic literature reviews(Okoli and Schabram 2010; Yamin, Katt, and Gkioulos 2020) or other articles referenced by the ones present in our literature review that provided more detail about specific topics.

5 Literature Review

In this section, to answer the second objective of this work shown in 4.1, the results of the literature review are shown. As mentioned in section 4, the literature review is comprised of 29 articles, discussing skills, competencies and knowledge required by cyber-security personnel for CIP. Before commencing the analysis of the articles, an important clarification must be made. This review will be focusing on articles discussing skills, competencies and abilities needed by CS workers in CI and not behaviours and personal traits. Multiple studies (Lebek et al. 2014; Padayachee 2012; Shropshire, Warkentin, and Sharma 2015; Öğütçü, Testik, and Chouseinoglou 2016) have shown how certain personality and cognitive traits (employees' intentions, attitudes, motivations or satisfaction, etc.) may influence employees security behaviours. Although mentions of these factors and possible interdependencies with specific competencies and skills are presented in this work, when discussed by articles analyzed in the following, it is out of the scope of this work to conduct a comprehensive analysis and mapping of these factors. Additionally, it must be noted that due to the lack of articles that specifically referred to sectors of CI, articles that discussed skills and competences for CS assurance in broader terms were included, if the skills described were deemed applicable to CI domains. To evaluate whether skills were applicable to CI domains, articles that discussed explicitly skills for CI CS were prioritized and articles that showed correlations with the findings of the former group were added. Many of the articles introduced skills and competencies as part of proposed solutions for CS awareness and training, often in the form of training frameworks and modules. Proposed solutions, when available, are also mapped later in section 6, to determine trends when it comes to skill acquisition methods found in the literature.

An example of this is the work conducted by Foo, Branagan, and Morris (2013). The authors propose a post-graduate curriculum that tries to close the gap between the thinking of control system engineers and information technology professionals. The curriculum consists of three sessions: an initial theoretical session, a hands-on practical session and a final debriefing session. The initial course has four main aims: raise awareness of information security issues and how they relate to control systems; raise awareness of issues within control systems; raise awareness in control system engineers of the dangers of cyber attacks and the capabilities of attackers in this area; raise awareness of the particular requirements of deploying information security remediation in the control systems arena. For the practical sessions, intensive five-day courses are proposed. Each course has a different focus, such as system audit, vulnerability analysis, penetration testing, forensic analysis and incident response. While the curriculum proposed by the authors offers a detailed and comprehensive set of interdisciplinary education and various training modules, the lack of evaluation of the curriculum leaves its effectiveness uncertain. Evaluation is especially important for

the hands-on exercises, as it may reveal the need to concentrate some effort in enhancing communication skills and other competencies that are not identified in the initial sessions.

Turkanović, Welzer, and Hölbl (2019) present an overview for a cyber-security education model, which is shaped after the recommendations of the Joint Task Force on Cyber-security Education and the expectations of the Slovene industry. The author identifies a set of interdisciplinary skills in various technical domains and fields, but also non-technical, more human-related skills (such as insider attacks, ethics) that are required by the cyber-security workforce. The model consists of education modules for different Bologna levels, each focusing on a different set of skills and knowledge. The offerings include both lectures and lab work. The primary focus areas of the model are information security and digital forensic fundamentals, which are followed by specialised education and training. The overall format and teachings offered in the model are well encompassing. The author states that further research will be conducted to evaluate the model by adapting it to local university programs. The results of this future analysis will be of great interest to compare the effectiveness of their model to the other proposed models.

LeClair, Abraham, and Shih (2013) propose both an interdisciplinary approach to cybersecurity education and best practices for integrating advanced instructional technologies to online cybersecurity education. Online education, in particular, is discussed as one of the more effective and future-oriented methods of education, as it is analysed to be both effective and approachable by a larger audience than class-bound education. One interesting observation made by the author is the need to motivate the targets to participate in the learning process actively. Project-based learning is suggested as an effective way of addressing this issue. Other benefits of online training are discussed, such as an increase in critical thinking and participation. The author identifies three pillars when it comes to cyber-security education: technology, processes and people. Overall, the author identifies a multi-dimensional process that needs to be incorporated into cyber-security education. This process needs to focus both on technical and non-technical aspects. The skills and competencies identified by the author should be implemented to a concrete framework in order to offer a realistic solution for cyber-security training and education.

Sobiesk et al. (2015) discuss a role appropriate, multi-level, multi discipline approach to cyber education. The authors start by providing a definition and examples of what constitutes *cyber* and the cyber-space. The multi-level offering discussed by Sobiesk et al. is composed of five levels: Cyber in general education, cyber electives, cyber threads, cyber minors and cyber-related majors. Each of these levels offers a different type of cyber-related education, with an increasing amount of specialisation in each subsequent level. The model presented by the authors has been adopted by West Point University, located in the United States. Feedback from the students that have completed the education program or are currently in the completion process would allow for the improvement of the modules and integration of any missing training.

König and Wolf (2018) discusses a competence developing game named GHOST for cyber-security awareness training of businesses. The authors start by analysing the requirements of a successful cyber-security training program. They identify three main motivation for personnel training: development of employee skills, increasing employee motivation and job satisfaction and strengthening the employee company relation. No time available to dispense employees and to miss internal capacity or funds to organise training is identified as the major reason that force companies not to conduct training. Due to the attributes of a game-based approach, these limitations would be addressed. The authors focus on discussing which is the most optimal configuration and interaction system for the game. A touch-based interaction that supports three different points of view is agreed to be optimal. The game consists in 5 different *mini-games*. Each of these has a different focus. Some examples of topics tackled are: handling of foreign flash drives, phishing emails, backups, mobile devices, and many others. This type of approach has multiple benefits, most of which are stated by the authors. From the ease of use to low cost, using a game-based approach can be useful in many scenarios, but mostly in company-oriented training. Key limitations to this type of approach are the relatively low number of topics that can be addressed in a game-based scenario and the limitations that come with the type of interface used.

Luallen and Labruyere (2013) develop a critical infrastructure and control system cybersecurity curriculum. The program, targeted at graduate and undergraduate students. One interesting aspect of the author's research is the use of questionnaires to assess the skill set of the participants and their respective expectations. The course consists of in-class lecture material and pre-class video assignments. Two existing textbooks have been suggested to support the teaching of more theoretical aspects. These lectures are supported by hands-on laboratory exercises listed below:

- PLC relay logic
- Attack a PLC
- Wireshark analysis of communication between a PLC and HMI
- Attack control system communication and operator console

To give additional hands-on experience, students were also assigned critical infrastructure testbed exercises. Overall, the curriculum offered by the author is quite extensive in both technical and practical content. The

curriculum has been positively adapted and refined using the participants' feedback and results. This type of continuous updating is key for guaranteeing a model or a curriculum's validity over the years against new threats and new technologies.

K. Evans and Reeder (2010) discuss the importance of having well trained and educated personnel for each key role of critical infrastructure security. They envision an all-encompassing career path and curriculum, starting from early education to training for experts in the sectors. This type of curriculum would start by providing education in core cyber-security skills (hardware, software, networking and business) and expand to later hands-on experience consisting of specialised training and work-related missions. In their proposal they suggest that the following solutions enhance current proposals in cyber-security workforce education: (i) encouraging younger students to pursue education and training in quantitative fields of science; (ii) develop more rigorous curricula in computer-related disciplines; (iii) automate daily tasks in cyber-security. The authors refer to multiple initiatives and programs that are currently being offered to enhance cyber-security skills for students and workforce. Unfortunately, they do not go into further detail in discussing the specific skills and competencies needed and whether the current offerings were valid and efficient. State-of-the-art laboratory facilities, with the required systems and testbeds, are also discussed by the author.

Mao, Chua, and Liang (2017) propose an infrastructure and curriculum design to support practical experimentation in cyber-security training. Thanks to a collaboration with the University of Singapore, they successfully built and implemented physical labs, designed for open experiments. For the curriculum design, the focus was kept in three areas: System security, Network security and Web security. The curriculum has been implemented for five years. The received feedback from students has been overall positive, although not much further details are given. The article lacks detail when it comes to the description of the single offerings. Additionally, the initial courses are structured, given the assumption that students do not know the subjects. An initial survey or more differentiation between offerings may allow for better efficiency in the teachings.

Svabensky et al. (2018) present two courses and an educational game in a cyber range, to aid students in adversary thinking. The course follows guidelines and standards set by the NSA/DHS CAE and the NIST NICE. The major competencies targeted are cyber defence, cyber threats, networking concepts, network defence, and penetration testing. The first exercise tests students in their ability to develop a game in a topic related to cyber-attack simulation. The objective of this exercise is to allow students to develop skills in performing penetration testing focused on a particular threat or vulnerability and using a cyber range both as a learner and as a designer of games running in it. The second exercise requires students to develop a tutorial on how to secure particular network services. The results of the courses and exercises are later tested in in-class presentations and consultations and test runs. The approach designed by the authors has multiple benefits, such as motivating students to engage in practical cyber-security activities and allowing them to receive expert reviewing. The downside of this type of exercises is the limited amount of hands-on tests that can be conducted and developed by the students during the duration of the course. An approach that relied on laboratories exercises simulating common cyber-security scenarios would allow for more practical testing.

Assante and Tobey (2011) discusses the best approaches to make sure that a higher number of cyber-security experts, with the necessary skills and knowledge for their role is produced each year. This demand is due to the increase in positions that require cyber-security expertise. Skills in forensics, operational response, and risk management are defined as critical for the new workforce. Due to the dynamicity of the cyber-field, traditional backwards-facing protection methods should be substituted with new practices. Moreover, advanced collaboration skills and a more rigid definition of roles should be promoted as well. The author identifies three main components that define an individual's talent: knowledge, skill, and ability The use of new methods in cognitive science to assess and measure skill and to distinguish knowledge from skill better are also suggested. The author characterises skill as a rapid and consistent response, increased situational awareness, and resilience to uncertainty, distraction, and distress. When it comes to training and simulation, the author states that all the following guidelines should be respected:

- address the human factors;
- focus on all phases of the end-to-end workforce development cycle;
- develop ground truth expertise;
- define the ladder of expertise by distinguishing professionals at each stage of development and providing feedback at an individual level to aid in professional development;

Additionally, they cite the Ground Truth Expertise Development model proposed by researchers at the National Board of Information Security Examiners as a base roadmap to develop effective cyber-security workforce. The authors should conduct experimental research to support their study and validate their results.

Igor et al. (2018) conduct a survey to identify the cyber-security research centres in Europe. The survey contained 27 open-ended and close-ended questions and was composed of 5 sections:

1. general information;
2. cyber-security expertise;
3. sectors, applications and technologies;
4. international collaborations and joint programs;
5. confirmation and agreement with the privacy policy;

The survey was completed a total of 665 times, with results coming from 61 European centres. Of the domains identified in the survey, all of them were well covered by the results, with education and training, data security and privacy, network and distributed systems showing the greatest coverage. On the other end, trust management, assurance and accountability and theoretical foundations of security analysis and design showed the lowest coverage. The survey also presents findings regarding the number of publications published from each centre and the domains of the publications. These results show a strong correlation with the previous findings. Based on ulterior results from the survey, the author notes that although there is a stake coverage of domains all across the centres, the real coverage of sub-domains is jeopardised, with only a few of them being realistically covered. Interestingly, many of the sub-domains that show lower coverage pertain to trust and trust management.

Curtis and Mehravari (2015) describe the Cyber Security Capability Maturity Model (C2M2) and two tailored versions of the model for the energy sector and the oil and natural gas sector. The model includes ten domains, and for each domain, it contains a structured set of cyber-security practices. Some of the major domains included are risk management, identity and access management, situational awareness, information sharing, incident and event response, workforce management and cyber-security program management. The model defines four maturity indicator levels, MILO (equivalent to *not performed* status) through MIL3 (equivalent to a *managed* status). These indicators are used to evaluate and rate the organisation and institutional progress in each domain. The evaluation conducted through the model allows to identify gaps and institute and perform solution plans. The comprehensiveness and continuous evolution of the models have made them a proven tool of evaluation for cyber-security maturity. One development that should be explored further is the adaptation of the model to more sectors of critical infrastructure and industry.

Yoon et al. (2016) provide a framework for evaluating the readiness of cyber first responders responsible for critical infrastructure protection. The evaluation criteria are based on NFPA1410 standards. A scenario-based evaluation is used for specific objectives. A list of the proposed scenario is found below:

- gain remote access and exfiltrate data;
- system denial-of-service attack;
- system crash;
- repeated reboot attack;
- covert manipulation of control;

Time and completeness and successfulness of the team are used as the main factors of evaluation. The model has been demonstrated to be better suited at evaluating practical abilities and skills of cyber-security first responders than exam-based certifications. The author notes that further research should be conducted to create environments that are adequate for training evaluation. (Hoffman, Burley, and Toregas 2011) proposes a holistic approach to develop the cyber-security workforce that considers technical and non-technical disciplines needed to produce cyber-security professionals.

M. Evans et al. (2016) try to identify elements of cyber-security that may need further research. Additionally, they propose a framework for cyber-security assurance for human behaviour. During their literature research, the authors found that many individuals are willing to take risky actions and undertake in risky behaviour, mostly due to the low level of awareness or weight given to the vulnerabilities they may be exposed to. The fear appeal has been reported as one of the better countermeasures to this type of behaviour. The proposed framework is based upon defined and repeatable quantification. This quantification is related to the range of human aspect tasks that provide or are intended not to affect cyber-security posture negatively. The framework should build upon defined techniques such as HRA, SQC. To address human-related vulnerabilities, a scoring system is proposed, which is based upon the previous considerations on human-related risks. While this approach is innovative in its objectives and initial considerations, not complementing it with a complete and effective educational model on technical skills would still leave future cyber-security workforce with gaps in their fundamental knowledge.

U. P. D. Ani, H. M. He, and Tiwari (2016) present a Workforce Cyber Security Capability evaluation model used to ensure that human personnel is not suffering knowledge and skills deficiencies. The authors define cyber-security assurance as a combination of technology, processes and people. The interaction of the user with technology to manage system processes is highlighted as the risk factor that creates vulnerabilities in a system. A system to evaluate the awareness and knowledge of the workforce is argued to be a better tool

for cyber-security assurance. The evaluation model proposed by the authors categorises workers in three main groups: IT security experts, Engineers/Field Operators/Technicians, and Corporate Managers. For the purpose of the evaluation with the model, they define skill as *the ability to use accumulated knowledge either from experience or training to spot or detect cyber-attack attempts, patterns and techniques, and the degree, in which the user can respond timely with appropriate countermeasures*(U. P. D. Ani, H. M. He, and Tiwari 2016). Knowledge is instead defined as *the measure of information and theoretical understanding about recurrent cyber threats, vulnerabilities, attack patterns and impacts to the target system that a user, employee or operator is working with*(U. P. D. Ani, H. M. He, and Tiwari 2016). The evaluation, which can be conducted at both at an individual level or at an organisational level, consists of 5 different methods: Questionnaires, Interviews, Observations, Attack Simulations (Penetration Testing), and Gamification. The validation of the model developed by the authors is conducted only theoretically, with a randomly generated vector consisting of values of skill and knowledge assigned to the generated sample. Naturally, such type of validation does not take into account many of the nuances that come with a realistic evaluation of the workforce.

In a later work, U. D. Ani, H. He, and Tiwari (2019) design an approach to evaluate the skill and capacity of the cyber-security workforce in the industrial control system. Through the use of statistical data, the authors identify the most susceptible groups of personnel and the skill and knowledge required by them to prevent incidents. Cognitive capabilities, human error, proficiency in IDS and other tools usage are some of the main factors listed by the authors. The proposed model, which is an extension of their previous work(U. P. D. Ani, H. M. He, and Tiwari 2016), uses the same type of testing and parameters of the older version. The main shrewdness in the newer model is that individuals are not noted as a harmonised point of the whole workforce, but as single entry points characterised by a specific set of vulnerabilities. This correction makes the model more in line with the reality of the human workforce, which is also supported by the results of the test-based scenarios conducted by the authors.

Boyce et al. (2011) research and identify the main areas of cyber-security regarding human performance that are currently lacking in depth. One of the observations made by the authors concerns the usability of the software. In particular, they note that having different users, with different necessities, using a multitude of software increases user dissatisfaction and creates a less safe environment. Authentication, risk awareness and other skills are also listed as contributing factors to incident prevention. Overall, the findings of the authors are in line with previous work. Their surface-level research is rather shallow in details and would require further work to identify additional factors, the difference in requirements between roles and preventive measures.

Rowe and Lunt (2012) map current efforts in cyber-security research in various disciplines. Their two-factor mapping shows the relationship between a scale of theoretical development (theories, principles, innovation) to more applied development (application, deployment, configuration) and computing programs. In particular, the following programs are identified: organisational issues and information systems, application technologies, software methods and technologies, system infrastructure. Cyber-security is defined as an overlaying layer over the five pillars of IT (programming, networking, human-computer interactions, databases, web systems), which connects all their body of knowledge. When it comes to critical infrastructure, the authors list the following as the major challenges to overcome:

- Aging legacy infrastructure;
- Lack of standardisation;
- Internet connectivity;
- Real-time industrial processes;
- Lack of security awareness among ICS1 designers and operators
- Lack of ICS awareness among computing professionals;

Paulsen et al. (2012) give an overview of NICE, one of the major national initiatives for cyber-security education. The initiative has four components: awareness, formal education, training and professional development, and workforce structure. While the first three components target the general population, the last one is reserved for more specialised personnel. One of the major efforts made by the program is to develop a framework that divides cyber-security workers into 7 high-level categories and recognises 31 speciality areas.

Newhouse et al. (2017) provide more detail about the content and achievements of NICE. More detail is given about the target audience, which includes: employers, current and future cyber-security workers, educators and trainers and lastly technology providers. Knowledge, skills and abilities are defined for the 31 speciality areas. Additionally, tasks are identified. A combination of tasks goes into forming a piece of work associated with a specific speciality area. A detailed table is given listing all of the single tasks, the skills and knowledge required for completion, the role of the personnel in charge of completion and the area associated with the task. This level of detail allows for the formulation of targeted training frameworks.

Mishra et al. (2015) discuss a flexible training framework for cyber-security training for critical infrastructure protection. The approach incorporates both the NICE and NIST guidelines for the protection of critical infrastructure for managing risks relating to cyber-security. The proposed framework is built on self-contained instructional modules. These modules can be either standalone classes or incorporated to cyber-security training courses. The modules consist of both theoretical and practical training, followed by an evaluation.

Choi, Levy, and Hovav (2013) examined the effect of user computer self-efficacy, cyber-security countermeasures awareness and cyber-security skills on users' computer misuse intention a government agency. User's cyber-security awareness on topics such as ethical conduct, trust, risk, and privacy is identified as having a positive impact on computer misuse intention. Cyber-security computing skills are defined by the authors as *the knowledge, ability, and experience of an individual to use protective applications to protect computers, computer networks, and IS*. Cyber-security initiative skills are instead defined as *the knowledge, ability, and experience needed to seek out as well as take advantage of security software and best security practices*. Finally, Cyber-security action skill is defined as *the knowledge, ability, and experience an individual has to commit to objectives in order to meet security compliance* (Levy 2005). Based on the author's research about the relation between User Awareness of Computer Monitoring and cyber-security computing skills and computing skills, they note a negative correlation, which may support the idea that monitoring of employees should either not be conducted or not be made public to the employees, at least at the initial stage. Further research should be conducted on this correlation.

Oltramari et al. (2015) evaluate the use of trust as a human factor in holistic cyber-security risk assessment, in an effort to develop a holistic and predictive cyber-security risk assessment model. The proposed Cyber-security Risk Framework would consist of three main parts: system-level metrics (evaluated at the full system), policy-related metrics (evaluating the risks associated with the policies that govern the network and network assets), and asset-related metrics (evaluated at the asset level, such as metrics to assess risks associated with specific machines, a virtual network, or an operating system). When discussing an ontological way of weighting trust, the authors suggest using behavioural characteristics, knowledge and skill characteristics, situational characteristics, and traits that influence behaviour as measures. The authors' work highlights the very urgent necessity to offer a modern and accurate framework to evaluate human-related factors, which are often harder to translate in numerical values. Incorporating such a type of ontology to a more technical standard should provide a comprehensive set of guidelines for cyber-security assurance.

Henry (2017) discuss the gap between the current teachings in cybersecurity curricula and the requirements for CS workforce in the industry. To achieve this goal, the authors conduct a literature review in order to build a new multi-level matrix, Cyberspace Education Framework. The utility of the framework comes from allowing them to understand the purpose of each education program and whether this purpose is aligned with the industry's needs. Additionally, the authors investigate whether generalistic programs are more advantageous than focused courses and finally compare the outcome of current educational offerings to the knowledge, skills and abilities (KSA) set out in the U.S. Government's work standards document as a proxy for what would be required major cyber work roles in Australia.

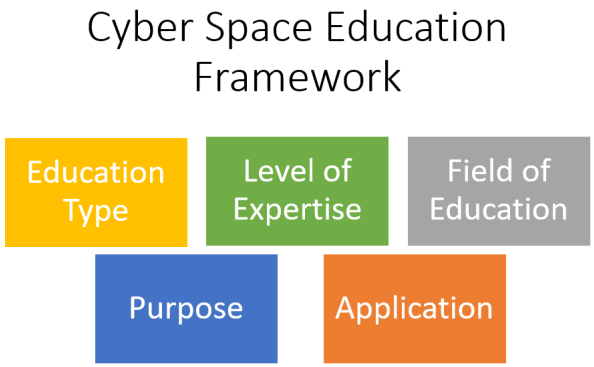


Fig. 1 Cyberspace education framework components, proposed by (Henry 2017)

Figure 1 shows the structure of the framework proposed by the authors to map different CS educational offerings. The authors note that in many cases, there is a significant gap in KSA required for positions in the industry and the final output of the current cyber-security educational programs. Additionally, these programs have been noted for offering little hands-on experience, which is a very crucial requirement for future CS experts preparedness (Henry 2017). The authors conclude by mapping possible skills and areas

to include in current offerings to make them more aligned with the industry's requirements and other areas that should be the focus of further research. While the framework proposed by the authors can be of use to evaluate an educational program's comprehensiveness, the authors do not delve in more depth regarding both knowledge and skills that should be integrated to current programs. A study on these two attributes would also allow for the extension of the proposed framework as a tool for improvement and optimization of current programs.

Potter and Vickers (2015) conduct a similar analysis as Henry (2017), by investigating industry requirements for cyber-security, by interviewing professionals and analysis current job listings. The authors noted that in most job listings, the skills that were required for the positions were often generic soft skills. Examples of the skills listed include the ability to work independently, process skills, leadership, presentation skills, time management, risk management, analysis, communication and problem-solving skills. Technical requirements were often summed up as the need for certifications and technical skills. The authors identified additional skills through a questionnaire that was sent to cyber-security experts. Some of the significant skills identified through the questionnaire include the ability to learn, leadership, management, problem-solving, communication, the ability to deal with people, analysis and motivation, experience and technical expertise. Moreover, job-specific skills were also identified. Many of these skills were shared between various positions, but a number of individual, job-specific skills were also found. The findings of the authors' research provide an interesting input in the discussion of skills and competencies' requirement for CS expertise. These results should be integrated with the current research or to future work on the technical requirements for cyber-security expertise in different fields and for different roles.

A more recent mapping of KSA for CS curriculum needed by students, based on data collected from interviews with CS professional was conducted by Jones, Namin, and Armstrong (2018). 44 cyber-security professionals were interviewed by the authors, with questions concerning demographic, 32 KSAs related to cyber-defence and other open-ended questions. Participants rated how important each KSA was to their job and indicated where they had learned that KSA.

Interestingly, for 31 of the 32 KSAs, participants indicated that they had learned the most about them directly from their job, indicating that very little practical skills or in-depth knowledge are acquired during their academic education. Participants were also asked what skills they had wished they had learnt during their academic formation. The most common answers included: recovery tasks, scanning skills, use of intrusion detection tools, network traffic analysis, packet-level analysis and penetration testing. Fifteen of the KSAs listed in the questionnaire were rated as being of significant importance, indicating a need for prioritization for that specific subset. Results from the tests and from the open-ended questions indicate that KSAs in the following areas are the most important for CS students after graduation: networks, vulnerabilities, programming, and communication. The results obtained by the authors provide a great indicator of which KSAs should be integrated and prioritized in current CS curricula. As the authors note, further research is required in understanding how to best integrate these KSAs to modern curricula, and also to verify the findings with some practical experimentation.

Carlton (2016) design, develop, and empirically test a set of hands-on tasks set to measure the cyber-security skills level of non-IT professionals. The list of skills used for the experimentation was extracted from previous work that defined an individual's technical knowledge, ability, and experience surrounding the hardware and software required to execute IS security to mitigate cyber-attacks as skills requirements(Axelrod 2006; Boyatzis and Kolb 1991; Choi, Levy, and Hovav 2013). Furthermore, the authors tried to determine whether there are any significant differences to cybersecurity skills levels based on gender, age, level of education, job function, primary online activity, hours accessing the Internet, and experience using technology. The results suggest that level of education and experience using technology may make a difference in the level of vulnerabilities and breaches caused by an employee. Whereas the type of work duties performed, the number of hours nor the activity completed online do not appear to make any difference on a non-IT professional's cybersecurity skills level.

6 Mapping of Results

In the following section, a mapping of the results of the literature review will be conducted to highlight common findings between the reviewed articles and establish prevalent attributes in terms of targets, areas and disciplines, and skills and competencies.

Table 1 shows a summary of the main target groups indicated in each research. Targets have been grouped into two major categories: the cyber workforce and students. The cyber workforce includes any individual that is in charge of tasks pertaining the use, protection and maintenance of cyberspace related functions. This includes both cyber-security personnel, but also individuals that cover different other roles. Additionally, the table provides information about the methods and solutions proposed by the authors to aid in

Work	Target	Suggested Method
K. Evans and Reeder (2010)	Cyber workforce & Students	Professional certification for cyber-security proficiency
Foo, Branagan, and Morris (2013)	Cyber workforce & Students	Local training program
Boyce et al. (2011)	Cyber Workforce & Students	X
Newhouse et al. (2017)	Cyber Workforce & Students	Framework for Improving Critical Infrastructure Cyber-security
Paulsen et al. (2012)	Cyber Workforce & Students	Program for cyber-security awareness, education, training
Choi, Levy, and Hovav (2013)	Cyber Workforce & Students	User computer self-efficacy
Jones, Namin, and Armstrong (2018)	Cyber Workforce & Students	X
Henry (2017)	Cyber Workforce & Students	Cyberspace Education Framework
Potter and Vickers (2015)	Cyber Workforce & Students	X
Turkanović, Welzer, and Hölbl (2019)	Cyber Workforce	Cyber-security education model
LeClair, Abraham, and Shih (2013)	Cyber Workforce	Inter disciplinary approach to cyber-security education
König and Wolf (2018)	Cyber Workforce	Competence Developing Game
Assante and Tobey (2011)	Cyber Workforce	X
Igor et al. (2018)	Cyber Workforce	X
Curtis and Mehravari (2015)	Cyber Workforce	Cyber Security Capability Maturity Model
Yoon et al. (2016)	Cyber Workforce	Cyber Training Exercise
Hoffman, Burley, and Toregas (2011)	Cyber Workforce	Holistic approach to developing the cyber-security workforce
M. Evans et al. (2016)	Cyber Workforce	Novel cyber-security framework
U. P. D. Ani, H. M. He, and Tiwari (2016)	Cyber Workforce	WCSC capability evaluation model
U. D. Ani, H. He, and Tiwari (2019)	Cyber Workforce	Scenario-based testing
Rowe and Lunt (2012)	Cyber Workforce	X
Mishra et al. (2015)	Cyber Workforce	Flexible, modular training framework
Dawson and Thomson (2018)	Cyber Workforce	Cybersecurity development plan
Oltramari et al. (2015)	Cyber Workforce	Holistic Cyber-security Risk Framework Human factor Ontology
Carlton (2016)	Cyber Workforce	Cybersecurity Skills Index
Luallen and Labruyere (2013)	Students	Cyber-security course curriculum
Mao, Chua, and Liang (2017)	Students	Scenario-Based Experiments
Svabensky et al. (2018)	Students	Two-course models
Sobiesk et al. (2015)	Students	Multi-level, multi-discipline approach to cyber education

Table 1: Targets and methods proposed for skill and competencies acquisition, identified from the articles analysed in the literature review.

achieving the skills and competencies that are reported in their research.

The table shows that 16 of the papers discuss skills and competencies for the cyber workforce, 4 for students and 9 for both cyber workforce and students. It is important to note that while a majority of papers indicates their targets to be the broader range of cyber personnel, several articles indicate specialised roles. For example, Curtis and Mehravari (2015) focus on research operators and owners of electrical and oil and gas CI. Newhouse et al. (2017) indicates that programs should be developed separately to train and develop educators, trainers and security providers. Hurst, Merabti, and Fergus (2014) states that managers and key executives should also have a background in cyber-security and focuses their research in the study of skills that need to be acquired by individuals in this role. A few considerations can be made on the of papers based on the target of their analysis:

– **Cyber Workforce & Students as targets:** This sub-set of papers can be further distinguished in papers that discuss skills and competencies for both targets in general terms and papers that utilize data collected on skills for cyber workforce to discuss the landscape of current CS curricula available for students. This latter case is more interesting as it often produced more significant results, providing more detail on skills developed or required for both targets. It is also a more demanding work, as it requires focused study on both domains. Potter and Vickers (2015), Henry (2017), and Jones, Namin, and Armstrong (2018) all discuss ways to improve current cyber-security curricula based on data collected through studies, questionnaires and interviews with CS experts. A shared conclusion raised by the authors is that many modern curricula do not focus enough on acquiring skills and knowledge through practical experience, which was supported to be the most effective way for training(McCrohan, Engel, and Harvey 2010). Additionally, it was also noted that many of the curricula offer more generalistic knowledge and skills, although in the industry there is a stronger need of focused technical and practical skills(Jones, Namin, and Armstrong 2018; Henry 2017). Developing effective ways to integrate the

missing skills and competencies in current CS curricula should be the next step in the research direction, as it would allow for the effective development and training of future CS personnel.

- **Cyber Workforce as targets:** papers that only have cyber workforce as target discuss either current needs for CS personnel in terms of knowledge, skills and abilities (KSA) or possible solutions to develop KSAs that are lacking or limited in development. When it comes to solutions offered for skill acquisition or development, many different proposals have been found in the literature, including: educational and training frameworks and programs, serious games, self-assessment modules, maturity models, scenario-based tests and exercises, and other interactive training solutions. Studies focused on understanding the effectiveness of certain CS awareness and training solutions(Tioh, Mina, and Jacobson 2017) and also works comparing the efficacy of different strategies(Luiijf et al. 2011) have been conducted over the years. Nonetheless, due to the novelty of the approaches proposed by some of the works in this literature review and also the implementation of skills and knowledge not present in previous training programs, research should be conducted to investigate on the comparative effectiveness of these solutions in instilling future CS workforce with new skills and knowledge.
- **Students as targets:** a relatively low number of papers has been found discussing students as the only target. All of these papers discuss and propose skill acquisition methods either as a stand-alone or to be integrated with current CS curricula. These approaches include fully-developed curricula, multi-discipline approaches, courses, modules and exercises. A limitation of these papers, which the first sub-set of papers discussing both cyber-workforce and students as targets overcame, is that they do not compare or analyse in depth the requirements with current industry needs for CS workforce to the material presented in their solutions. Integrating this type of comparison would allow both to validate their results in terms of future requirements and make their solutions more attractive to institutions.

7 Skills and Competencies for CI Cyber-security

As evidenced by the literature review in 5, there is not a universally agreed selection of skills and competencies needed for critical infrastructure cyber-security or cyber-security assurance. Nonetheless, general trends and commonalities can be seen between the different proposals made over the years. Cyber-security skills and competencies can be grouped in the following categories:

- **Technical Skills**: Technical skills include a vast array of competencies and knowledge that may be needed for cyber-security assurance. Specific skills often depend on the role of an individual inside a firm. Technical skills may relate to: architecture, administration, and management of operating systems, networking, virtualization software and other fields. Additionally, to combat specific threats, personnel may need knowledge relating and exclusive to the single threat. This means that with new threats being continually developed, there is a constant need for an update in the type of knowledge and technical skills required to defend against attacks;
- **Soft Skills**: soft skills include a large number of skills and dispositions. Communication skills, both as a listener and as a speaker, trustworthiness, work habits are some of the skills that can influence an individual's ability to perform in cyber-security tasks. While in the past, less focus was put in understanding the relationship between soft skills and cyber-security assurance, recent research(U. Ani, H. He, and Tiwari 2018) has shown a very strong correlation between the two. This motivated the inclusion of training modules for soft skills in many recent proposals for CI cyber-security education and training programs;
- **Implementation Skills**: implementation skills are what often distinguish junior cyber-security experts to seniors. This set of skills allows studying the architecture of systems and networks, then use that information to identify the security controls in place and how they are used. Same with weaknesses in databases and app deployment.:
- **Management Skills**: management skills are usually required by chief personnel in charge of organizing and coordinating technical vulnerability assessments (systems and network vulnerability assessments and other types of vulnerability assessment), penetration testing, web-application assessments, social engineering assessments, physical security assessments, wireless security assessments and implementing secure infrastructure solutions.

The skills and competencies that have been found in the literature review have been summarized and mapped in table 2. The mapping consisted in grouping each skill in one of the four categories identified previously: technical skills, soft skills implementation skills and management skills.

A few observations can be made from the mapping of the skills in table 2. Firstly, it can be noticed from the table that the majority of skills and competencies reported could be defined as *general skills*(Potter and Vickers 2015). In this work, this definition is interpreted as "skills that combine either interdisciplinary or area-specific knowledge, to perform a learned psychomotor act or an observable behavior(Newhouse et al.

Skills Mapping Table			
Technical Skills	**Soft Skills**	**Implementation Skills**	**Management Skills**
1. Understanding of digital security concepts; 2. Understanding of evolving threats; 3. Understanding of attack intelligence; 4. Penetration testing skills; 5. Cryptology knowledge; 6. SW & HW security skills; 7. Network security skills; 8. Computer forensics skills; 9. Programming skills; 10. Data analytics skills; 11. Information security skills; 12. Wireless security skills; 13. Ability in using IDS tools;	1. Information sharing and communications; 2. Public speaking and presentation skills; 3. Situational Awareness; 4. Cognitive and behaviour analysis; 5. Ability to work independently; 6. Trust management; 7. Teamwork; 8. Motivation; 9. Time management; 10. Networking; 11. Confidence; 12. Work habits;	1. Threat and vulnerability assessment & management; 2. Event and Incident Response; 3. Continuity of Operations;	1. Risk management; 2. Identity and access management; 3. Asset, change and configuration management; 4. System administration; 5. Workforce management; 6. Cyber-security program management; 7. Supply chain and external dependencies management; 8. Evaluation of policies effectiveness; 9. Project planning;

Table 2 Mapping of skills and competencies for Critical Infrastructure Protection (CIP) found in the literature review

2017) required for multiple, if not the majority of roles in CS". To determine which of the skills that are defined in the literature are general, the findings of the literature review were used either directly or in the form of quantitative data, together with the documentation for the NICE framework(Newhouse et al. 2017) and later frameworks based on NICE. This information was used to establish which skills were considered critical for CS expertise, as well as skills that encompassed a broad range of knowledge or combined other individual skills. In the NICE framework, a significantly higher number of skills and abilities is listed, many of which could be defined as *specialized skills*. Specialized skills are differentiated from general skills due to being required for specific roles or missions in CS. In the framework, specialized skills are associated with speciality areas and tasks that have been identified as being part of a cybersecurity work role. The NICE framework identifies a total of 630 knowledge areas, 374 skills and 176 abilities that cyber-security workers should possess depending on their roles. This Knowledge, skills and abilities (KSAs) are later mapped in the same documentation to 51 individual roles in CS-related fields. While this mapping is undoubtedly comprehensive, this high level of granularity is not always advantageous, as it can become detrimental in many cases, some of which are discussed in detail below.

Research has shown that for the education and training of students for specific CS roles, generalist programs are less effective than mission-specific programs(Henry 2017). For example, Henry (2017) has shown how a master course in forensic computing and cyber-crime investigation from the University College Dublin covered almost all KSAs reported by CS experts in this role, while equivalent generic programs offered a significantly lower level of coverage. The master course offered at the University College Dublin offered more specialized units of studies, such as mobile devices investigation, Linux for investigators, live data forensics, data and database forensics, online fraud investigations, legislation and financial fraud investigation, along with other units. The units in the generalistic programs instead covered broader topics such as information security, programming, project management, wireless security and data analytics. The specialization of the former units is what rendered the first program more effective for the roles in computer forensic and cyber-crime investigation.

On the other side, generalization and highlighting of KSAs that are valued more for CS purposes are essential for the development of introductory courses to CS, but also to develop multi-role/mission courses. Such courses would allow students to develop interdisciplinary skills needed for multiple positions in the CS work sphere.

In (Potter and Vickers 2015), through the analysis of multiple job advertisement in different CS-related positions, the authors found that a number of skills were highly sought after for multiple different roles.

In particular, soft skills such as teamwork and communication skills were shared as requirements for most positions.

Jones, Namin, and Armstrong (2018) has also shown that certain KSAs should be prioritized over other, more specialized KSAs. After asking 44 participants to rate from 1 to 6 the importance of given KSAs, 3 received a mean rating over 5, another 11 received a rating between 5 and 4.5, while all the other received a lower rating. The 14 KSAs that received the highest scores are reported in the table 3. This shows a general consensus from CS experts when it comes to defining KSAs that should be prioritized during training.

Most valuable Knowledge, Skills and Abilities (KSAs) table	
$m > 5$	$4.5 < m < 5$
How traffic flows across the network; Network protocols; System and application security threats and vulnerabilities;	Basic system administration, network, and operating system hardening techniques; Network security architecture concepts; General attack stages; Different classes of attacks and recovery concepts and tools; Recognizing and categorizing types of vulnerabilities and associated attacks; Conducting vulnerability scans and recognizing vulnerabilities in security systems; Computer network defence policies, procedures, and regulations; Securing network communications; Programming language structures and logic; Information assurance principles and organizational requirements; What constitutes a network attack and the relationship to both threats and vulnerabilities;

Table 3 KSAs with mean score m higher than 5 on the left and with a score between 4.5 and 5 on the right, as reported by (Jones, Namin, and Armstrong 2018)

One other criticism for the mapping utilized in the NICE framework is detailed in the work of Jacob et al. (2018). As previously stated in section 2, the authors argue that for less technological-related roles in cyber-security, the framework provide poor job descriptions for specific work roles, inadequate competencies and training and career guidance, no predictable outcomes or metrics to determine effectiveness, etc. Providing a general mapping of skills and competencies for CS workforce has the advantage of facilitating the development of introductory, or general courses and programs, for the development and training of future CS experts. Moreover, the higher focus given in mapping key soft skills also provides a beneficial input from this work, compared to the data contained in the NICE documentation.

As anticipated, many of the soft skills identified in the literature are usually general skills needed by most CS workers. In particular, developing good communication and teamwork skills is fundamental to increase the effectiveness and efficiency of incident prediction and prevention actions(Svabensky et al. 2018; Mishra et al. 2015). Simulation exercises and interactive, team-based solutions are often suggested as possible methods for building better team-working and communication abilities(Svabensky et al. 2018). Other soft skills, such as trust management, can pose more of a challenge, both in terms of definition and development.

Oltramari et al. (2015) aggregates multiple concepts such as competence, benevolence, integrity, predictability, attitude, intention, behaviour, reliability, dependability, and faith as defining characteristics to building trust. While some of these characteristics can be developed through experience and knowledge acquisition, others are dependent on individuals' behavioural characteristics(Oltramari et al. 2015). This adds a human-dependent factor to CS assurance, which is often exploited during cyber-attacks, as it represents one of the weakest points of CIP(U. Ani, H. He, and Tiwari 2018). In fact, a significant number of successful attacks against CI involve the use of social engineering techniques(Conteh and Schmick 2016). While in most cases, non-security experts or staff not involved in cyber-security or other technical positions that require digital expertise are the most susceptible to this attacks, it is not uncommon for CS personnel to be also exploited(Conteh and Schmick 2016). Development of future training frameworks and programs for CIP should thus consider including modules finalized in educating staff to detect and prevent such attacks.

As mentioned in their definition, both implementation and management skills are often required by senior CS experts or by individuals covering specific roles, including leadership positions, but are often not required by many other roles in CS. This caused the development of only a selected number of curricula

and training frameworks for the advancement of these competencies(Curtis and Mehravari 2015; Boyce et al. 2011; Knowles et al. 2015). These programs usually can only be completed if a lengthy number of technical pre-requisites have already been acquired by the individuals, or are taught during long-lasting teachings and courses preceding the ones for management or implementation skills development. Although there is less concentration of studies and methods for the development of these skills, having qualified key figures in managerial positions and CS experts lead large-scale implementation projects is crucial for the longevity of any critical infrastructure architecture. Additionally, many of the managerial and implementation competencies required by CS professionals can only be acquired if a solid technical background is already present. Threat and vulnerability management, for example, requires not only implementations of plans and procedures to detect and counter threats, but also the installation and use of technologies and software to identify, analyze, manage, and respond to cyber-security threats(Curtis and Mehravari 2015). Similarly, asset, change and configuration management requires hardware and software knowledge to manage the organization's information technology and operations assets(Curtis and Mehravari 2015). Many of these skills require advanced technical knowledge, in addition to experience in the position. Lastly, it must be noted that with the exception of most soft skills, other skills require continuous updating in the content and amount of knowledge required to achieve them. This is mainly caused by the fast pace of innovation of technologies and landscape of new attack vectors. For this reason, detailed mappings of skills and competencies to their respective body of required knowledge should be mostly evaluated based on their publication period and not used as definitive standards.

8 Conclusions & Future Work

The level of knowledge and skills necessary from current cyber-security workers involved in critical infrastructure protection has significantly increased in recent years. Some of the identified causes that induced this increase include: continuous innovation in the digital technology sector and CI sectors(Ye Yan et al. 2012; Hsu and Marinucci 2013), development of new attacks vectors and discovery of new cyber-security threats(Jang-Jaccard and Nepal 2014), increase in attacks targeting humans as the vulnerable factor(Conteh and Schmick 2016; Abraham and Chengalur-Smith 2010) and results from multiple studies showing a strong correlation between cyber-security assurance and human-related attributes, such as behavioural and cognitive abilities(U. Ani, H. He, and Tiwari 2018; Assante and Tobey 2011; M. Evans et al. 2016; U. D. Ani, H. He, and Tiwari 2019) among others. Due to this continuous need for updates and additions to CS curricula, mapping skills, competencies, and other requirements for CI cyber security is a challenging task. Nonetheless, having a current mapping of the most crucial skills is advantageous, as it allows for the development of comprehensive training programs and frameworks for CI cyber-security.

In this work, we conducted a systematic literature review to identify scientific papers discussing and evaluating competencies, skills and essential attributes needed by CI staff for cyber-security assurance. The identified skills have been mapped to establish categories of belonging and to highlight shared attributes. Results from the review show that a wide array of skills are needed for CS CIP. While some of the findings included skills in narrow fields, discussed by only seldom articles, many of the skills identified where commonly agreed as fundamental by multiple authors. Nonetheless, the relevance of the former skills should not be dismissed, as they can be critical for correct and comprehensive CS assurance.

It has been noticed that there is often a lack of conciliation between the skills and competencies taught in academia and the one required for the jobs available in the current market. Current educational curricula should be re-adapted, when necessary, to reflect to current needs in CS roles.

During this review, it was found that in recent years more effort has been taken to include the training of soft skills for CS preparedness. Nonetheless, further research is still required to understand how each of these skills affect various aspects of CS assurance. One area where research is still somewhat lacking is the relation between behavioural and cognitive abilities and CS efficacy. Although a number of studies had shown how certain behavioural predispositions could influence an individual's ability in CS assurance, more research is needed to clarify this link further and to understand how future solutions should address the issue.

During the comparative analysis of the articles, it was noted that many different solutions for CS awareness and training have been developed over the years. Nonetheless, there is still no agreement on what are the best procedures to integrate the training of these skills to existing offerings or how to develop effective new solutions. Further work will be conducted to evaluate current solutions for CS training and establish the most effective ways to provide comprehensive and effective methods for CS training of the skills collected and described in this work.

9 Compliance with Ethical Standards

9.1 Funding

Funding: this study was funded by the Norwegian University of Science and Technology (NTNU), as part of research for the CybWin project.

9.2 Ethical approval

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors

References

Abraham, Sherly and InduShobha Chengalur-Smith (2010). "An overview of social engineering malware: Trends, tactics, and implications". In: *Technology in Society* 32.3, pp. 183–196.

Ani, Uchenna Daniel, Hongmei He, and Ashutosh Tiwari (2019). "Human factor security: evaluating the cybersecurity capacity of the industrial workforce". In: *Journal of Systems and Information Technology*.

Ani, Uchenna P Daniel, Hongmei Mary He, and Ashutosh Tiwari (2016). "Human capability evaluation approach for cyber security in critical industrial infrastructure". In: *Advances in Human Factors in Cybersecurity*. Springer, pp. 169–182.

Ani, Uchenna, Hongmei He, and Ashutosh Tiwari (Nov. 2018). "Human factor security: evaluating the cybersecurity capacity of the industrial workforce". In: *Journal of Systems and Information Technology* 21. DOI: 10.1108/JSIT-02-2018-0028.

Assante, Michael J and David H Tobey (2011). "Enhancing the cybersecurity workforce". In: *IT professional* 13.1, pp. 12–15.

Axelrod, C Warren (2006). "Cybersecurity and the critical infrastructure: Looking beyond the perimeter". In: *Information Systems Control Journal* 3, p. 24.

Boyatzis, Richard E and David A Kolb (1991). "Assessing individuality in learning: The learning skills profile". In: *Educational Psychology* 11.3-4, pp. 279–295.

Boyce, Michael W et al. (2011). "Human performance in cybersecurity: A research agenda". In: *Proceedings of the Human Factors and Ergonomics Society annual meeting*. Vol. 55. 1. SAGE Publications Sage CA: Los Angeles, CA, pp. 1115–1119.

Carlton, Melissa (2016). "Development of a cybersecurity skills index: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills". In:

Choi, MinSuk, Yair Levy, and Anat Hovav (2013). "The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse". In: *Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC–Workshop on Information Security and Privacy (WISP)*.

Chris, Debo (Feb. 2015). "Preventing Cyberattacks and Data Breaches via Employee Awareness Training and Phishing Simulations". In: *schneiderdowns*. URL: https://www.schneiderdowns.com/our-thoughts-on/.

Conteh, Nabie Y and Paul J Schmick (2016). "Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks". In: *International Journal of Advanced Computer Research* 6.23, p. 31.

Curtis, Pamela D and Nader Mehravari (2015). "Evaluating and improving cybersecurity capabilities of the energy critical infrastructure". In: *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*. IEEE, pp. 1–6.

Davis, Jessica (Jan. 2020). *Ransomware, Phishing Attacks Compromised Half US Orgs in 2019*. Ed. by Healthysecurity.com. [Online; posted 28-January-2020]. URL: https://healthitsecurity.com/news/ransomware-phishing-attacks-compromised-half-us-orgs-in-2019.

Dawson, Jessica and Robert Thomson (June 2018). "The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance". In: *Frontiers in Psychology* 9, p. 744. DOI: 10.3389/fpsyg.2018.00744.

Evans, Karen and Franklin Reeder (2010). *A human capital crisis in cybersecurity: Technical proficiency matters*. CSIS.

Evans, Mark et al. (2016). "Human behaviour as an aspect of cybersecurity assurance". In: *Security and Communication Networks* 9.17, pp. 4667–4679.

Foo, Ernest, Mark Branagan, and Thomas Morris (2013). "A proposed australian industrial control system security curriculum". In: *2013 46th Hawaii International Conference on System Sciences*. IEEE, pp. 1754–1762.

Ghafir, I. et al. (Aug. 2016). "A Survey on Network Security Monitoring Systems". In: *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pp. 77–82. DOI: 10.1109/W-FiCloud.2016.30.

Ghafir, Ibrahim, Martin Husák, and Vaclav Prenosil (Aug. 2014). "A Survey on Intrusion Detection and Prevention Systems". In:

Gratian, Margaret et al. (2018). "Correlating human traits and cyber security behavior intentions". In: *computers & security* 73, pp. 345–358.

Hashim, Mohd Shamir (2011). "Malaysia's national cyber security policy: The country's cyber defense initiatives". In: *Proceedings of the Second Worldwide Cybersecurity Summit*. URL: https://www.cybersecurity.my/.

Henry, A (2017). "Mastering the cyber security skills crisis: realigning educational outcomes to industry requirements". In: *ACCS discussion paper* 4.

Hoffman, Lance, Diana Burley, and Costis Toregas (2011). "Holistically building the cybersecurity workforce". In: *IEEE Security & Privacy* 10.2, pp. 33–39.

Hsu, D Frank and Dorothy Marinucci (2013). *Advances in cyber security: Technology, operation, and experiences*. Fordham Univ Press.

Hurst, William, Madjid Merabti, and Paul Fergus (2014). "A Survey of Critical Infrastructure Security". In: *Critical Infrastructure Protection VIII*. Ed. by Jonathan Butts and Sujeet Shenoi. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 127–138. ISBN: 978-3-662-45355-1.

Igor, Nai Fovino et al. (2018). *Cybersecurity Competence Survey*. DOI: https://doi.org/10.2760/42369. URL: https://ec.europa.eu/jrc/en/publication/european-cybersecurity-centre-expertise-cybersecurity-competence-survey.

IRM (2015). "Amateyrs attack technology. Professional hackers target people". In: *www.irmplc.com*. URL: www.irmplc.com/issues/human-behaviour.

Jacob, Johanna et al. (2018). "Is The NICE Cybersecurity Workforce Framework (NCWF) Effective For A Workforce Comprised Of Interdisciplinary Majors?" In: *Proceedings of the International Conference on Scientific Computing (CSC)*. The Steering Committee of The World Congress in Computer Science, Computer ..., pp. 124–130.

Jang-Jaccard, Julian and Surya Nepal (2014). "A survey of emerging threats in cybersecurity". In: *Journal of Computer and System Sciences* 80.5, pp. 973–993.

Jones, Keith S, Akbar Siami Namin, and Miriam E Armstrong (2018). "The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals". In: *ACM Transactions on Computing Education (TOCE)* 18.3, pp. 1–12.

Knowles, William et al. (2015). "A survey of cyber security management in industrial control systems". In: *International Journal of Critical Infrastructure Protection* 9, pp. 52–80. ISSN: 1874-5482. DOI: https://doi.org/10.1016/j.ijcip.2015.02.002. URL: http://www.sciencedirect.com/.

König, Johannes A and Martin R Wolf (2018). *Cybersecurity Awareness Training provided by the Competence Developing Game GHOST*.

Lebek, Benedikt et al. (2014). "Information security awareness and behavior: a theory-based literature review". In: *Management Research Review*.

LeClair, Jane, Sherly Abraham, and Lifang Shih (2013). "An interdisciplinary approach to educating an effective cyber security workforce". In: *Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference*, pp. 71–78.

Leszczyna, Rafał (2018). "A review of standards with cybersecurity requirements for smart grid". In: *Computers and Security* 77, pp. 262–276. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2018.03.011. URL: http://www.sciencedirect.com/.

Levy, Yair (2005). "A case study of management skills comparison in online and on-campus MBA programs". In: *International Journal of Information and Communication Technology Education (IJICTE)* 1.3, pp. 1–20.

Luallen, Matthew E and Jean-Philippe Labruyere (2013). "Developing a critical infrastructure and control systems cybersecurity curriculum". In: *2013 46th Hawaii International Conference on System Sciences*. IEEE, pp. 1782–1791.

Luiijf, HAM et al. (2011). "Ten national cyber security strategies: A comparison". In: *International Workshop on Critical Information Infrastructures Security*. Springer, pp. 1–17.

Mao, Jian, Zheng Leong Chua, and Zhenkai Liang (2017). "Enabling practical experimentation in cybersecurity training". In: *2017 IEEE Conference on Dependable and Secure Computing*. IEEE, pp. 516–517.

McCrohan, Kevin F, Kathryn Engel, and James W Harvey (2010). "Influence of awareness and training on cyber security". In: *Journal of internet Commerce* 9.1, pp. 23–41.

Mishra, Sumita et al. (2015). "On building cybersecurity expertise in critical infrastructure protection". In: *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*. IEEE, pp. 1–6.

Newhouse, W et al. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, Special Publication 800-181*.

NISTIR (2014). "NISTI7628 7628 Rev. 1 Guidelines for Smart Grid Cybersecurity". In: *National Institute of Standards and Technology*. URL: https://csrc.nist.gov/publications/detail/nistir.

Öğütçü, Gizem, Özlem Müge Testik, and Oumout Chouseinoglou (2016). "Analysis of personal information security behavior and awareness". In: *Computers & Security* 56, pp. 83–93.

Okoli, Chitu and Kira Schabram (May 2010). "A Guide to Conducting a Systematic Literature Review of Information Systems Research". In: *SSRN Electronic Journal* 10. DOI: 10.2139/ssrn.1954824.

Oltramari, Alessandro et al. (2015). "Towards a Human Factors Ontology for Cyber Security." In: *STIDS*, pp. 26–33.

Padayachee, Keshnee (2012). "Taxonomy of compliant information security behavior". In: *Computers & Security* 31.5, pp. 673–680.

Paulsen, Celia et al. (2012). "NICE: Creating a cybersecurity workforce and aware public". In: *IEEE Security & Privacy* 10.3, pp. 76–79.

Potter, Leigh Ellen and Gregory Vickers (2015). "What skills do you need to work in cyber security? A look at the Australian market". In: *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, pp. 67–72.

Rahim, Noor et al. (May 2015). "A systematic review of approaches to assessing cybersecurity awareness". In: *Kybernetes*. DOI: 10.1108/K-12-2014-0283.

Rowe, Dale C and Barry Lunt (2012). "Mapping the cyber security terrain in a research context". In: *Proceedings of the 1st annual conference on Research in Information Technology*, pp. 7–12.

Shropshire, Jordan, Merrill Warkentin, and Shwadhin Sharma (2015). "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior". In: *Computers & Security* 49, pp. 177–191.

Sklyar, Vladimir (Jan. 2012). "Cyber Security of Safety-Critical Infrastructures: A Case Study for Nuclear Facilities". In: *Information and Security: An International Journal* 28, pp. 98–107. DOI: 10.11610/isij.2808.

Sobiesk, Edward et al. (2015). "Cyber education: a multi-level, multi-discipline approach". In: *Proceedings of the 16th Annual Conference on Information Technology Education*, pp. 43–47.

Svabensky, Valdemar et al. (2018). "Enhancing cybersecurity skills by creating serious games". In: *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, pp. 194–199.

Tioh, Jin-Ning, Mani Mina, and Douglas W Jacobson (2017). "Cyber security training a survey of serious games in cyber security". In: *2017 IEEE Frontiers in Education Conference (FIE)*. IEEE, pp. 1–5.

Turkanović, M., T. Welzer, and M. Hölbl (2019). "An Example of a Cybersecurity Education Model". In: *2019 29th Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEEIE)*, pp. 1–4.

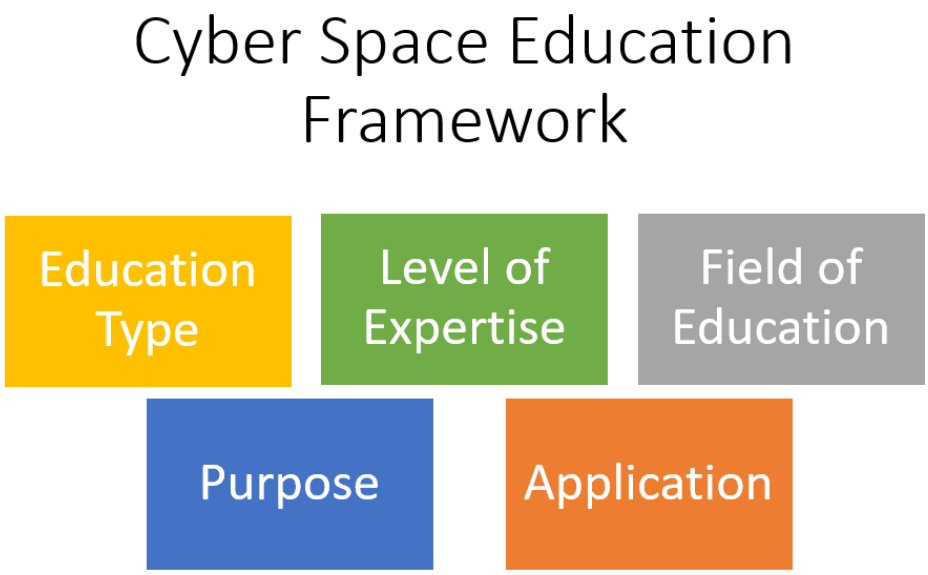
Webster, Jane and Richard T Watson (2002). "Analyzing the past to prepare for the future: Writing a literature review". In: *MIS quarterly*, pp. xiii–xxiii.

Yamin, Muhammad Mudassar, Basel Katt, and Vasileios Gkioulos (2020). "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture". In: *Computers and Security* 88, p. 101636. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2019.101636. URL: http://www.sciencedirect.com/.

Yan, Y. et al. (Apr. 2012). "A Survey on Cyber Security for Smart Grid Communications". In: *IEEE Communications Surveys Tutorials* 14.4, pp. 998–1010. ISSN: 2373-745X. DOI: 10.1109/SURV.2012.010912.00035.

Yan, Ye et al. (2012). "A survey on cyber security for smart grid communications". In: *IEEE Communications Surveys & Tutorials* 14.4, pp. 998–1010.

Yoon, Jungsang et al. (2016). "Evaluating the readiness of cyber first responders responsible for critical infrastructure protection". In: *International Journal of Critical Infrastructure Protection* 13, pp. 19–27.



Cyberspace education framework components