DOI: 10.53477/1842-9904-24-13

VALIDATION AND PRIORITIZATION OF KNOWLEDGE, SKILLS AND ABILITIES FOR CYBERINTELLIGENCE ANALYSIS IN INTELLIGENCE AND NATIONAL SECURITY

Cristian CONDRUȚ*

Cybersecurity educational endeavours are nowadays of interest to public and private institutions as proven by the fact that multiple academic and training formats are available in academia and professional organizations. Given that cyberintelligence developed as a subfield of both intelligence and national security and cybersecurity, education and training are needed to form intelligence analysts that deal with cybersecurity threats in intelligence and national security organizations. Our main objective is to validate and prioritize a set of cybersecurity and intelligence competences that can be used in education and training endeavours for the cyberintelligence analysts in intelligence and national security organizations. Our results show that the high-priority competences for this type of professionals are a mix between intelligence and cybersecurity competences, most prevalent being the analytical and contextual dependent ones. In our article, we also elaborate on examples of educational practices that can be applied to high priority competences.

Keywords: *cyberintelligence analysis; intelligence analysis; national security; competences; knowledge; skills; abilities; education.*

***** Cristian CONDRUȚ is a PhD Candidate at the Doctoral School of Intelligence and Security within “Mihai Viteazul” National Intelligence Academy, Romania. He holds a MSc in Theory of Information Encoding and Storage at Politehnica Bucharest University, Bucharest. E-mail: condrut.cristian@animv.eu***

Introduction

Nowadays, most formal and informal educational endeavours begin with a proper process of identification and development of competences. One of the principles that underpins the definition of competence is that it involves applying contextually-appropriate knowledge and skills (Vitello, Greatorex and Shaw 2021, pp. 15 - 16). Thus, given that cyberintelligence analysis is still a novel field in cybersecurity and in intelligence and national security, in which the diversity and complexity of cyber threat actors are quite high, it is really important to train future professionals by using educational programs that are well-calibrated and adjusted to their purposes.

In our particular research context, which is cyberintelligence analysis in intelligence and national security, it is important to capitalize on previous cybersecurity and intelligence and national security expertise. Borum and Sanders in *Preparing America's Cyber Intelligence Workforce* presented 5 types of competences needed by the cyberintelligence analyst: technical, knowledge management, analytical, contextual, and communicational and organizational (Borum and Sanders 2020, 67-73). In our previous researches, we clustered knowledge, skills and abilities retrieved from the Workforce Framework for Cybersecurity (NICE framework), which was elaborated by the US National Institute of Standards and Technology (NIST), into the aforementioned types of cyberintelligence competences developed by Borum and Sanders (Condruț 2023). Thus, we identified 51 knowledge units, 28 skills and eight abilities necessary for the cyberintelligence analyst in intelligence and national security (Condruț 2023, 4205 - 4206). Given that our previous researches is based only on secondary data (i.e., employing a content analysis methodology on analytical cybersecurity reports), the following research question will guide our endeavour towards a more empirical approach that will involve the employment of research methods needed for the collection of primary data: *How can we validate and prioritize knowledge, skills and abilities needed by the cyberintelligence analyst in intelligence and national security?*

Thus, our research objective is to validate and prioritize the set of competencies retrieved in our previous researches by applying a survey with the participation of cybersecurity, cyberintelligence and intelligence and national security experts. We consider that validation of our previously discovered set could be satisfactory for research purposes, but the prioritization of these competences is necessary for research and educational purposes, given the limited human, financial and logistical resources that could be employed in an educational setting.

In order to test de validity of a more comprehensive set of competencies, we proposed to add eight more knowledge units presented by Alsmadi in *The NICE Cyber Security Framework. Cyber Security Intelligence and Analytics Second Edition*

(Alsmadi 2023) that refer to intelligence analysis and dissemination processes and emergent technology knowledge, thus capitalizing not only on cybersecurity, but also on intelligence analysis. We will present the complete set of competences in the *Methodology* section.

1. Methodology

As stated in the introduction, we applied the survey research method. Thus, our research includes a data collection stage and a data processing stage. In the collection stage we applied a mixed questionnaire (i.e., both with closed and open questions) to cybersecurity, cyberintelligence and intelligence and national security experts from organizations that deal directly with cyberintelligence or that are at the nexus of the tree aforementioned professional domains.

We chose to sample the organization from whom we aim to retrieve answers by using the judgmental sampling procedure (Sharma 2017, 751 - 752), given the fact that we aimed at collecting opinions from intelligence and national security professionals that work in organizations which do not disclose their number of employees in public sources. We selected public and private organizations that have legal responsibilities, commercial, educational or research interests in cyberintelligence, cybersecurity or in intelligence and national security. Thus, we distributed the questionnaire to experts associated with Intelligence College in Europe, International Association for Intelligence Education, NATO Cooperative Cyber Defence Centre of Excellence, European Union Agency for Cybersecurity, Romanian National Cyber Security Directorate, National Institute for Research & Development in Informatics - ICI Bucharest, Romanian Association for Information Security Assurance, Rey Juan Carlos University from Madrid, National University for Science and Technology Politehnica București and Recorded Future.

The questionnaire used included a total of 95 knowledge units (i.e. 59), skills (i.e. 28) and abilities (i.e. 8) [1], each of them being a separate variable and is organized into four sections that contains both closed and open questions: 1) knowledge units; 2) skills; 3) abilities; 4) demographics. For the first three sections, the participants are asked to evaluate on a 6-point Likert scale the importance of each knowledge

[1] Given that the 95 competences are a part of our doctoral research, the main list, consisting of 87 competences, can be consulted in the First Scientific Report, "Cunoștințe, abilități și aptitudini de securitate cibernetică derivate din interacțiunea dintre securitate cibernetică în intelligence" [Cybersecurity Knowledge, Skills and Abilities Derived from the Interaction Between Cybersecurity and Intelligence], library code REF.18, and the 8 additional competences presented in the Introduction, can be consulted in the Second Scientific Report, "Proiectarea instrumentului de evaluare a competențelor prioritare de analiză de cyberintelligence în domeniul intelligence și securitate națională" [Designing a Pedagogical Assessment Instrument for Cyberintelligence Analysis High Priority Competences in Intelligence and National Security], available at "Mihai Viteazul" National Intelligence Academy Library, library code REF.22.

unit, skill and ability. After each of the first three sections, participants are asked to provide any missing elements and arguments. In the last section, demographics, participants are asked to provide their gender, age, work experience in cyber security or a related field, main work field and geographical location of the current employer. The questionnaire was distributed mostly online, but also on-site, depending on the accessibility of the researcher to the chosen experts. After the questionnaire dissemination and analysis of responses, the collection stage of our research was finished.

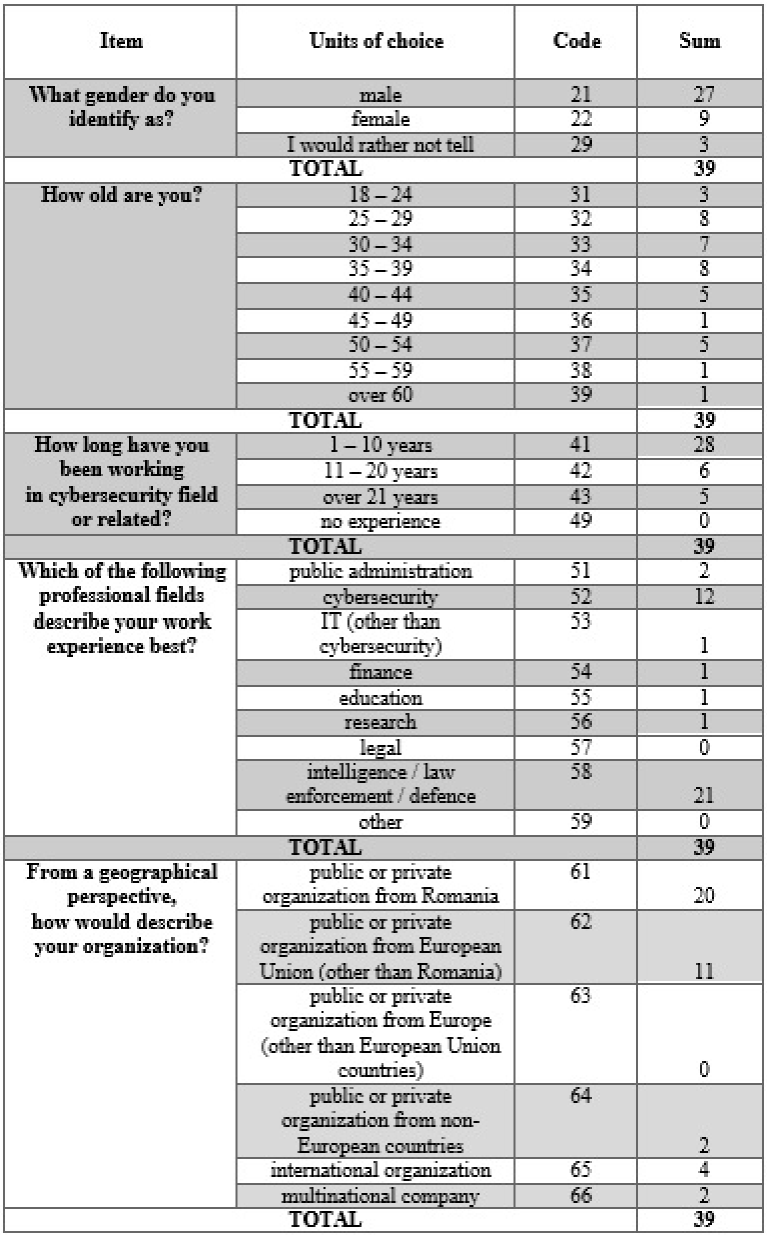
In order to ensure the reliability of the collected data, we applied two cumulative criteria: 1) exclusion of all responses generated by respondents who have no experience in cybersecurity or in a related field; 2) exclusion of all responses generated by a respondent that did not answer to all of the closed questions (i.e., this applies only for the on-site distributed questionnaires). In order to statistically analyse the data, we applied a procedure based on frequency analysis, mean and standard deviation for each knowledge unit, skill and ability. The following procedure, and in particular the threshold values, are inspired from Nilsen, that conducted similar research in order to validate and prioritize generic cybersecurity competences for regular users in public and private organizations (Nilsen 2017, p. 5). Our statistical analysis procedure followed two stages, each of them corresponding to validation and, respectively, prioritization of cybersecurity competences for the cyberintelligence analyst in intelligence and national security.

In the first stage of our statistical analysis, we considered a particular competence to be validated only if the sum of the frequency of the superior values on the 6-point Likert scale (i.e., 4, 5 and 6) is equal or above the value obtained by computing 70% of the total valid responses obtained for that particular competence. In the second stage of our statistical analysis, we considered a particular competence to have great priority, only if it respects the following descending criteria in order of importance: 1) standard deviation is less than 1, given the fact that we aim to select only those competences that generated consensus among responders; 2) average is above 5 for the valid responses (i.e., out of a maximum of 6), given the fact that we aim to select only those competences that are very important (i.e., the fifth point on the 6-point Likert scale) or extremely important (i.e., the sixth point on the 6-point Likert scale) for most respondents; 3) the value computed in the first stage of the statistical analysis is above 90%, given that we aim to filter from the validated competences only those that are extremely important for 9 out of 10 respondents.

2. Results

The questionnaire was distributed online, between June and September 2023, via Google Forms, and on-site, by the researcher. We collected a total number of 44 responses and by applying the exclusion criteria presented in the *Methodology* section, we considered 39 as valid (i.e., 5 of the respondents having no experience in cybersecurity field or in related one). Thus, in Table no. 1 we present the demographic data associated with our valid responses.

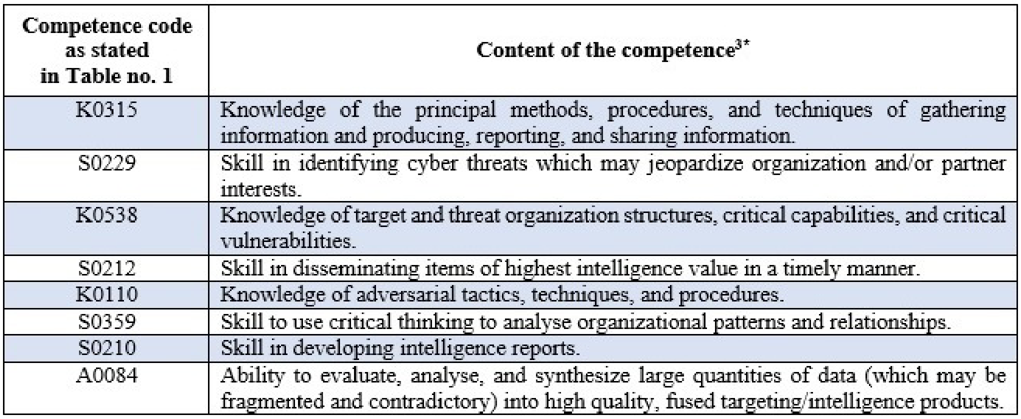
Table no. 1: Valid responses



Item	Units of choice	Code	Sum
What gender do you identify as?	male	21	27
	female	22	9
	I would rather not tell	29	3
TOTAL			39
How old are you?	18 – 24	31	3
	25 – 29	32	8
	30 – 34	33	7
	35 – 39	34	8
	40 – 44	35	5
	45 – 49	36	1
	50 – 54	37	5
	55 – 59	38	1
	over 60	39	1
TOTAL			39
How long have you been working in cybersecurity field or related?	1 – 10 years	41	28
	11 – 20 years	42	6
	over 21 years	43	5
	no experience	49	0
TOTAL			39
Which of the following professional fields describe your work experience best?	public administration	51	2
	cybersecurity	52	12
	IT (other than cybersecurity)	53	1
	finance	54	1
	education	55	1
	research	56	1
	legal	57	0
	intelligence / law enforcement / defence	58	21
	other	59	0
TOTAL			39
From a geographical perspective, how would describe your organization?	public or private organization from Romania	61	20
	public or private organization from European Union (other than Romania)	62	11
	public or private organization from Europe (other than European Union countries)	63	0
	public or private organization from non-European countries	64	2
	international organization	65	4
	multinational company	66	2
TOTAL			39

By applying the first stage procedure of our statistical analysis, we identified that 86 out of the total of 95 analysed competences were validated by respondents (i.e., 91.5% of our set of competences were validated)[2]. We will elaborate on those results in the *Discussions* section of the current article. By applying the second stage procedure of our statistical analysis, we discovered that only 8 competences are following the established quantitative criteria. Thus, in Table no. 2 we present the high priority competences for the cyberintelligence analyst in intelligence and national security. We will also elaborate on this results in the *Discussions* section.

Table no. 2: High priority competences of the cyberintelligence analyst in intelligence and national security



Competence code as stated in Table no. 1	Content of the competence[3]*
K0315	Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing information.
S0229	Skill in identifying cyber threats which may jeopardize organization and/or partner interests.
K0538	Knowledge of target and threat organization structures, critical capabilities, and critical vulnerabilities.
S0212	Skill in disseminating items of highest intelligence value in a timely manner.
K0110	Knowledge of adversarial tactics, techniques, and procedures.
S0359	Skill to use critical thinking to analyse organizational patterns and relationships.
S0210	Skill in developing intelligence reports.
A0084	Ability to evaluate, analyse, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.

3. Discussions[3]

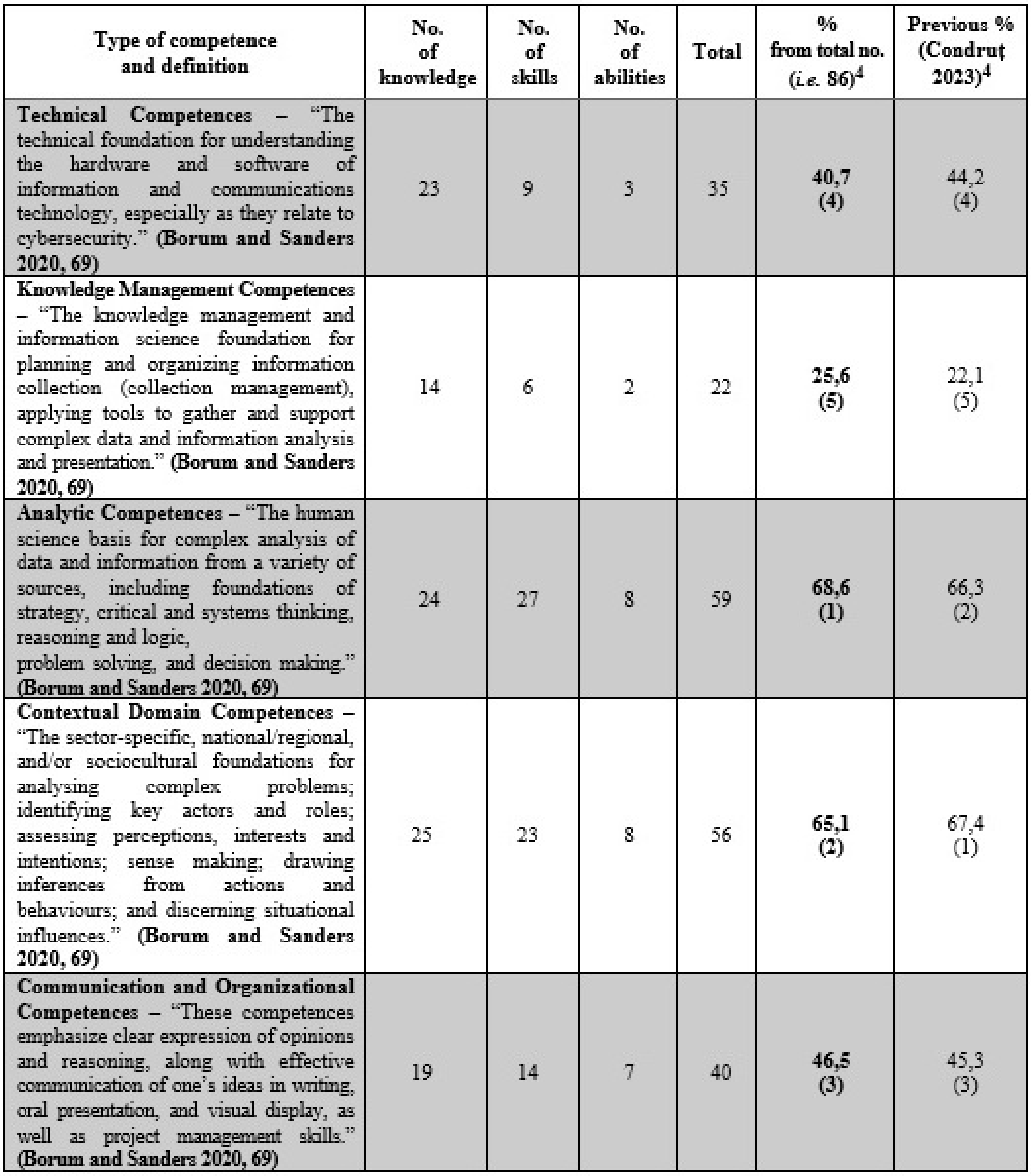
3.1. Clustering validated competences

In order to have a more structured view of the validated competences, we continued our previous research (Condruț 2023, 4206 - 4207) by clustering the validated knowledge, skills and abilities into the five types of cyberintelligence analysis competences proposed by Borum and Sanders (2020). Thus, in Table no. 3, we present how many of the validated competences can be clustered in each of the five types and we compare our current results with our previous ones (2023, pp. 4206 - 4207). We performed our clustering by applying definitions for each type of competences for every validated cyberintelligence analysis knowledge, skill and ability.

[2] The complete results can be consulted in The Second Scientific Report, *"Proiectarea instrumentului de evaluare a competențelor prioritare de analiză de cyberintelligence în domeniul intelligence și securitate națională"* [*Designing a Pedagogical Assessment Instrument for Cyberintelligence Analysis High Priority Competences in Intelligence and National Security*], available at "Mihai Viteazul" National Intelligence Academy Library.

[3] As stated in 2017 version of NICE Framework spreadsheet available at https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions

Table no. 3: Clustering the validated cyberintelligence knowledge, skills and abilities



Type of competence and definition	No. of knowledge	No. of skills	No. of abilities	Total	% from total no. (*i.e.* 86)[4]	Previous % (Condruț 2023)[4]
Technical Competences – "The technical foundation for understanding the hardware and software of information and communications technology, especially as they relate to cybersecurity." **(Borum and Sanders 2020, 69)**	23	9	3	35	**40,7** **(4)**	44,2 (4)
Knowledge Management Competences – "The knowledge management and information science foundation for planning and organizing information collection (collection management), applying tools to gather and support complex data and information analysis and presentation." **(Borum and Sanders 2020, 69)**	14	6	2	22	**25,6** **(5)**	22,1 (5)
Analytic Competences – "The human science basis for complex analysis of data and information from a variety of sources, including foundations of strategy, critical and systems thinking, reasoning and logic, problem solving, and decision making." **(Borum and Sanders 2020, 69)**	24	27	8	59	**68,6** **(1)**	66,3 (2)
Contextual Domain Competences – "The sector-specific, national/regional, and/or sociocultural foundations for analysing complex problems; identifying key actors and roles; assessing perceptions, interests and intentions; sense making; drawing inferences from actions and behaviours; and discerning situational influences." **(Borum and Sanders 2020, 69)**	25	23	8	56	**65,1** **(2)**	67,4 (1)
Communication and Organizational Competences – "These competences emphasize clear expression of opinions and reasoning, along with effective communication of one's ideas in writing, oral presentation, and visual display, as well as project management skills." **(Borum and Sanders 2020, 69)**	19	14	7	40	**46,5** **(3)**	45,3 (3)

By comparing our previous cluster analysis results with our current results, we observe that there are some differences between the two hierarchical orders of competences from Table no. 3. Thus, in our hierarchical order, the analytical

[4] We present in brackets the hierarchical order of each type of competence, 1 being the highest and 5 the lowest.

competences (i.e., 68,6%) have a slightly higher percentage than contextual domain competences (i.e., 65,1%), while our previous research hierarchical order, contextual domain competences (i.e., 67,4%) have a slightly higher percentage than analytic competences (i.e., 66,3%). This result could be a consequence of the way the questionnaire sample was built or a consequence of difference knowledge, skills and abilities that were considered in our cluster. Even more interesting is that the cluster percentages can be grouped in approximately three intervals, thus giving us an interpretation regarding the composition of our validated competences set: 1) analytic and contextual domain competences are grouped around 67%, with a deviation of 2%; 2) communication and organizational competences and technical competences can be grouped around 43% value with a deviation of maximum 2.5%; 3) knowledge competences scored 25.6% and cannot be grouped with other types of competences. This result shows us that analytic and contextual domain competences are the most prevalent in our validated set of competences, meaning that the cyberintelligence analyst should be more oriented towards knowledge, skills and abilities that are associated with the intelligence and national security domain, rather than with the technical ones. This inference is completed by the results associated with the second and the third interval, given the fact that technical and knowledge management competences are the least prevalent in our validated competences set. Thus, we assess that the cyberintelligence analyst should possess competences oriented towards intelligence analysis, applied to particular security contexts and general understanding of technical concepts. Also, it is important to note that in the second interval, we find the communication and organizational competences. This suggests the fact that the cyberintelligence analyst in intelligence and national security organizations has to be aware and apply internal regulation, protocols and norms and, in general, be adapted to the particularities of the organizational culture from these organizations.

3.2. Development of high priority competences

As previously stated, our research intention is to prioritize the validated competences in order to serve as the basis for the optimization of educational endeavours in cyberintelligence analysis. Therefore, we will analyse and discuss each of the high priority knowledge, skill and ability[5] from a teaching format perspective. Each high priority competence is discussed while taking into account particular topics of interest, examples and use cases, meaning that other researchers or educators could have different visions.

[5] Knowledge, skills and abilities discussed in this section can be found at the *NICE Framework: Current Versions* webpage on the *National Institute for Standards and Technology* website, available at https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions

- *K0315 - Knowledge of the principal methods, procedures, and techniques of gathering information and producing, reporting, and sharing information.*

One approach that could contribute to the successful knowledge transfer in this case is to structure the educational content by considering the stages of the intelligence cycle (CIA n.d.) and the cyberintelligence cycle - planning, collection, processing, analysis, dissemination and feedback (Recorded Future 2023). This is especially important given that the future cyberintelligence professionals will activate in intelligence and national security, but should also gain context dependent competences that, in this case, come from cybersecurity. Thus, methods, procedures and techniques should be taught by following each step of the intelligence and cyberintelligence cycle, with permanent links to the realm of cybersecurity (ex., technical equipment, sources of data in cybersecurity, levels of collection and analysis of threat intelligence).

- *S0229 - Skill in identifying cyber threats which may jeopardize organization and/or partner interests.*

In cyberintelligence professional settings, this skill is connected to the previous knowledge unit (i.e., K0315) as it is its foundation. In order to identify cybersecurity threats, one should understand how to ask oneself the right analytical questions and how to find the appropriate answers. Moreover, if the appropriate answers are found, it is important to integrate data that come from different sources and feeds of cyberintelligence. Many educational endeavours in cyberintelligence focus their efforts in the formation of this particular skill[6], but do not approach elements that are particular to the intelligence and national security field, such as collection from HUMINT. Integration of multiple sources and data specific to cybersecurity with HUMINT collection or other intelligence and national security-dependent types of sources is crucial in order to have a comprehensive understanding of a cybersecurity threat.

- *K0538 - Knowledge of target and threat organization structures, critical capabilities, and critical vulnerabilities.*

In order to make a proper transfer of this knowledge, the educator should focus the educational content around the understanding of the role and objectives of an organization. Besides these elements, understanding organization structures, critical capabilities and vulnerabilities is also dependent on understanding what the architecture of a particular IT&C infrastructure is and what particular elements are of critical importance. Thus, we believe that this knowledge can be trained by understanding management and risk analysis concepts and principles. This emphasizes the aforementioned idea that the cyberintelligence analyst should not

[6] *Mastering Cyber Threat Identification and Defense Strategies* by Public Sector Network, available at https://publicsectornetwork.com/event/online-training-mastering-cyber-threat-identification-in-the-public-sector/ and *Detecting and Mitigating Cyber Threats and Attacks* by Colorado University, available at https://www.coursera.org/learn/detecting-cyber-attacks

focus on possessing practical technical skills, but rather on understanding the technical elements that could support them in the analytical processes. In this particular case, if an organization is a victim of a cyber threat, the analyst should not only investigate the attacker, but also the victim. This way of thinking about the materialization of a cyber treat is implemented in the *Diamond Model* (Caltagirone 2020).

- *S0212 - Skill in disseminating items of highest intelligence value in a timely manner* and *S0210 - Skill in developing intelligence reports.*

We will approach both skills concurrently, because they refer to similar aspects, given the fact that intelligence dissemination depends on intelligence reporting. These skills are important not only for cyberintelligence analysis, but also for intelligence analysis in general. The US Government states on its Intelligence Careers website that "The final output of intelligence analysis is a carefully crafted intelligence report that provides political and military leaders with the information they need to make critical decisions. Skills central to the profession include analytical thinking and logical reasoning, the ability to write clear, concise reports and the ability to objectively analyse all sides of any given issue" (US Government n.d.). Still, cyberintelligence analysis is different from intelligence analysis performed in other national security branches, such as counterterrorism or counterespionage, given the fact that cyberintelligence analysis requires understanding and integration of technical aspects derived from cybersecurity investigations. This aspect generates the need for education and training endeavours specially designed to facilitate understanding and make it possible to operate with concepts specific to cyber threats, cyber vulnerabilities, tactics, techniques and procedures of hostile actors, our high priority competences being composed of such elements. Despite cybersecurity-derived knowledge units, the cyberintelligence analyst in intelligence and national security should be able to adapt to their beneficiary, given that not all decision-makers have the same level of understanding of cybersecurity technical aspects that could be a part of an intelligence product. If we corroborate this aspect with the reasonable expectation of not having a pattern for the actions performed by hostile threat actors, we infer that dissemination of high-quality intelligence products in a timely manner is crucial for countering any cyber threat. Thus, we believe that training actions for developing S0210 and S0212 are dependent on good practices and principles of intelligence analysis writing, one important work in this field being *Writing Classified and Unclassified Papers in the Intelligence Community* (Major 2009). Adding to this academic work, one could be able to identify training formats that focus on cybersecurity writing, such as *Cybersecurity Writing: Hack the Reader* (SANS Institute n.d.). Our educational approach regarding these particular skills and abilities would elaborate on Major's intelligence analysis writing principles while applying them to cybersecurity and cyberintelligence information.

- *K0110 – Knowledge of adversarial tactics, techniques, and procedures.*

While this is one of the most technical knowledge units from our set, from an educational perspective it is one of the most straightforward, if we consider the existence of *MITRE ATT&ACK Framework*[7], that is a database which consists of tactics, techniques and procedures specific to a large number of well-known threat actors. Also, given the fact that *MITRE ATT&CK Framework* contains definitions and use cases for every tactic, technique and procedure, it can be considered a really good educational resource, both for self-paced learning as well as for teacher-led formats. By gaining K0110, future cyberintelligence analysist in intelligence and national security, will be able to better understand how threat actors operate, how certain ways of operations interact and will be able to actively contribute to cyberintelligence investigations and to integrate technical data into cyberintelligence products designed to be disseminated to decision-makers.

- *S0359 – Skill to use critical thinking to analyse organisational patterns and relationships.*

Although critical thinking is a skill that can be educated with specific theoretical and practical content, we believe that in the context of cyberintelligence analysis training endeavours it might be one of the hardest to foster. As stated before, cyberintelligence analysis in intelligence and national security is highly dependent on contextual competences, which means that trainees and professionals in this field should be exposed to multiple use cases in real or fictious investigations, which can foster expert judgement ability and critical thinking skills. This perspective is complemented by Srinivas who states that the cyberintelligence analysts should imagine themselves in the role of a cyber attacker, in order to make the best possible analytical judgements (Srinivas 2018, p. 406). In order for this to happen, we insist on the fact that the cyberintelligence analyst should be exposed to many practical examples of cybersecurity and cyberintelligence investigations and case, that can diversify their expertise on this matter. Also, an important aspect for fostering critical thinking is to expose the cyberintelligence analyst to multiple and different analytical methods and ways of disseminating intelligence materials both theoretically and practically.

- *A0084 – Ability to evaluate, analyse, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.*

Like S0359, we believe that A0084 is equally hard to train. This ability is rather trained on a continuum of educational activities, than by crafting and applying specific educational content and practical activities. Still, in a cyberintelligence analysis educational setting, one educator can propose to students' examples of fictitious use cases that are comprised of large quantities of data, both technical

[7] Available at URL: https://attack.mitre.org/

and non-technical, from which the students should extract the most important facts and perform assessments. For doing this kind of activities, cyberintelligence analyst should be able to apply structured analytical techniques, such as sorting, chronologies and timelines, event trees, event mapping and source check (US Defense Intelligence Agency 2008) and to possess good communication and organizational skills, especially when information is fragmented and contradictory and requires clarifications from collectors.

Conclusions

Starting from the research question – *How can we validate and prioritize knowledge, skills and abilities needed by the cyberintelligence analyst in intelligence and national security?* – we managed to achieve our research objective – *validate and prioritize the set of cybersecurity and intelligence competencies by applying a survey with the participation of cybersecurity, cyberintelligence and intelligence and national security experts*. In the first phase, we validated 86 out of the 95 cybersecurity and intelligence competences, most of them being clustered in analytical and context dependent competences. This shows us that cyberintelligence analysis is rather dependent on the type of organization where it is performed, intelligence and national security agencies, and on the specific context that is taken into account when performing an investigation, rather than on the technical aspects that are fundamental to the cybersecurity field. Thus, cyberintelligence analysis is more of an intelligence analysis subfield, rather than a cybersecurity one, proving that intelligence and national security organizations should consider crafting a profile of competences specific to their own organizational needs and subsequent training and education formats. In this context, relying separately on cybersecurity and intelligence courses and training endeavours is not sufficient and closing the gap in this matter consists in creating bespoke educational activities.

Also, we managed to classify as high priority eight out of the 86 priorly identified competences and to briefly elaborate on the specific educational practices and contexts that could be applied by educators in cyberintelligence analysis. In the particular context of these eight high priority competences, we believe that the educational approaches should combine cybersecurity and intelligence content, while understanding that cyberintelligence analysis competences can be trained over time, ideally by combing classical training formats with professional expertise. Thus, a cyberintelligence analyst learner profile should include intelligence analysis competences, dependent on knowledge, skills and abilities regarding collection, reporting, disseminating and sharing of information, and cybersecurity competences, dependent on knowledge referring to tactics, techniques and procedures of cyber hostile actors, cybersecurity vulnerabilities and critical capabilities. The utmost important thing for a cyberintelligence analysis educator is to combine those elements and not teach them separately.

Regarding the limits of our research, we appreciate that the low response rate corroborated with the judgment sampling method, could induce bias to our results. Thus, in order to really test our research results it is important to verify them in real educational settings, by performing experimental studies, this being one of the future research directions.

A possible direction to continue our research would be to integrate the validated competences into a coherent cyberintelligence analysis professional framework, that could be used by employers and educators.

BIBLIOGRAPHY:

Alsmadi, Izzat. 2023. *The NICE Cyber Security Framework. Cyber Security Intelligence and Analytics Second Edition.* San Antonio, Texas: Springer.

Borum, Randy, and Ron Sanders. 2020. "Preparing America's Cyber Intelligence Workforce." *IEEE Security & Privacy* (IEEE) 18 (5): 67-73. Accessed August 24, 2023. doi:10.1109/MSEC.2020.3005035.

Borum, Randy, and Ron Sanders. 2020. "Preparing America's Cyber Intelligence Workforce." *IEEE Security & Privacy* 18 (5): 67 - 73. doi:10.1109/MSEC.2020.3005035.

Caltagirone, Sergio. 2020. *The Diamond Model of Intrusion Analysis.* ThreatIntellAcademy. https://www.threatintel.academy/wp-content/uploads/2020/07/diamond_summary.pdf

CIA. n.d. "Spy Kids." *Central Intelligence Agency.* Accessed December 7, 2023. https://www.cia.gov/spy-kids/parents-teachers/docs/Briefing-intelligence-cycle.pdf

Condruț, Cristian. 2023. "CYBERSECURITY KNOWLEDGE, SKILLS AND ABILITIES FOR INTELLIGENCE AND NATIONAL SECURITY ANALYSTS." *16th annual International Conference of Education, Research and Innovation.* Seville: IATED. 4200 - 4209.

Major, James. 2009. *Writing Classified and Unclassified Papers in the Intelligence Community.* New York: Scarecrow Press.

Nilsen, Richard. 2017. *Measuring Cybersecurity Competency: An Exploratory Investigation of the Cybersecurity Knolwledge, Skills and Abilities Necessary for Organizational Network Access Privileges.* Fort Lauderdale-Davie, Florida: Nova Southeastern University.

PennState. n.d. *Intelligence Writing.* Accessed December 7, 2023. https://www.e-education.psu.edu/geog571/node/431

Petersen, Rodney, Danielle Santos, Karen Wetzel, Matthew Smith, şi Greg Witte. 2020. “The Workforce Framework for Cybersecurity (NICE Framework).” *NIST.* noiembrie. Accessed November 27, 2023. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Recorded Future. 2023. *What the 6 Phases of the Threat Intelligence Lifecycle Mean for Your Team.* octombrie 24. Accessed December 7, 2023. https://www.recordedfuture.com/threat-intelligence-lifecycle-phases

SANS Institute. n.d. Accessed December 7, 2023. https://www.sans.org/cyber-security-courses/cyber-security-writing-hack-the-reader/

Sharma, Gaganpreet. 2017. “Pros and cons of different sampling techniques.” *International Journal of Applied Research* 3 (7): 749 - 752.

Srinivas, Nowduri. 2018. “Critical Thinking and Best Practices for Cyber Security.” *International Journal of Cyber-Security and Digital Forensics* (The Society of Digital Information and Wireless Communications) 7 (4): 391 - 409.

US Defense Intelligence Agency. 2008. *A Tradecraft Primer: Basic Structured Analytic Techniques.* Primer, Directorate for Analysis.

US Government. n.d. *CAREER FIELDS.* Accessed December 7, 2023. https://www.intelligencecareers.gov/career-fields#intelligence-analysis

Vitello, Sylvia, Jackie Greatorex, and Stuart Shaw. 2021. *What is competence? A shared interpretation of competence to support teaching, learning and assessment.* Cambridge: Cambridge University Press & Assessment.